kaspersky

Kaspersky Security Center 15.1 Windows

© 2026 AO Kaspersky Lab

Sommario

Guida di Kaspersky Security Center 15.1

Novità

Informazioni su Kaspersky Security Center

- Architettura
- Requisiti hardware e software
  - Requisiti di Administration Server
  - Requisiti di Web Console
  - Requisiti dei server mobili
  - Requisiti di Administration Console
  - Requisiti di Network Agent
- Applicazioni e soluzioni Kaspersky compatibili
- Licenze e funzionalità di Kaspersky Security Center 15.1
- Informazioni sulla compatibilità dei componenti di Kaspersky Security Center
- Confronto tra Kaspersky Security Center basato su Windows e basato su Linux
- Informazioni di Kaspersky Security Center Cloud Console

Kaspersky Security Center 15.1

- Concetti di base
  - Administration Server
  - Gerarchia di Administration Server
  - Administration Server virtuale
  - Server per dispositivi mobili
  - Server Web
  - Network Agent
  - Gruppi di amministrazione
  - Dispositivo gestito
  - Dispositivo non assegnato
  - Workstation dell'amministratore
  - Plug-in di gestione
  - Plug-in Web di gestione
  - Criteri
  - Profili criterio
  - Attività
  - Ambito attività
  - Relazioni tra impostazioni locali delle applicazioni e criteri
  - Punto di distribuzione
  - Gateway di connessione
- Scenario di installazione principale
- Porte utilizzate da Kaspersky Security Center
- Certificati per l'utilizzo di Kaspersky Security Center
  - Informazioni sui certificati di Kaspersky Security Center
  - Informazioni sul certificato di Administration Server
  - Requisiti per i certificati personalizzati utilizzati in Kaspersky Security Center
  - Scenario: Specificazione del certificato di Administration Server personalizzato

Sostituzione del certificato di Administration Server con l'utilità klsetsrvcert
Connessione dei Network Agent ad Administration Server con l'utilità klmover
Riemissione del certificato del server Web
Schemi per traffico dati e utilizzo delle porte
Administration Server e dispositivi gestiti nella LAN
Administration Server primario nella LAN e due Administration Server secondari
Administration Server nella LAN, dispositivi gestiti in Internet, proxy inverso in uso
Administration Server nella LAN, dispositivi gestiti in Internet, gateway di connessione in uso
Administration Server all'interno della rete perimetrale, dispositivi gestiti in Internet
Interazione dei componenti di Kaspersky Security Center e delle applicazioni di protezione: ulteriori informazioni
Convenzioni utilizzate negli schemi di interazione
Administration Server e DBMS
Administration Server e Administration Console
Administration Server e dispositivo client: gestione dell'applicazione di protezione
Upgrade del software in un dispositivo client tramite un punto di distribuzione
Gerarchia di Administration Server: Administration Server primario e Administration Server secondario
Gerarchia di Administration server con un Administration Server secondario nella rete perimetrale
Administration Server, un gateway di connessione in un segmento di rete e un dispositivo client
Administration Server e due dispositivi nella rete perimetrale: un gateway di connessione e un dispositivo client
Administration Server e Kaspersky Security Center Web Console
Attivazione e gestione dell'applicazione di protezione in un dispositivo mobile
Best practice per la distribuzione
Guida all'hardening
Distribuzione di Administration Server
Sicurezza della connessione
Account e autenticazione
Gestione della protezione di Administration Server
Gestione della protezione dei dispositivi client
Configurazione della protezione per le applicazioni gestite
Manutenzione di Administration Server
Trasferimento di eventi a sistemi di terzi
Suggerimenti sulla sicurezza per i sistemi informativi di terze parti
Suggerimenti per l'utilizzo delle applicazioni di protezione Kaspersky
Preparazione per la distribuzione
Pianificazione della distribuzione di Kaspersky Security Center
Schemi tipici di distribuzione di un sistema di protezione
Informazioni sulla pianificazione della distribuzione di Kaspersky Security Center nella rete di un'organizzazione
Selezione di una struttura per la protezione di un'azienda
Configurazioni standard di Kaspersky Security Center
Configurazione standard: singola sede
Configurazione standard: poche sedi su larga scala gestite da amministratori distinti
Configurazione standard: più sedi remote di piccole dimensioni
Selezione di un DBMS per Administration Server
Configurazione del server MariaDB x64 per l'utilizzo con Kaspersky Security Center 15.1
Configurazione del server MySQL x64 per l'utilizzo con Kaspersky Security Center 15.1
Configurazione del server PostgreSQL o Postgres per l'utilizzo con Kaspersky Security Center 15.1
Gestione dei dispositivi mobili con Kaspersky Endpoint Security for Android

Concessione dell'accesso via Internet all'Administration Server
Accesso a Internet: Administration Server in una rete locale
Accesso a Internet: Administration Server in una rete perimetrale
Accesso a Internet: Network Agent come gateway di connessione nella rete perimetrale
Informazioni sui punti di distribuzione
Aumento del limite dei descrittori di file per il servizio klnagent
Calcolo del numero e configurazione dei punti di distribuzione
Gerarchia di Administration Server
Administration Server virtuali
Informazioni sulle limitazioni di Kaspersky Security Center
Carico di rete
Distribuzione iniziale della protezione anti-virus
Aggiornamento iniziale dei database anti-virus
Sincronizzazione di un client con Administration Server
Aggiornamento aggiuntivo dei database anti-virus
Elaborazione di eventi nei client da parte di Administration Server
Traffico nell'arco di 24 ore
Preparazione per Mobile Device Management
Server per dispositivi mobili MDM iOS
Configurazione standard: gestione di Kaspersky Device Management for iOS nella rete perimetrale
Configurazione standard: server per dispositivi mobili MDM iOS nella rete locale di un'organizzazione
Gestione dei dispositivi mobili con Kaspersky Endpoint Security for Android
Informazioni sulle prestazioni di Administration Server
Limitazioni relative alla connessione a un Administration Server
Risultati dei test sulle prestazioni di Administration Server
Risultati dei test sulle prestazioni del server proxy KSN
Impostazioni di rete per l'interazione con servizi esterni
Distribuzione di Network Agent e dell'applicazione di protezione
Distribuzione iniziale
Configurazione dei programmi di installazione
Pacchetti di installazione
Proprietà e file di trasformazione MSI
Distribuzione con strumenti di terze parti per l'installazione remota delle applicazioni
Informazioni sulle attività di installazione remota in Kaspersky Security Center
Distribuzione tramite l'acquisizione e la copia dell'immagine di un dispositivo
Errori di copia di un'immagine del disco rigido
Distribuzione tramite i criteri di gruppo di Microsoft Windows
Distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center
Esecuzione di pacchetti indipendenti creati tramite Kaspersky Security Center
Opzioni per l'installazione manuale delle applicazioni
Creazione di un file MST
Installazione remota delle applicazioni nei dispositivi in cui è installato Network Agent
Gestione dei riavvii dei dispositivi nell'attività di installazione remota
Aggiornamento dei database in un pacchetto di installazione di un'applicazione di protezione
Utilizzo di strumenti per l'installazione remota di applicazioni in Kaspersky Security Center per l'esecuzione di file eseguibili nei dispositivi gestiti
Monitoraggio della distribuzione

Configurazione dei programmi di installazione
Informazioni generali
Installazione in modalità automatica (con un file di risposta)
Installazione di Network Agent in modalità automatica (senza un file di risposta)
Configurazione parziale dell'installazione tramite setup.exe
Parametri di installazione di Administration Server
Parametri di installazione di Network Agent
Infrastruttura virtuale
Suggerimenti per la riduzione del carico sulle macchine virtuali
Supporto delle macchine virtuali dinamiche
Supporto della copia delle macchine virtuali
Supporto del rollback del file system per i dispositivi con Network Agent
Installazione locale delle applicazioni
Installazione locale di Network Agent
Installazione di Network Agent in modalità automatica
Installazione di Network Agent per Linux in modalità automatica (con un file di risposte)
Preparazione di un dispositivo in cui viene eseguito Astra Linux in modalità ambiente software chiuso per l'installazione di Network Agent
Installazione di Network Agent per Linux in modalità interattiva
Installazione locale del plug-in di gestione dell'applicazione
Installazione di applicazioni in modalità automatica
Installazione delle applicazioni tramite pacchetti indipendenti
Impostazioni del pacchetto di installazione di Network Agent
Visualizzazione dell'Informativa sulla privacy
Distribuzione di sistemi per la gestione dei dispositivi mobili
Distribuzione di un sistema per la gestione tramite il protocollo MDM iOS
Installazione del server MDM iOS
Installazione di un server MDM iOS in modalità automatica
Scenari di distribuzione del server MDM iOS
Schema di distribuzione semplificato
Schema di distribuzione tramite Kerberos Constrained Delegation (KCD)
Ricezione di un certificato APNs
Rinnovo di un certificato APNs
Configurazione di un certificato del server per dispositivi mobili MDM iOS di riserva
Installazione di un certificato APNs in un server MDM iOS
Configurazione dell'accesso al servizio Apple Push Notification
Emissione e installazione di un certificato condiviso in un dispositivo mobile
Aggiunta di un dispositivo KES all'elenco dei dispositivi gestiti
Connessione dei dispositivi KES ad Administration Server
Connessione diretta dei dispositivi all'Administration Server
Schema per la connessione dei dispositivi KES al server tramite Kerberos Constrained Delegation (KCD)
Utilizzo di Firebase Cloud Messaging
Integrazione con PKI (Public Key Infrastructure)
Server Web di Kaspersky Security Center
Installazione di Kaspersky Security Center
Preparazione dell'installazione
Account per l'utilizzo del DBMS

Configurazione degli account per l'utilizzo di SQL Server (autenticazione di Windows)
Configurazione degli account per l'utilizzo di SQL Server (autenticazione di SQL Server)
Configurazione degli account per l'utilizzo di MySQL e MariaDB
Spostamento dei dati da un tablespace condiviso a un tablespace file per tabella in un DBMS MySQL e MariaDB
Configurazione degli account per l'utilizzo di PostgreSQL e Postgres Pro
Scenario: Autenticazione di Microsoft SQL Server
Scenario: autenticazione di MySQL Server
Scenario: autenticazione del server PostgreSQL
Raccomandazioni sull'installazione di Administration Server
Creazione degli account per i servizi di Administration Server in un cluster di failover
Definizione di una cartella condivisa
Installazione remota con gli strumenti di Administration Server tramite i criteri di gruppo di Active Directory
Installazione remota tramite l'invio del percorso UNC di un pacchetto indipendente
Aggiornamento dalla cartella condivisa di Administration Server
Installazione di immagini dei sistemi operativi
Specificazione dell'indirizzo dell'Administration Server
Installazione standard
Passaggio 1. Visualizzazione del Contratto di licenza e dell'Informativa sulla privacy
Passaggio 2. Selezione del metodo di installazione
Passaggio 3. Installazione di Kaspersky Security Center Web Console
Passaggio 4. Selezione delle dimensioni della rete
Passaggio 5. Selezione di un database
Passaggio 6. Configurazione di SQL Server
Passaggio 7. Selezione di un metodo di autenticazione
Passaggio 8. Decompressione e installazione dei file nel disco rigido
Installazione personalizzata
Passaggio 1. Visualizzazione del Contratto di licenza e dell'Informativa sulla privacy
Passaggio 2. Selezione del metodo di installazione
Passaggio 3. Selezione dei componenti da installare
Passaggio 4. Installazione di Kaspersky Security Center Web Console
Passaggio 5. Selezione delle dimensioni della rete
Passaggio 6. Selezione di un database
Passaggio 7. Configurazione di SQL Server
Passaggio 8. Selezione di un metodo di autenticazione
Passaggio 9. Selezione dell'account per l'avvio di Administration Server
Passaggio 10. Selezione dell'account per l'esecuzione dei servizi di Kaspersky Security Center
Passaggio 11. Selezione di una cartella condivisa
Passaggio 12. Configurazione della connessione ad Administration Server
Passaggio 13. Definizione dell'indirizzo di Administration Server
Passaggio 14. Indirizzo di Administration Server per la connessione dei dispositivi mobili
Passaggio 15. Selezione dei plug-in di gestione dell'applicazione
Passaggio 16. Decompressione e installazione dei file nel disco rigido
Distribuzione del cluster di failover Kaspersky Security Center
Scenario: Distribuzione di un cluster di failover Kaspersky Security Center
Informazioni sul cluster di failover Kaspersky Security Center
Preparazione di un file server per un cluster di failover Kaspersky Security Center
Preparazione dei nodi per un cluster di failover Kaspersky Security Center

Installazione di Kaspersky Security Center nei nodi del cluster di failover Kaspersky Security Center
Avvio e arresto manuale dei nodi del cluster
Installazione di Administration Server in un cluster di failover di Windows Server
Passaggio 1. Visualizzazione del Contratto di licenza e dell'Informativa sulla privacy
Passaggio 2. Selezionare il tipo di installazione nel cluster
Passaggio 3. Definizione del nome dell'Administration Server virtuale
Passaggio 4. Definizione dei dettagli di rete dell'Administration Server virtuale
Passaggio 5. Definizione di un gruppo di cluster
Passaggio 6. Per selezionare un archivio dati del cluster
Passaggio 7. Definizione di un account per l'installazione remota
Passaggio 8. Selezione dei componenti da installare
Passaggio 9. Selezione delle dimensioni della rete
Passaggio 10. Selezione di un database
Passaggio 11. Configurazione di SQL Server
Passaggio 12. Selezione di un metodo di autenticazione
Passaggio 13. Selezione dell'account per l'avvio di Administration Server
Passaggio 14. Selezione dell'account per l'esecuzione dei servizi di Kaspersky Security Center
Passaggio 15. Selezione di una cartella condivisa
Passaggio 16. Configurazione della connessione ad Administration Server
Passaggio 17. Definizione dell'indirizzo di Administration Server
Passaggio 18. Indirizzo di Administration Server per la connessione dei dispositivi mobili
Passaggio 19. Decompressione e installazione dei file nel disco rigido
Installazione di Administration Server in modalità automatica
Installazione di Administration Console nella workstation dell'amministratore
Modifiche apportate al sistema dopo l'installazione di Kaspersky Security Center
Disinstallazione dell'applicazione
Informazioni sull'aggiornamento di Kaspersky Security Center
Upgrade di Kaspersky Security Center da una versione precedente
Aggiornamento di Kaspersky Security Center nei nodi del cluster di failover Kaspersky Security Center
Aggiornamento di Kaspersky Security Center nei nodi del cluster di failover Microsoft
Configurazione iniziale di Kaspersky Security Center
Guida all'hardening
Avvio rapido guidato di Administration Server
Informazioni sull'avvio rapido guidato
Avvio dell'Avvio rapido guidato di Administration Server
Passaggio 1. Configurazione di un server proxy
Passaggio 2. Selezione del metodo di attivazione dell'applicazione
Passaggio 3. Selezione delle aree di protezione e dei sistemi operativi
Passaggio 4. Selezione dei plug-in per le applicazioni gestite
Passaggio 5. Download dei pacchetti di distribuzione e creazione dei pacchetti di installazione
Passaggio 6. Configurazione dell'utilizzo di Kaspersky Security Network
Passaggio 7. Configurazione delle notifiche e-mail
Passaggio 8. Configurazione della gestione degli aggiornamenti
Passaggio 9. Creazione di una configurazione della protezione iniziale
Passaggio 10. Connessione dei dispositivi mobili
Passaggio 11. Download degli aggiornamenti
Passaggio 12. Device discovery

Passaggio 13. Chiusura dell'Avvio rapido guidato
Configurazione della connessione di Administration Console ad Administration Server
Configurazione delle impostazioni di accesso a Internet per Administration Server
Connessione dei dispositivi fuori sede
Scenario: Connessione dei dispositivi fuori sede tramite un gateway di connessione
Scenario: connessione di dispositivi fuori sede tramite un Administration Server secondario in DMZ
Informazioni sulla connessione dei dispositivi fuori sede
Connessione dei dispositivi desktop esterni ad Administration Server
Informazioni sui profili di connessione per gli utenti fuori sede
Creazione di un profilo di connessione per gli utenti fuori sede
Informazioni sul passaggio di Network Agent ad altri Administration Server
Creazione di una regola per il passaggio di Network Agent in base al percorso di rete
Notifiche degli eventi
Configurazione delle notifiche degli eventi
Testing delle notifiche
Notifiche degli eventi visualizzate dall'esecuzione di un file eseguibile
Criptaggio delle comunicazioni con TLS
Configurazione dell'interfaccia
Individuazione dei dispositivi nella rete
Scenario: Individuazione dei dispositivi nella rete
Dispositivi non assegnati
Device discovery
Polling della rete Windows
Polling Active Directory
Polling intervallo IP
Polling zeroconf
Utilizzo di domini Windows. Visualizzazione e modifica delle impostazioni del dominio
Configurazione delle regole di conservazione per i dispositivi non assegnati
Utilizzo degli intervalli IP
Creazione di un intervallo IP
Visualizzazione e modifica delle impostazioni degli intervalli IP
Utilizzo di gruppi Active Directory. Visualizzazione e modifica delle impostazioni dei gruppi
Creazione di regole per lo spostamento automatico dei dispositivi nei gruppi di amministrazione
Utilizzo della modalità dinamica VDI nei dispositivi client
Abilitazione della modalità dinamica VDI nelle proprietà di un pacchetto di installazione per Network Agent
Ricerca dei dispositivi appartenenti a VDI
Spostamento dei dispositivi da VDI a un gruppo di amministrazione
Inventario dei dispositivi
Aggiunta di informazioni sui nuovi dispositivi
Configurazione dei criteri utilizzati per definire i dispositivi aziendali
Configurazione dei campi personalizzati
Licensing
Eventi di superamento del limite di licenze
Informazioni sulle licenze
Informazioni sulla licenza
Informazioni sul Contratto di licenza con l'utente finale
Informazioni sul certificato di licenza

Informazioni sulla chiave di licenza
Informazioni sul file chiave
Informazioni sull'abbonamento
Informazioni sul codice di attivazione
Revoca del consenso a un Contratto di licenza con l'utente finale
Informazioni sulla trasmissione dei dati
Opzioni di licensing per Kaspersky Security Center
Funzionalità di gestione delle licenze di Kaspersky Security Center e delle applicazioni gestite
Applicazioni Kaspersky. Distribuzione centralizzata
Sostituzione di applicazioni di protezione di terzi
Installazione delle applicazioni tramite un'attività di installazione remota
Installazione di un'applicazione nei dispositivi selezionati
Installazione di un'applicazione nei dispositivi client di un gruppo di amministrazione
Installazione di un'applicazione utilizzando i criteri di gruppo di Active Directory
Installazione remota delle applicazioni nei dispositivi macOS
Installazione di applicazioni negli Administration Server secondari
Installazione delle applicazioni tramite l'Installazione remota guidata
Utilizzo dei plug-in di gestione
Visualizzazione di un rapporto sulla distribuzione della protezione
Rimozione remota delle applicazioni
Rimozione remota di un'applicazione dai dispositivi client del gruppo di amministrazione
Rimozione remota di un'applicazione dai dispositivi selezionati
Utilizzo dei pacchetti di installazione
Creazione di un pacchetto di installazione
Creazione di pacchetti di installazione indipendenti
Creazione di pacchetti di installazione personalizzati
Visualizzazione e modifica delle proprietà dei pacchetti di installazione personalizzati
Come ottenere il pacchetto di installazione di Network Agent dal kit di distribuzione di Kaspersky Security Center
Distribuzione dei pacchetti di installazione agli Administration Server secondari
Distribuzione dei pacchetti di installazione tramite punti di distribuzione
Trasferimento dei risultati sull'installazione delle applicazioni a Kaspersky Security Center
Definizione dell'indirizzo del server proxy KSN per i pacchetti di installazione
Ricezione delle versioni aggiornate delle applicazioni
Preparazione di un dispositivo Windows per l'installazione remota
Preparazione di un dispositivo Linux e installazione di Network Agent in un dispositivo Linux da remoto
Preparazione di un dispositivo che esegue SUSE Linux Enterprise Server 15 per l'installazione di Network Agent
Preparazione di un dispositivo macOS per l'installazione remota di Network Agent
Applicazioni Kaspersky: licensing e attivazione
Licensing delle applicazioni gestite
Visualizzazione delle informazioni sulle chiavi di licenza in uso
Aggiunta di una chiave di licenza all'archivio dell'Administration Server
Rimozione di una chiave di licenza di Administration Server
Distribuzione di una chiave di licenza ai dispositivi client
Distribuzione automatica di una chiave di licenza
Creazione e visualizzazione di un rapporto sull'utilizzo delle chiavi di licenza
Visualizzazione delle informazioni sulle chiavi di licenza dell'applicazione
Esportazione di un file di chiave di licenza

Configurazione della protezione di rete
Scenario: Configurazione della protezione di rete
Configurazione e propagazione dei criteri: approccio incentrato sui dispositivi
Informazioni sui metodi di gestione della protezione incentrati sui dispositivi e incentrati sugli utenti
Configurazione manuale del criterio di Kaspersky Endpoint Security
Configurazione del criterio nella sezione Protezione minacce avanzata
Configurazione del criterio nella sezione Protezione minacce essenziale
Configurazione del criterio nella sezione Impostazioni generali
Configurazione del criterio nella sezione Configurazione eventi
Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security
Configurazione manuale dell'attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security
Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
Configurazione manuale dell'attività di gruppo per l'installazione degli aggiornamenti e la correzione delle vulnerabilità
Impostazione del numero massimo di eventi nell'archivio eventi
Impostazione del periodo di archiviazione massimo per le informazioni sulle vulnerabilità corrette
Gestione di attività
Creazione di un'attività
Creazione dell'attività di Administration Server
Creazione di un'attività per dispositivi specifici
Creazione di un'attività locale
Visualizzazione di un'attività di gruppo ereditata nell'area di lavoro di un gruppo nidificato
Accensione automatica dei dispositivi prima dell'avvio di un'attività
Spegnimento automatico di un dispositivo dopo il completamento di un'attività
Limitazione del tempo di esecuzione delle attività
Esportazione di un'attività
Importazione di un'attività
Conversione di attività
Avvio e arresto manuale di un'attività
Sospensione e ripresa manuale di un'attività
Monitoraggio dell'esecuzione delle attività
Visualizzazione dei risultati dell'esecuzione delle attività memorizzati in Administration Server
Configurazione di filtri per le informazioni sui risultati dell'esecuzione delle attività
Modifica di un'attività. Rollback delle modifiche
Confronto delle attività
Account per l'avvio delle attività
Esportazione delle cronologia esecuzione attività
Procedura guidata per la modifica della password delle attività
Passaggio 1. Immissione delle credenziali
Passaggio 2. Selezione di un'azione da eseguire
Passaggio 3. Visualizzazione dei risultati
Creazione di una gerarchia di gruppi di amministrazione subordinati a un Administration Server virtuale
Criteri e profili criterio
Gerarchia di criteri tramite i profili criterio
Gerarchia dei criteri
Profili criterio
Ereditarietà delle impostazioni dei criteri
Gestione dei criteri

Creazione di un criterio
Visualizzazione dei criteri ereditati in un sottogruppo
Attivazione di un criterio
Attivazione automatica di un criterio quando si verifica un evento Epidemia di virus
Applicazione di un criterio fuori sede
Modifica di un criterio. Rollback delle modifiche
Confronto dei criteri
Visualizzazione del grafico dello stato di distribuzione dei criteri
Eliminazione di un criterio
Copia di un criterio
Esportazione di un criterio
Importazione di un criterio
Conversione di criteri
Gestione dei profili criterio
Creazione di un profilo criterio
Modifica di un profilo criterio
Eliminazione di un profilo criterio
Creazione di una regola di attivazione del profilo criterio
Regole di spostamento dei dispositivi
Clonazione delle regole di spostamento dei dispositivi
Classificazione del software
Prerequisiti per l'installazione delle applicazioni nei dispositivi di un'organizzazione client
Visualizzazione e modifica delle impostazioni locali delle applicazioni
Aggiornamento di Kaspersky Security Center e delle applicazioni gestite
Scenario: Aggiornamento periodico di database e applicazioni Kaspersky
Informazioni sull'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky
Informazioni sull'utilizzo dei file diff per l'aggiornamento dei database e dei moduli del software Kaspersky
Abilitazione della funzionalità Download dei file diff
Creazione dell'attività per il download degli aggiornamenti nell'archivio di Administration Server
Creazione dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione
Configurazione dell'attività Scarica aggiornamenti nell'archivio di Administration Server
Verifica degli aggiornamenti scaricati
Configurazione di criteri di test e attività ausiliarie
Visualizzazione degli aggiornamenti scaricati
Installazione automatica degli aggiornamenti di Kaspersky Endpoint Security nei dispositivi
Modello offline per il download degli aggiornamenti
Abilitazione e disabilitazione del modello offline per il download degli aggiornamenti
Installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center
Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center
Distribuzione automatica degli aggiornamenti
Distribuzione automatica degli aggiornamenti ai dispositivi client
Distribuzione automatica degli aggiornamenti agli Administration Server secondari
Assegnazione automatica di punti di distribuzione
Assegnazione manuale di un punto di distribuzione a un dispositivo
Rimozione di un dispositivo dall'elenco dei punti di distribuzione
Download degli aggiornamenti tramite punti di distribuzione

Eliminazione di aggiornamenti software dall'archivio
Installazione patch per un'applicazione Kaspersky in modalità cluster
Gestione delle applicazioni di terzi nei dispositivi client
Informazioni sulle applicazioni di terze parti
Installazione degli aggiornamenti software di terze parti
Scenario: Aggiornamento di software di terze parti
Visualizzazione delle informazioni sugli aggiornamenti disponibili per le applicazioni di terze parti
Approvazione e rifiuto degli aggiornamenti software
Sincronizzazione degli aggiornamenti da Windows Update con Administration Server
Passaggio 1. Stabilire se ridurre o meno il traffico
Passaggio 2. Applicazioni
Passaggio 3. Categorie di aggiornamenti
Passaggio 4. Lingue degli aggiornamenti
Passaggio 5. Selezione dell'account per l'avvio dell'attività
Passaggio 6. Configurazione di una pianificazione di avvio delle attività
Passaggio 7. Definizione del nome dell'attività
Passaggio 8. Completamento della creazione dell'attività
Installazione manuale degli aggiornamenti nei dispositivi
Configurazione degli aggiornamenti di Windows in un criterio di Network Agent
Correzione delle vulnerabilità del software di terze parti
Scenario: Individuazione e correzione delle vulnerabilità del software di terze parti
Informazioni sulla ricerca e la correzione delle vulnerabilità del software
Visualizzazione delle informazioni sulle vulnerabilità del software
Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti
Scansione delle applicazioni per rilevare la presenza di vulnerabilità
Correzione delle vulnerabilità delle applicazioni
Correzione delle vulnerabilità in una rete isolata
Scenario: Correzione delle vulnerabilità del software di terze parti in una rete isolata
Informazioni sulla correzione delle vulnerabilità del software di terzi in una rete isolata
Configurazione dell'Administration Server con accesso a Internet per correggere le vulnerabilità in una rete isolata
Configurazione di Administration Server isolati per la correzione delle vulnerabilità in una rete isolata
Trasmissione delle patch e installazione degli aggiornamenti in una rete isolata
Disabilitazione dell'opzione per trasmettere patch e installare aggiornamenti in una rete isolata
Ignorare le vulnerabilità del software
Selezione di correzioni utente per le vulnerabilità del software di terze parti
Regole per l'installazione dell'aggiornamento
Gruppi di applicazioni
Utilizzo di Controllo Applicazioni per gestire i file eseguibili
Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client
Creazione delle categorie di applicazioni per i criteri di Kaspersky Endpoint Security for Windows
Creazione di una categoria di applicazioni con contenuto aggiunto manualmente
Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati
Creazione di una categoria di applicazioni che include i file eseguibili da una cartella specifica
Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni
Configurazione della gestione dell'avvio delle applicazioni nei dispositivi client
Visualizzazione dei risultati dell'analisi statistica delle regole di avvio applicate ai file eseguibili
Visualizzazione del registro delle applicazioni

Modifica dell'ora di inizio dell'inventario software
Informazioni sulla gestione delle chiavi di licenza di applicazioni di terze parti
Creazione di gruppi di applicazioni concesse in licenza
Gestione delle chiavi di licenza per i gruppi di applicazioni concesse in licenza
Inventario dei file eseguibili
Visualizzazione delle informazioni sui file eseguibili
Monitoraggio e generazione dei rapporti
Scenario: monitoraggio e generazione dei rapporti
Monitoraggio dei semafori e degli eventi registrati in Administration Console
Utilizzo di rapporti, statistiche e notifiche
Utilizzo dei rapporti
Creazione di un modello di rapporto
Visualizzazione e modifica delle proprietà dei modelli di rapporto
Formato filtro esteso nei modelli di rapporto
Conversione del filtro nel formato esteso
Configurazione del filtro esteso
Creazione e visualizzazione di un rapporto
Salvataggio di un rapporto
Creazione di un'attività di invio dei rapporti
Passaggio 1. Selezione del tipo di attività
Passaggio 2. Selezione del tipo di rapporto
Passaggio 3. Azioni su un rapporto
Passaggio 4. Selezione dell'account per l'avvio dell'attività
Passaggio 5. Configurazione di una pianificazione attività
Passaggio 6. Definizione del nome dell'attività
Passaggio 7. Completamento della creazione dell'attività
Gestione delle statistiche
Configurazione delle notifiche degli eventi
Creazione di un certificato per un server SMTP
Selezioni eventi
Visualizzazione di una selezione eventi
Personalizzazione di una selezione eventi
Creazione di una selezione eventi
Esportazione di una selezione eventi in un file di testo
Eliminazione di eventi da una selezione
Aggiunta di applicazioni alle esclusioni in base alle richieste utente
Selezioni dispositivi
Visualizzazione di una selezione dispositivi
Configurazione di una selezione dispositivi
Esportazione delle impostazioni di una selezione dispositivi in un file
Creazione di una selezione dispositivi
Creazione di una selezione dispositivi in base a impostazioni importate
Rimozione di dispositivi dai gruppi di amministrazione in una selezione
Monitoraggio dell'installazione e della disinstallazione delle applicazioni
Eventi dei componenti di Kaspersky Security Center
Struttura dei dati della descrizione del tipo di evento
Eventi di Administration Server

Eventi critici di Administration Server
Eventi di errore funzionale di Administration Server
Eventi di avviso di Administration Server
Eventi informativi di Administration Server
Eventi di Network Agent
Eventi di errore funzionale di Network Agent
Eventi di avviso di Network Agent
Eventi informativi di Network Agent
Eventi di Server per dispositivi mobili MDM iOS
Eventi di errore funzionale di Server per dispositivi mobili MDM iOS
Eventi di avviso di Server per dispositivi mobili MDM iOS
Eventi informativi di Server per dispositivi mobili MDM iOS
Blocco degli eventi frequenti
Informazioni sul blocco degli eventi frequenti
Gestione del blocco degli eventi frequenti
Rimozione del blocco degli eventi frequenti
Esportazione di un elenco degli eventi frequenti in un file
Controllo delle modifiche di stato delle macchine virtuali
Monitoraggio dello stato della protezione anti-virus tramite le informazioni del Registro di sistema
Visualizzazione e configurazione delle azioni per i dispositivi inattivi
Disabilitazione degli annunci di Kaspersky
Regolazione di punti di distribuzione e gateway di connessione
Configurazione standard dei punti di distribuzione: singola sede
Configurazione standard dei punti di distribuzione: più sedi remote di piccole dimensioni
Assegnazione di un dispositivo gestito a cui assegnare il ruolo di punto di distribuzione
Collegamento di un dispositivo Linux come gateway nella rete perimetrale
Collegamento di un dispositivo Linux ad Administration Server tramite un gateway di connessione
Aggiunta di un gateway di connessione nella rete perimetrale come punto di distribuzione
Assegnazione automatica di punti di distribuzione
Informazioni sull'installazione locale di Network Agent in un dispositivo selezionato come punto di distribuzione
Informazioni sull'utilizzo di un punto di distribuzione come gateway di connessione
Aggiunta di intervalli IP all'elenco di intervalli sottoposti a polling da un punto di distribuzione
Utilizzo di un punto di distribuzione come server push
Altre operazioni di routine
Gestione degli Administration Server
Creazione di una gerarchia di Administration Server: l'aggiunta un Administration Server secondario
Connessione a un Administration Server e passaggio da un Administration Server all'altro
Diritti di accesso ad Administration Server e ai relativi oggetti
Condizioni per la connessione a un Administration Server tramite Internet
Connessione criptata a un Administration Server
Autenticazione dell'Administration Server quando un dispositivo è connesso
Autenticazione di Administration Server durante la connessione di Administration Console
Configurazione di una lista di indirizzi IP consentiti per la connessione ad Administration Server
Utilizzo dell'utilità klscflag per chiudere la porta 13291
Disconnessione da un Administration Server
Aggiunta di un Administration Server alla struttura della console
Rimozione di un Administration Server dalla struttura della console

- Aggiunta di un Administration Server virtuale alla struttura della console
- Modifica di un account del servizio di Administration Server. Utilità klsrvswch
- Modifica delle credenziali del DBMS
- Modifica della cartella condivisa di Administration Server
- Risoluzione dei problemi relativi ai nodi di Administration Server
- Visualizzazione e modifica delle impostazioni di un Administration Server
  - Regolazione delle impostazioni generali di un Administration Server
  - Impostazioni dell'interfaccia di Administration Console
  - Elaborazione e archiviazione di eventi in Administration Server
  - Visualizzazione del registro delle connessioni all'Administration Server
  - Controllo delle epidemie di virus
  - Limitazione del traffico
  - Configurazione di Server Web
  - Utilizzo di utenti interni
- Backup e ripristino delle impostazioni di Administration Server
  - Utilizzo di uno snapshot del file system per ridurre la durata del backup
  - Un dispositivo con Administration Server è inutilizzabile
  - Le impostazioni di Administration Server o il database sono danneggiati
- Backup e ripristino dei dati di Administration Server
  - Attività Backup dei dati di Administration Server
  - Utilità per il backup e il ripristino dei dati (klbackup)
  - Backup e ripristino dei dati in modalità interattiva
  - Backup e ripristino dei dati in modalità automatica
  - Utilizzo dell'utilità klbackup per cambiare i dispositivi gestiti sotto la gestione di un altro Administration Server
  - Backup e ripristino dei dati di Administration Server quando si utilizza MySQL o MariaDB
  - Ottimizzazione del backup e ripristino dei dati di Administration Server
- Spostamento di Administration Server in un altro dispositivo
- Prevenzione dei conflitti tra più Administration Server

Gestione dei gruppi di amministrazione

- Creazione dei gruppi di amministrazione
- Spostamento di gruppi di amministrazione
- Eliminazione di gruppi di amministrazione
- Creazione automatica di una struttura di gruppi di amministrazione
- Installazione automatica delle applicazioni nei dispositivi di un gruppo di amministrazione

Gestione dei dispositivi client

- Connessione dei dispositivi client ad Administration Server
- Connessione manuale di un dispositivo client ad Administration Server. Utilità Klmover
- Tunneling della connessione tra un dispositivo client e Administration Server
- Connessione remota al desktop di un dispositivo client
  - Connessione ai dispositivi client Windows
  - Connessione ai dispositivi client macOS
- Connessione ai dispositivi tramite Condivisione desktop Windows
- Configurazione del riavvio di un dispositivo client
- Controllo delle azioni in un dispositivo client remoto
- Verifica della connessione tra un dispositivo client e Administration Server
  - Verifica automatica della connessione tra un dispositivo client e Administration Server
  - Verifica manuale della connessione tra un dispositivo client e Administration Server. Utilità Klnagchk

Informazioni sul controllo del tempo di connessione tra un dispositivo e Administration Server
Identificazione dei dispositivi client in Administration Server
Spostamento dei dispositivi in un gruppo di amministrazione
Modifica di Administration Server per i dispositivi client
Spostamento dei dispositivi connessi ad Administration Server tramite gateway di connessione a un altro Administration Server
Cluster e array di server
Accensione, spegnimento e riavvio dei dispositivi client in remoto
Informazioni sull'utilizzo della connessione continua tra un dispositivo gestito e Administration Server
Informazioni sulla sincronizzazione forzata
Informazioni sulla pianificazione di connessione
Invio di messaggi agli utenti dei dispositivi
Gestione di Kaspersky Security for Virtualization
Configurazione del passaggio degli stati del dispositivo
Tagging dei dispositivi e visualizzazione dei tag assegnati
Tagging automatico dei dispositivi
Visualizzazione e configurazione dei tag assegnati a un dispositivo
Diagnostica remota dei dispositivi client. Utilità di diagnostica remota di Kaspersky Security Center
Connessione dell'utilità di diagnostica remota a un dispositivo client
Generazione di un file di dump per un'applicazione
Abilitazione e disabilitazione della traccia, download del file di traccia
Download delle impostazioni delle applicazioni
Download dei registri eventi
Download di più elementi di informazioni diagnostiche
Avvio della diagnostica e download dei risultati
Avvio, arresto e riavvio delle applicazioni
Dispositivi di protezione UEFI
Impostazioni di un dispositivo gestito
Impostazioni generali dei criteri
Impostazioni del criterio di Network Agent
Gestione degli account utente
Utilizzo degli account utente
Aggiunta di un account di un utente interno
Modifica di un account di un utente interno
Modifica del numero di tentativi di immissione della password consentiti
Configurazione del controllo dell'univocità del nome di un utente interno
Aggiunta di un gruppo di protezione
Aggiunta di un utente a un gruppo
Configurazione dei diritti di accesso alle funzionalità dell'applicazione. Controllo dell'accesso basato sui ruoli
Diritti di accesso alle funzionalità dell'applicazione
Ruoli utente predefiniti
Aggiunta di un ruolo utente
Assegnazione di un ruolo a un utente o un gruppo di protezione
Assegnazione delle autorizzazioni a utenti e gruppi
Propagazione dei ruoli utente agli Administration Server secondari
Assegnazione dell'utente come proprietario dispositivo
Invio di messaggi agli utenti

Visualizzazione dell'elenco dei dispositivi mobili dell'utente
Installazione di un certificato per un utente
Visualizzazione dell'elenco dei certificati rilasciati a un utente
Informazioni sull'amministratore del Administration Server virtuale
Installazione remota di sistemi operativi e applicazioni
Creazione di immagini dei sistemi operativi
Installazione di immagini dei sistemi operativi
Configurazione dell'indirizzo del server proxy KSN
Aggiunta di driver per Ambiente preinstallazione di Windows (WinPE)
Aggiunta di driver a un pacchetto di installazione con un'immagine del sistema operativo
Configurazione dell'utilità sysprep.exe
Distribuzione di sistemi operativi nei nuovi dispositivi della rete
Distribuzione di sistemi operativi nei dispositivi client
Creazione di pacchetti di installazione delle applicazioni
Emissione di un certificato per i pacchetti di installazione delle applicazioni
Installazione delle applicazioni nei dispositivi client
Gestione delle revisioni degli oggetti
Informazioni sulle revisioni degli oggetti
Visualizzazione della sezione Cronologia revisioni
Confronto delle revisioni degli oggetti
Impostazione del periodo di archiviazione per le revisioni degli oggetti e le informazioni sugli oggetti eliminati
Visualizzazione di una revisione degli oggetti
Salvataggio di una revisione degli oggetti in un file
Rollback delle modifiche
Aggiunta di una descrizione della revisione
Eliminazione di oggetti
Eliminazione di un oggetto
Visualizzazione delle informazioni sugli oggetti eliminati
Eliminazione definitiva di oggetti dall'elenco degli oggetti eliminati
Mobile Device Management
Scenario: Distribuzione di Mobile Device Management
Informazioni sul criterio di gruppo per la gestione dei dispositivi MDM iOS
Abilitazione di Mobile Device Management
Modifica delle impostazioni per Mobile Device Management
Disabilitazione di Mobile Device Management
Utilizzo dei comandi per i dispositivi mobili
Comandi per Mobile Device Management
Utilizzo di Firebase Cloud Messaging
Invio di comandi
Visualizzazione dello stato dei comandi nel log dei comandi
Utilizzo dei certificati dei dispositivi mobili
Avvio dell'Installazione guidata certificato
Passaggio 1. Selezionare il tipo di certificato
Passaggio 2. Selezione del tipo di dispositivo
Passaggio 3. Selezione di un utente
Passaggio 4. Selezione dell'origine del certificato
Passaggio 5. Assegnazione di un tag al certificato

Passaggio 6. Specificazione delle impostazioni di pubblicazione del certificato
Passaggio 7. Selezione del metodo di notifica all'utente
Passaggio 8. Generazione del certificato
Configurazione delle regole di emissione dei certificati
Integrazione con PKI (Public Key Infrastructure)
Abilitazione del supporto per la delega vincolata Kerberos
Aggiunta dei dispositivi mobili iOS all'elenco dei dispositivi gestiti
Aggiunta dei dispositivi mobili Android all'elenco dei dispositivi gestiti
Gestione dei dispositivi MDM iOS
Firma di un profilo MDM iOS tramite un certificato
Aggiunta di un profilo di configurazione
Installazione di un profilo di configurazione in un dispositivo
Rimozione del profilo di configurazione da un dispositivo
Aggiunta di un nuovo dispositivo tramite la pubblicazione di un collegamento a un profilo
Aggiunta di un nuovo dispositivo tramite l'installazione del profilo da parte dell'amministratore
Aggiunta di un profilo di provisioning
Installazione di un profilo di provisioning in un dispositivo
Rimozione di un profilo di provisioning da un dispositivo
Aggiunta di un'applicazione gestita
Installazione di un'app in un dispositivo mobile
Rimozione di un'app da un dispositivo
Configurazione del roaming in un dispositivo mobile MDM iOS
Visualizzazione delle informazioni su un dispositivo MDM iOS
Disconnessione di un dispositivo MDM iOS dalla gestione
Invio di comandi a un dispositivo
Controllo dello stato di esecuzione dei comandi inviati
Gestione dei dispositivi KES
Creazione di un pacchetto applicazioni mobili per i dispositivi KES
Abilitazione dell'autenticazione basata su certificato dei dispositivi KES
Visualizzazione delle informazioni su un dispositivo KES
Disconnessione di un dispositivo KES dalla gestione
Criptaggio e protezione dei dati
Visualizzazione dell'elenco dei dispositivi criptati
Visualizzazione dell'elenco degli eventi di criptaggio
Esportazione dell'elenco degli eventi di criptaggio in un file di testo
Creazione e visualizzazione di rapporti sul criptaggio
Trasmissione delle chiavi di criptaggio tra Administration Server
Archivi dati
Esportazione di un elenco di oggetti di un archivio in un file di testo
Pacchetti di installazione
Stati principali dei file nell'archivio
Attivazione delle regole in modalità Smart Training
Visualizzazione dell'elenco dei rilevamenti eseguiti tramite Controllo adattivo delle anomalie
Aggiunta di esclusioni dalle regole di Controllo adattivo delle anomalie
Passaggio 1. Selezione dell'applicazione
Passaggio 2. Selezione del criterio (criteri)
Passaggio 3. Elaborazione del criterio (criteri)

Quarantena e Backup
Abilitazione della gestione remota per i file negli archivi
Visualizzazione delle proprietà di un file inserito in un archivio
Eliminazione di file dagli archivi
Ripristino di file dagli archivi
Salvataggio di un file su disco dagli archivi
Scansione dei file in quarantena
Minacce attive
Disinfezione di un file non elaborato
Salvataggio su disco di un file non elaborato
Eliminazione dei file dalla cartella "Minacce attive"
Finestra Kaspersky Security Network (KSN)
Informazioni su KSN
Impostazione dell'accesso a Kaspersky Security Network
Abilitazione e disabilitazione di KSN
Visualizzazione dell'Informativa KSN accettata
Visualizzazione delle statistiche del server proxy KSN
Accettazione di un'Informativa KSN aggiornata
Protezione avanzata con Kaspersky Security Network
Verifica per stabilire se il punto di distribuzione funziona come server proxy KSN
Passaggio dalla Guida in linea alla Guida offline e viceversa
Esportazione di eventi nei sistemi SIEM
Configurazione dell'esportazione di eventi nei sistemi SIEM
Prima di iniziare
Informazioni sugli eventi in Kaspersky Security Center
Informazioni sull'esportazione degli eventi
Informazioni sulla configurazione dell'esportazione di eventi in un sistema SIEM
Contrassegno degli eventi per l'esportazione nei sistemi SIEM in formato Syslog
Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog
Contrassegno di eventi generici per l'esportazione nel formato Syslog
Informazioni sull'esportazione degli eventi utilizzando il formato Syslog
Informazioni sull'esportazione degli eventi tramite i formati CEF e LEEF
Configurazione di Kaspersky Security Center per l'esportazione degli eventi nel sistema SIEM
Esportazione degli eventi direttamente dal database
Esecuzione di una query SQL tramite l'utilità klsql2
Esempio di una query SQL nell'utilità klsql2
Visualizzazione del nome del database di Kaspersky Security Center
Visualizzazione dei risultati dell'esportazione
Utilizzo di SNMP per l'invio di statistiche ad applicazioni di terze parti
Configurazione del servizio SNMP per l'utilizzo con Kaspersky Security Center
Agente SNMP e identificatori oggetto
Ottenere un nome di contatore di stringhe da un identificatore oggetto
Valori degli identificatori oggetto per SNMP
Risoluzione dei problemi
Utilizzo di un ambiente cloud
Informazioni sull'utilizzo di un ambiente cloud
Scenario: Distribuzione per un ambiente cloud

Prerequisiti per la distribuzione di Kaspersky Security Center in un ambiente cloud
Requisiti hardware per Administration Server in un ambiente cloud
Opzioni di licenza in un ambiente cloud
Opzioni del database per l'utilizzo in un ambiente cloud
Utilizzo dell'ambiente cloud Amazon Web Services
Informazioni sull'utilizzo dell'ambiente cloud Amazon Web Services
Creazione di ruoli IAM e account utente IAM per le istanze Amazon EC2
Verifica delle autorizzazioni di Kaspersky Security Center Administration Server per l'utilizzo di AWS
Creazione di un ruolo IAM per l'Administration Server
Creazione di un account utente IAM per l'utilizzo di Kaspersky Security Center
Creazione di un ruolo IAM per l'installazione delle applicazioni nelle istanze Amazon EC2
Utilizzo di Amazon RDS
Creazione di un'istanza Amazon RDS
Creazione di gruppo di opzioni per l'istanza Amazon RDS
Modifica del gruppo di opzioni
Modifica delle autorizzazioni per il ruolo IAM per l'istanza di database Amazon RDS
Preparazione del bucket Amazon S3 per il database
Migrazione del database ad Amazon RDS
Utilizzo dell'ambiente cloud Microsoft Azure
Informazioni sull'utilizzo di Microsoft Azure
Creazione di una sottoscrizione, un ID applicazione e una password
Assegnazione di un ruolo all'ID applicazione Azure
Distribuzione di Administration Server in Microsoft Azure e selezione del database
Utilizzo di Azure SQL
Creazione dell'account di archiviazione Azure
Creazione del database SQL Azure e del server SQL
Migrazione del database ad Azure SQL
Utilizzo in Google Cloud
Creazione di e-mail client, ID progetto e chiave privata
Utilizzo di Google Cloud SQL per l'istanza MySQL
Prerequisiti dei dispositivi client in un ambiente cloud per l'utilizzo di Kaspersky Security Center
Creazione dei pacchetti di installazione necessari per la configurazione dell'ambiente cloud
Configurazione dell'ambiente cloud
Informazioni sulla procedura guidata Configura ambiente cloud
Passaggio 1. Selezione del metodo di attivazione dell'applicazione
Passaggio 2. Selezione dell'ambiente cloud
Passaggio 3. Autorizzazione nell'ambiente cloud
Passaggio 4. Configurazione della sincronizzazione con Cloud e selezione delle azioni successive
Passaggio 5. Configurazione di Kaspersky Security Network nell'ambiente cloud
Passaggio 6. Configurazione delle notifiche e-mail nell'ambiente cloud
Passaggio 7. Creazione di una configurazione iniziale della protezione dell'ambiente cloud
Passaggio 8. Selezione dell'azione nel momento in cui deve essere riavviato il sistema operativo durante l'installazione (per l'ambiente cloud)
Passaggio 9. Ricezione degli aggiornamenti da parte di Administration Server
Controllo della configurazione
Gruppo di dispositivi Cloud
Polling dei segmenti di rete

Aggiunta di connessioni per il polling dei segmenti cloud
Eliminazione di connessioni per il polling dei segmenti cloud
Configurazione della pianificazione di polling
Installazione di applicazioni nei dispositivi in un ambiente cloud
Visualizzazione delle proprietà dei dispositivi cloud
Sincronizzazione con il cloud
Distribuzione di Kaspersky Security Center in Yandex.Cloud
Appendici
Funzioni avanzate
Automazione delle operazioni di Kaspersky Security Center. utilità klakaut
Strumenti personalizzati
Modalità di clonazione del disco di Network Agent
Preparazione di un dispositivo di riferimento in cui è installato Network Agent per la creazione di un'immagine del sistema operativo
Configurazione della ricezione dei messaggi da File Integrity Monitor
Manutenzione di Administration Server
Accesso ai server DNS pubblici
Finestra Metodo di notifica all'utente
Finestra Selezione dispositivi
Finestra Definire il nome del nuovo oggetto
Funzionalità per l'utilizzo dell'interfaccia di gestione
Struttura della console
Come aggiornare i dati nell'area di lavoro
Come spostarsi nella struttura della console
Come aprire le proprietà degli oggetti nell'area di lavoro
Come selezionare un gruppo di oggetti nell'area di lavoro
Come modificare il set di colonne nell'area di lavoro
Informazioni di riferimento
Comandi del menu di scelta rapida
Elenco dei dispositivi gestiti. Descrizione delle colonne
Stati di dispositivi, attività e criteri
Icone di stato dei file in Administration Console
Ricerca ed esportazione dei dati
Ricerca di dispositivi
Impostazioni di ricerca del dispositivo
Utilizzo di maschere nelle variabili stringa
Utilizzo di espressioni regolari nel campo di ricerca
Esportazione di elenchi dalle finestre di dialogo
Impostazioni delle attività
Impostazioni generali delle attività
Impostazioni dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server
Impostazioni dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione
Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti
Impostazioni dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità
Elenco globale delle subnet
Aggiunta di subnet all'elenco globale delle subnet
Visualizzazione e modifica delle proprietà delle subnet nell'elenco globale delle subnet

- Utilizzo di Network Agent per Windows, Linux e macOS a confronto
- Kaspersky Security Center Web Console
  - Diagramma di distribuzione di Kaspersky Security Center Administration Server e Kaspersky Security Center Web Console
  - Porte utilizzate da Kaspersky Security Center Web Console
  - Interfaccia di Kaspersky Security Center Web Console
  - Blocco e sblocco delle sezioni del menu principale
  - Scenario: Installazione e configurazione iniziale di Kaspersky Security Center Web Console
  - Installazione
    - Installazione di Kaspersky Security Center (Installazione standard)
    - Installazione di Kaspersky Security Center Web Console
    - Installazione di Kaspersky Security Center Web Console connesso all'Administration Server installato nei nodi del cluster di failover
    - Upgrade di Kaspersky Security Center Web Console
    - Certificati per l'utilizzo con Kaspersky Security Center Web Console
      - Riemissione del certificato per Kaspersky Security Center Web Console
      - Sostituzione del certificato per Kaspersky Security Center Web Console
      - Specifica dei certificati per gli Administration Server attendibili in Kaspersky Security Center Web Console
      - Conversione di un certificato PFX nel formato PEM
  - Migrazione da Kaspersky Security Center Windows
    - Migrazione a Kaspersky Security Center Cloud Console
    - Migrazione a Kaspersky Next XDR Expert
    - Migrazione a Kaspersky Security Center Linux
      - Migrazione a Kaspersky Security Center Linux utilizzando il backup dei dati di Administration Server
      - Migrazione a Kaspersky Security Center Linux tramite la Migrazione guidata
        - Esportazione di oggetti di gruppo da Kaspersky Security Center Windows
        - Importazione del file di esportazione in Kaspersky Security Center Linux
        - Passaggio dei dispositivi gestiti alla gestione di Kaspersky Security Center Linux
  - Accesso a Kaspersky Security Center Web Console e disconnessione
  - Identity and Access Manager in Kaspersky Security Center Web Console
    - Informazioni su Identity and Access Manager
    - Abilitazione di Identity and Access Manager: scenario
    - Configurazione di Identity and Access Manager in Kaspersky Security Center Web Console
    - Registrazione dell'applicazione Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Web Console
    - Durata dei token e timeout dell'autorizzazione per Identity and Access Manager
    - Download e distribuzione dei certificati IAM
    - Disabilitazione di Identity and Access Manager
  - Configurazione dell'autenticazione del dominio utilizzando i protocolli NTLM e Kerberos
  - Configurazione di Administration Server
    - Configurazione della connessione di Kaspersky Security Center Web Console ad Administration Server
    - Configurazione della registrazione degli eventi di connessione ad Administration Server
    - Configurazione delle impostazioni di accesso a Internet per Administration Server
    - Impostazione del numero massimo di eventi nell'archivio eventi
    - Impostazioni di connessione dei dispositivi di protezione UEFI
    - Creazione di una gerarchia di Administration Server: l'aggiunta un Administration Server secondario
    - Visualizzazione dell'elenco degli Administration Server secondari
    - Eliminazione di una gerarchia di Administration Server

Manutenzione di Administration Server
Configurazione dell'interfaccia
Gestione di Administration Server virtuali
Creazione di un Administration Server virtuale
Abilitazione e disabilitazione di un Administration Server virtuale
Assegnazione di un amministratore per un Administration Server virtuale
Modifica di Administration Server per i dispositivi client
Eliminazione di un Administration Server virtuale
Abilitazione della protezione dell'account dalle modifiche non autorizzate
Backup e ripristino dei dati di Administration Server
Creazione di un'attività di backup dei dati
Spostamento di Administration Server in un altro dispositivo
Controllo dell'integrità dei moduli mediante le utilità klscmodchk e integrity_checker
Configurazione iniziale di Kaspersky Security Center Web Console
Avvio rapido guidato (Kaspersky Security Center Web Console)
Passaggio 1. Definizione delle impostazioni della connessione Internet
Passaggio 2. Download degli aggiornamenti necessari
Passaggio 3. Selezione delle risorse da proteggere
Passaggio 4. Selezione del criptaggio nelle soluzioni
Passaggio 5. Configurazione dell'installazione dei plug-in per le applicazioni gestite
Passaggio 6. Installazione dei plug-in selezionati
Passaggio 7. Download dei pacchetti di distribuzione e creazione dei pacchetti di installazione
Passaggio 8. Configurazione di Kaspersky Security Network
Passaggio 9. Selezione del metodo di attivazione dell'applicazione
Passaggio 10. Definizione delle impostazioni di gestione degli aggiornamenti di terze parti
Passaggio 11. Creazione di una configurazione della protezione di rete di base
Passaggio 12. Configurazione delle notifiche e-mail
Passaggio 13. Esecuzione di un polling della rete
Passaggio 14. Chiusura dell'Avvio rapido guidato
Connessione dei dispositivi fuori sede
Scenario: Connessione dei dispositivi fuori sede tramite un gateway di connessione
Scenario: connessione di dispositivi fuori sede tramite un Administration Server secondario in DMZ
Informazioni sulla connessione dei dispositivi fuori sede
Connessione dei dispositivi desktop esterni ad Administration Server
Informazioni sui profili di connessione per gli utenti fuori sede
Creazione di un profilo di connessione per gli utenti fuori sede
Informazioni sul passaggio di Network Agent ad altri Administration Server
Creazione di una regola per il passaggio di Network Agent in base al percorso di rete
Distribuzione guidata della protezione
Passaggio 1. Avvio della Distribuzione guidata della protezione
Passaggio 2. Selezione del pacchetto di installazione
Passaggio 3. Selezione di un metodo per la distribuzione del file chiave o del codice di attivazione
Passaggio 4. Selezione della versione di Network Agent
Passaggio 5. Selezione dei dispositivi
Passaggio 6. Specificazione delle impostazioni dell'attività di installazione remota
Passaggio 7. Gestione riavvio
Passaggio 8. Rimozione delle applicazioni incompatibili prima dell'installazione

Passaggio 9. Spostamento dei dispositivi in Dispositivi gestiti
Passaggio 10. Selezione degli account per l'accesso ai dispositivi
Passaggio 11. Avvio dell'installazione
Distribuzione delle applicazioni Kaspersky tramite Kaspersky Security Center Web Console
Scenario: Distribuzione delle applicazioni Kaspersky tramite Kaspersky Security Center Web Console
Recupero dei plug-in per le applicazioni Kaspersky
Download e creazione dei pacchetti di installazione per le applicazioni Kaspersky
Modifica del limite relativo alle dimensioni dei dati del pacchetto di installazione personalizzato
Download dei pacchetti di distribuzione per le applicazioni Kaspersky
Controllo della corretta distribuzione di Kaspersky Endpoint Security
Creazione di pacchetti di installazione indipendenti
Visualizzazione dell'elenco dei pacchetti di installazione indipendenti
Creazione di pacchetti di installazione personalizzati
Distribuzione dei pacchetti di installazione agli Administration Server secondari
Installazione delle applicazioni tramite un'attività di installazione remota
Installazione remota di un'applicazione
Installazione di un'applicazione utilizzando i criteri di gruppo di Active Directory
Installazione di applicazioni negli Administration Server secondari
Definizione delle impostazioni per l'installazione remota nei dispositivi Unix
Avvio e arresto delle applicazioni Kaspersky.
Mobile Device Management
Sostituzione di applicazioni di protezione di terzi
Individuazione dei dispositivi nella rete
Scenario: Individuazione dei dispositivi nella rete
Device discovery
Polling della rete Windows
Polling intervallo IP
Aggiunta e modifica di un intervallo IP
Polling zeroconf
Polling del controller di dominio
Autenticazione e connessione a un controller di dominio
Configurazione di un controller di dominio Samba
Configurazione delle regole di conservazione per i dispositivi non assegnati
Inventario dei dispositivi
Aggiunta di informazioni sui nuovi dispositivi
Configurazione dei criteri utilizzati per definire i dispositivi aziendali
Applicazioni Kaspersky: licensing e attivazione
Licensing delle applicazioni gestite
Aggiunta di una chiave di licenza all'archivio dell'Administration Server
Aggiunta di una chiave di licenza di Administration Server
Distribuzione di una chiave di licenza ai dispositivi client
Distribuzione automatica di una chiave di licenza
Visualizzazione delle informazioni sulle chiavi di licenza in uso
Rimozione di una chiave di licenza dall'archivio
Revoca del consenso a un Contratto di licenza con l'utente finale
Rinnovo delle licenze per le applicazioni Kaspersky
Utilizzo di Kaspersky Marketplace per scegliere le soluzioni aziendali Kaspersky

Configurazione della protezione di rete
Scenario: Configurazione della protezione di rete
Informazioni sui metodi di gestione della protezione incentrati sui dispositivi e incentrati sugli utenti
Configurazione e propagazione dei criteri: approccio incentrato sui dispositivi
Configurazione e propagazione dei criteri: approccio incentrato sull'utente
Impostazioni del criterio di Network Agent
Confronto tra le impostazioni dei criteri di Network Agent in base ai sistemi operativi
Abilitazione e disabilitazione della modalità a basso consumo di risorse per Network Agent
Configurazione manuale del criterio di Kaspersky Endpoint Security
Configurazione di Kaspersky Security Network
Controllo dell'elenco delle reti protette dal Firewall
Disabilitazione della scansione delle unità di rete
Esclusione dei dettagli del software dalla memoria di Administration Server
Configurazione dell'accesso all'interfaccia di Kaspersky Endpoint Security for Windows nelle workstation
Salvataggio degli eventi di criteri importanti nel database dell'Administration Server
Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security
Concessione dell'accesso offline al dispositivo esterno bloccato da Controllo Dispositivi
Rimozione di applicazioni o aggiornamenti software in remoto
Attività
Informazioni sulle attività
Informazioni sull'ambito dell'attività
Creazione di un'attività
Avvio manuale di un'attività
Visualizzazione dell'elenco delle attività
Impostazioni generali delle attività
Esportazione di un'attività
Importazione di un'attività
Avvio della Procedura guidata per la modifica della password delle attività
Passaggio 1. Immissione delle credenziali
Passaggio 2. Selezione di un'azione da eseguire
Passaggio 3. Visualizzazione dei risultati
Creazione dell'attività Esegui script da remoto
Installazione remota delle applicazioni nei dispositivi che utilizzano l'attività Esegui script da remoto
Configurazione delle notifiche e del monitoraggio per l'attività Esegui script da remoto
Preparazione di un archivio per l'attività Esegui script da remoto
Creazione di un pacchetto di installazione basato su un file manifesto
Gestione dei dispositivi client
Impostazioni di un dispositivo gestito
Creazione dei gruppi di amministrazione
Aggiunta manuale dei dispositivi a un gruppo di amministrazione
Spostamento manuale dei dispositivi o dei cluster in un gruppo di amministrazione
Creazione delle regole di spostamento dei dispositivi
Copia delle regole di spostamento dei dispositivi
Condizioni di una regola di spostamento dei dispositivi
Informazioni sui cluster e sugli array di server
Proprietà di un cluster o di un array di server
Visualizzazione e configurazione delle azioni per i dispositivi inattivi

Informazioni sugli stati dei dispositivi
Configurazione del passaggio degli stati del dispositivo
Connessione remota al desktop di un dispositivo client
Connessione ai dispositivi tramite Condivisione desktop Windows
Selezioni dispositivi
Visualizzazione dell'elenco dei dispositivi da una selezione di dispositivi
Creazione di una selezione dispositivi
Configurazione di una selezione dispositivi
Esportazione dell'elenco dei dispositivi da una selezione di dispositivi
Rimozione di dispositivi dai gruppi di amministrazione in una selezione
Tag dispositivo
Creazione di un tag dispositivo
Ridenominazione di un tag dispositivo
Eliminazione di un tag dispositivo
Visualizzazione dei dispositivi a cui è assegnato un tag
Visualizzazione dei tag assegnati a un dispositivo
Tagging manuale di un dispositivo
Rimozione di un tag assegnato a un dispositivo
Visualizzazione delle regole per il tagging automatico dei dispositivi
Modifica di una regola per il tagging automatico dei dispositivi
Creazione di una regola per il tagging automatico dei dispositivi
Esecuzione di regole per il tagging automatico dei dispositivi
Eliminazione di una regola per il tagging automatico dei dispositivi
Gestione dei tag del dispositivo tramite l'utilità klscflag
Criteri e profili criterio
Informazioni su criteri e profili criterio
Informazioni su blocco e impostazioni bloccate
Ereditarietà di criteri e profili criterio
Gerarchia dei criteri
Profili criterio in una gerarchia di criteri
Modalità di implementazione delle impostazioni in un dispositivo gestito
Gestione dei criteri
Visualizzazione dell'elenco di criteri
Creazione di un criterio
Modifica di un criterio
Impostazioni generali dei criteri
Abilitazione e disabilitazione di un'opzione di ereditarietà dei criteri
Copia di un criterio
Spostamento di un criterio
Esportazione di un criterio
Importazione di un criterio
Visualizzazione del grafico dello stato di distribuzione dei criteri
Eliminazione di un criterio
Gestione dei profili criterio
Visualizzazione dei profili di un criterio
Modifica della priorità di un profilo criterio
Creazione di un profilo criterio

Modifica di un profilo criterio
Copia di un profilo criterio
Creazione di una regola di attivazione del profilo criterio
Eliminazione di un profilo criterio
Criptaggio e protezione dei dati
Visualizzazione dell'elenco delle unità criptate
Visualizzazione dell'elenco degli eventi di criptaggio
Creazione e visualizzazione di rapporti sul criptaggio
Concedere l'accesso a un'unità criptata in modalità offline
Utenti e ruoli utente
Informazioni sui ruoli utente
Visualizzazione degli account utente e delle sessioni
Configurazione dei diritti di accesso alle funzionalità dell'applicazione. Controllo dell'accesso basato sui ruoli
Diritti di accesso alle funzionalità dell'applicazione
Ruoli utente predefiniti
Assegnazione dei diritti di accesso a oggetti specifici
Assegnazione dei diritti di accesso a utenti e gruppi di protezione
Aggiunta di un account di un utente interno
Creazione di un gruppo di protezione
Modifica di un account di un utente interno
Modifica di un gruppo di protezione
Assegnazione di un ruolo a un utente o un gruppo di protezione
Aggiunta di account utente a un gruppo di protezione interno
Assegnazione di un utente come proprietario dispositivo
Configurazione della verifica in due passaggi per tutti gli utenti
Informazioni sulla verifica in due passaggi
Abilitazione della verifica in due passaggi per il proprio account (Web Console)
Abilitazione della verifica in due passaggi per il proprio account (basata su MMC)
Abilitazione della verifica in due passaggi richiesta per tutti gli utenti (Web Console)
Abilitazione della verifica in due passaggi per tutti gli utenti (basata su MMC)
Disabilitazione della verifica in due passaggi per un account utente (Web Console)
Disabilitazione della verifica in due passaggi per un account utente (basata su MMC)
Disabilitazione della verifica in due passaggi richiesta per tutti gli utenti (Web Console)
Disabilitazione della verifica in due passaggi richiesta per tutti gli utenti (basata su MMC)
Esclusione di account dalla verifica in due passaggi (Web Console)
Esclusione di account dalla verifica in due passaggi (basata su MMC)
Modifica del nome dell'emittente del codice di sicurezza (Web Console)
Modifica del nome dell'emittente del codice di sicurezza (basata su MMC)
Configurazione della verifica in due passaggi per il proprio account (Web Console)
Configurazione della verifica in due passaggi per il proprio account (basata su MMC)
Generazione di una nuova chiave segreta
Impedisci ai nuovi utenti di impostare la verifica in due passaggi per se stessi
Assegnazione di un utente come proprietario dispositivo Linux dopo l'installazione di Network Agent
Eliminazione di un utente o un gruppo di protezione
Modifica della password per un account utente
Creazione di un ruolo utente
Modifica di un ruolo utente

Modifica dell'ambito di un ruolo utente
Eliminazione di un ruolo utente
Associazione dei profili criterio ai ruoli
Propagazione dei ruoli utente agli Administration Server secondari
Modifica della password dell'account
Revoca dei diritti di amministratore locale
Gestione delle revisioni degli oggetti
Rollback di un oggetto a una revisione precedente
Aggiunta di una descrizione della revisione
Visualizzazione e salvataggio della revisione di un criterio
Eliminazione di oggetti
Finestra Kaspersky Security Network (KSN)
Informazioni su KSN
Impostazione dell'accesso a KSN
Abilitazione e disabilitazione dell'utilizzo di KSN
Visualizzazione dell'Informativa KSN accettata
Accettazione di un'Informativa KSN aggiornata
Verifica per stabilire se il punto di distribuzione funziona come server proxy KSN
Scenario: Upgrade di Kaspersky Security Center e delle applicazioni di protezione gestite
Aggiornamento di database e applicazioni Kaspersky
Scenario: Aggiornamento periodico di database e applicazioni Kaspersky
Informazioni sull'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky
Creazione dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server
Verifica degli aggiornamenti scaricati
Creazione dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione
Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center
Installazione automatica degli aggiornamenti per Kaspersky Endpoint Security for Windows
Approvazione e rifiuto degli aggiornamenti software
Aggiornamento di Administration Server
Abilitazione e disabilitazione del modello offline per il download degli aggiornamenti
Aggiornamento dei database e dei moduli software Kaspersky nei dispositivi offline
Backup e ripristino dei plug-in Web
Regolazione di punti di distribuzione e gateway di connessione
Configurazione standard dei punti di distribuzione: singola sede
Configurazione standard dei punti di distribuzione: più sedi remote di piccole dimensioni
Informazioni sull'assegnazione dei punti di distribuzione
Assegnazione automatica di punti di distribuzione
Assegnazione manuale di punti di distribuzione
Modifica dell'elenco dei punti di distribuzione per un gruppo di amministrazione
Sincronizzazione forzata
Abilitazione di un server push
Gestione delle applicazioni di terzi nei dispositivi client
Installazione degli aggiornamenti software di terze parti
Scenario: Aggiornamento di software di terze parti
Installazione degli aggiornamenti software di terze parti
Creazione dell'attività Trova vulnerabilità e aggiornamenti richiesti

Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti
Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità
Aggiunta delle regole per l'installazione dell'aggiornamento
Creazione dell'attività Installa aggiornamenti di Windows Update
Visualizzazione delle informazioni sugli aggiornamenti software di terze parti disponibili
Esportazione dell'elenco degli aggiornamenti software disponibili in un file
Approvazione e rifiuto degli aggiornamenti software di terze parti
Creazione dell'attività Esegui sincronizzazione di Windows Update
Aggiornamento automatico delle applicazioni di terze parti
Correzione delle vulnerabilità del software di terze parti
Scenario: Individuazione e correzione delle vulnerabilità del software di terze parti
Informazioni sulla ricerca e la correzione delle vulnerabilità del software
Correzione delle vulnerabilità del software di terze parti
Creazione dell'attività Correggi vulnerabilità
Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità
Aggiunta delle regole per l'installazione dell'aggiornamento
Selezione di correzioni utente per le vulnerabilità del software di terze parti
Visualizzazione delle informazioni sulle vulnerabilità del software rilevate in tutti i dispositivi gestiti
Visualizzazione delle informazioni sulle vulnerabilità del software rilevate nel dispositivo gestito selezionato
Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti
Esportazione dell'elenco delle vulnerabilità del software in un file
Ignorare le vulnerabilità del software
Gestione delle applicazioni in esecuzione nei dispositivi client
Utilizzo di Controllo Applicazioni per gestire i file eseguibili
Modalità e categorie di Controllo Applicazioni
Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client
Creazione di una categoria di applicazioni con contenuto aggiunto manualmente
Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati
Creazione di una categoria di applicazioni che include i file eseguibili in una cartella selezionata
Visualizzazione dell'elenco delle categorie di applicazioni
Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni
Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows
Recupero e visualizzazione di un elenco delle applicazioni installate nei dispositivi client
Creazione di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky
Visualizzazione e modifica delle impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky
Impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky
Tag applicazione
Creazione di un tag applicazione
Ridenominazione di un tag applicazione
Assegnazione di tag a un'applicazione
Rimozione dei tag assegnati a un'applicazione
Eliminazione di un tag applicazione
Monitoraggio e generazione dei rapporti
Scenario: monitoraggio e generazione dei rapporti
Informazioni sui tipi di monitoraggio e generazione dei rapporti
Dashboard e widget

- Utilizzo del dashboard
- Aggiunta di widget al dashboard
- Occultamento di un widget dal dashboard
- Spostamento di un widget nel dashboard
- Modifica delle dimensioni o dell'aspetto del widget
- Modifica delle impostazioni del widget
- Informazioni sulla modalità Solo dashboard
- Configurazione della modalità Solo dashboard

Rapporti

- Utilizzo dei rapporti
- Creazione di un modello di rapporto
- Visualizzazione e modifica delle proprietà dei modelli di rapporto
- Esportazione di un rapporto in un file
- Generazione e visualizzazione di un rapporto
- Creazione di un'attività di invio dei rapporti
- Eliminazione di modelli di rapporto

Eventi e selezioni di eventi

- Informazioni sugli eventi di Kaspersky Security Center
- Utilizzo di selezioni eventi
- Creazione di una selezione eventi
- Modifica di una selezione eventi
- Visualizzazione di un elenco di una selezione eventi
- Esportazione di una selezione di eventi
- Importazione di una selezione di eventi
- Visualizzazione dei dettagli di un evento
- Esportazione degli eventi in un file
- Visualizzazione della cronologia di un oggetto da un evento
- Eliminazione di eventi
- Eliminazione di selezioni eventi
- Impostazione del periodo di archiviazione per un evento
- Eventi dei componenti di Kaspersky Security Center
  - Struttura dei dati della descrizione del tipo di evento
  - Eventi di Administration Server
    - Eventi critici di Administration Server
    - Eventi di errore funzionale di Administration Server
    - Eventi di avviso di Administration Server
    - Eventi informativi di Administration Server
  - Eventi di Network Agent
    - Eventi di errore funzionale di Network Agent
    - Eventi di avviso di Network Agent
    - Eventi informativi di Network Agent
  - Eventi di Server per dispositivi mobili MDM iOS
    - Eventi di errore funzionale di Server per dispositivi mobili MDM iOS
    - Eventi di avviso di Server per dispositivi mobili MDM iOS
    - Eventi informativi di Server per dispositivi mobili MDM iOS
- Blocco degli eventi frequenti
  - Informazioni sul blocco degli eventi frequenti

Gestione del blocco degli eventi frequenti
Rimozione del blocco degli eventi frequenti
Ricezione di eventi da Kaspersky Security for Microsoft Exchange Servers
Notifiche e stati del dispositivo
Utilizzo delle notifiche
Visualizzazione delle notifiche sullo schermo
Informazioni sugli stati dei dispositivi
Configurazione del passaggio degli stati del dispositivo
Configurazione dell'invio delle notifiche
Notifiche degli eventi visualizzate dall'esecuzione di un file eseguibile
Annunci Kaspersky
Informazioni sugli annunci di Kaspersky
Configurazione delle impostazioni per gli annunci di Kaspersky
Disabilitazione degli annunci di Kaspersky
Visualizzazione delle informazioni sui rilevamenti delle minacce
Cloud Discovery
Abilitazione di Cloud Discovery utilizzando il widget
Aggiunta del widget Cloud Discovery al dashboard
Visualizzazione delle informazioni sull'utilizzo dei servizi cloud
Livello di rischio di un servizio cloud
Blocco dell'accesso ai servizi cloud indesiderati
Registrazione delle attività di Kaspersky Security Center Web Console
Integrazione tra Kaspersky Security Center e altre soluzioni
Stabilire una connessione in background
Esportazione di eventi nei sistemi SIEM
Configurazione dell'esportazione di eventi nei sistemi SIEM
Prima di iniziare
Informazioni sugli eventi in Kaspersky Security Center
Informazioni sull'esportazione degli eventi
Informazioni sulla configurazione dell'esportazione di eventi in un sistema SIEM
Contrassegno degli eventi per l'esportazione nei sistemi SIEM in formato Syslog
Informazioni sul contrassegno degli eventi per l'esportazione nel sistema SIEM in formato Syslog
Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog
Contrassegno di eventi generici per l'esportazione nel formato Syslog
Informazioni sull'esportazione degli eventi tramite i formati CEF e LEEF
Conversione degli eventi nel formato CEF o LEEF
Informazioni sull'esportazione degli eventi utilizzando il formato Syslog
Configurazione di Kaspersky Security Center per l'esportazione degli eventi nel sistema SIEM
Esportazione degli eventi direttamente dal database
Esecuzione di una query SQL tramite l'utilità klsql2
Esempio di una query SQL nell'utilità klsql2
Visualizzazione del nome del database di Kaspersky Security Center
Visualizzazione dei risultati dell'esportazione
Utilizzo di Kaspersky Security Center Web Console in un ambiente cloud
Configurazione dell'ambiente cloud in Kaspersky Security Center Web Console
Passaggio 1. Controllo dei plug-in e dei pacchetti di installazione necessari
Passaggio 2. Informazioni sull'applicazione

Passaggio 3. Selezione dell'ambiente cloud e autorizzazione
Passaggio 4. Polling dei sistemi, configurazione della sincronizzazione con il cloud e selezione delle azioni successive
Passaggio 5. Selezione di un'applicazione per la quale creare criteri e attività
Passaggio 6. Configurazione di Kaspersky Security Network per Kaspersky Security Center
Passaggio 7. Creazione di una configurazione iniziale della protezione
Polling dei segmenti di rete tramite Kaspersky Security Center Web Console
Aggiunta di connessioni per il polling dei segmenti cloud
Eliminazione di una connessione per il polling dei segmenti cloud
Configurazione della pianificazione di polling tramite Kaspersky Security Center Web Console
Visualizzazione dei risultati del polling dei segmenti cloud tramite Kaspersky Security Center Web Console
Visualizzazione delle proprietà dei dispositivi cloud tramite Kaspersky Security Center Web Console
Sincronizzazione con il cloud: configurazione della regola di spostamento
Installazione remota delle applicazioni nelle macchine virtuali Azure
Creazione dell'attività Backup dei dati di Administration Server con l'utilizzo di un DBMS cloud
Diagnostica remota dei dispositivi client
Apertura della finestra di diagnostica remota
Abilitazione e disabilitazione del tracciamento per le applicazioni
Download dei file di traccia di un'applicazione
Eliminazione dei file di traccia
Download delle impostazioni delle applicazioni
Download dei registri eventi
Avvio, arresto, riavvio dell'applicazione
Esecuzione della diagnostica remota di Kaspersky Security Center Network Agent e download dei risultati
Esecuzione di un'applicazione in un dispositivo client
Generazione di un file di dump per un'applicazione
Esecuzione della diagnostica remota in un dispositivo client basato su Linux
Download ed eliminazione dei file da Quarantena e Backup
Download dei file da Quarantena e Backup
Modifica della lingua dell'interfaccia di Kaspersky Security Center Web Console
Guida di riferimento API
Procedure consigliate per i provider di servizi
Pianificazione della distribuzione di Kaspersky Security Center
Concessione dell'accesso via Internet all'Administration Server
Configurazione standard di Kaspersky Security Center
Informazioni sui punti di distribuzione
Gerarchia di Administration Server
Administration Server virtuali
Gestione dei dispositivi mobili con Kaspersky Endpoint Security for Android
Distribuzione e configurazione iniziale
Raccomandazioni sull'installazione di Administration Server
Creazione degli account per i servizi di Administration Server in un cluster di failover
Selezione di un DBMS
Specificazione dell'indirizzo dell'Administration Server
Configurazione della protezione nella rete di un'organizzazione client
Configurazione manuale del criterio di Kaspersky Endpoint Security
Configurazione del criterio nella sezione Protezione minacce avanzata
Configurazione del criterio nella sezione Protezione minacce essenziale

Configurazione del criterio nella sezione Impostazioni generali
Configurazione del criterio nella sezione Configurazione eventi
Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security
Configurazione manuale dell'attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security
Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
Configurazione manuale dell'attività di gruppo per l'installazione degli aggiornamenti e la correzione delle vulnerabilità
Creazione di una struttura di gruppi di amministrazione e assegnazione dei punti di distribuzione
Configurazione del client MSP standard: singola sede
Configurazione del client MSP standard: più sedi remote di piccole dimensioni
Gerarchia di criteri tramite i profili criterio
Gerarchia dei criteri
Profili criterio
Attività
Regole di spostamento dei dispositivi
Classificazione del software
Informazioni sulle applicazioni multi-tenant
Backup e ripristino delle impostazioni di Administration Server
Un dispositivo con Administration Server è inutilizzabile
Le impostazioni di Administration Server o il database sono danneggiati
Distribuzione di Network Agent e dell'applicazione di protezione
Distribuzione iniziale
Configurazione dei programmi di installazione
Pacchetti di installazione
Proprietà e file di trasformazione MSI
Distribuzione con strumenti di terze parti per l'installazione remota delle applicazioni
Informazioni generali sulle attività di installazione remota in Kaspersky Security Center
Distribuzione tramite i criteri di gruppo di Microsoft Windows
Distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center
Esecuzione di pacchetti indipendenti creati tramite Kaspersky Security Center
Opzioni per l'installazione manuale delle applicazioni
Installazione remota delle applicazioni nei dispositivi in cui è installato Network Agent
Gestione dei riavvii dei dispositivi nell'attività di installazione remota
Aggiornamento dei database in un pacchetto di installazione di un'applicazione anti-virus
Rimozione di applicazioni di protezione di terzi non compatibili
Rimozione di Network Agent protetto da password utilizzando il prompt dei comandi
Utilizzo di strumenti per l'installazione remota di applicazioni in Kaspersky Security Center per l'esecuzione di file eseguibili nei dispositivi gestiti
Monitoraggio della distribuzione
Configurazione dei programmi di installazione
Informazioni generali
Installazione in modalità automatica (con un file di risposta)
Installazione di Network Agent in modalità automatica (senza un file di risposta)
Configurazione parziale dell'installazione tramite setup.exe
Parametri di installazione di Administration Server
Impostazioni di installazione di Network Agent
Infrastruttura virtuale
Suggerimenti per la riduzione del carico sulle macchine virtuali

Supporto delle macchine virtuali dinamiche
Supporto della copia delle macchine virtuali
Supporto del rollback del file system per i dispositivi con Network Agent
Informazioni sui profili di connessione per gli utenti fuori sede
Distribuzione della funzionalità Mobile Device Management
Connessione dei dispositivi KES ad Administration Server
Connessione diretta dei dispositivi all'Administration Server
Schema per la connessione dei dispositivi KES al server tramite Kerberos Constrained Delegation (KCD)
Utilizzo di Firebase Cloud Messaging
Integrazione con PKI (Public Key Infrastructure)
Server Web di Kaspersky Security Center
Altre operazioni di routine
Monitoraggio dei semafori e degli eventi registrati in Administration Console
Accesso remoto ai dispositivi gestiti
Utilizzo dell'opzione "Non eseguire la disconnessione da Administration Server" per garantire connettività continua tra un dispositivo gestito e Administration Server
Informazioni sul controllo del tempo di connessione tra un dispositivo e Administration Server
Informazioni sulla sincronizzazione forzata
Informazioni sul tunneling
Guida per il dimensionamento
Informazioni sulla guida
Informazioni sulle limitazioni di Kaspersky Security Center
Calcoli per gli Administration Server
Calcolo delle risorse hardware per Administration Server
Requisiti hardware per il DBMS e l'Administration Server
Calcolo dello spazio del database
Calcolo dello spazio su disco (con e senza l'utilizzo della funzionalità Vulnerability e patch management)
Calcolo del numero e configurazione degli Administration Server
Suggerimenti per la connessione di macchine virtuali dinamiche a Kaspersky Security Center
Calcoli per punti di distribuzione e gateway di connessione
Requisiti per un punto di distribuzione
Calcolo del numero e configurazione dei punti di distribuzione
Calcolo del numero di gateway di connessione
Registrazione delle informazioni sugli eventi per le attività e i criteri
Considerazioni specifiche e impostazioni ottimali di determinate attività
Frequenza della device discovery
Attività di backup dei dati di Administration Server e attività di manutenzione di Administration Server
Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
Attività di inventario
Dettagli del carico di rete trasmesso fra Administration Server e dispositivi protetti
Consumo del traffico in diversi scenari
Utilizzo del traffico medio nell'arco di 24 ore
Contatta Assistenza tecnica
Come ottenere assistenza tecnica
Assistenza tecnica tramite Kaspersky CompanyAccount
Recupero dei file di dump di Administration Server
Fonti di informazioni sull'applicazione

Glossario
- Administration Console
- Administration Server
- Administration Server principale
- Administration Server virtuale
- Agente di Autenticazione
- Aggiorna
- Aggiornamento disponibile
- Amazon Machine Image (AMI)
- Ambiente cloud
- Amministratore client
- Amministratore del provider di servizi
- Amministratore di Kaspersky Security Center
- API (Application Programming Interface) AWS
- Applicazione incompatibile
- Archivio eventi
- Attacco MITM
- Attività
- Attività di gruppo
- Attività locale
- Attività per dispositivi specifici
- Backup dei dati di Administration Server
- Cartella di backup
- Certificato condiviso
- Certificato di Administration Server
- Chiave attiva
- Chiave di accesso AWS IAM
- Chiave di licenza aggiuntiva (o di riserva)
- Client di Administration Server (dispositivo client)
- Cloud Discovery
- Console di gestione AWS
- Criterio
- Database anti-virus
- Diritti di amministratore
- Dispositivi gestiti
- Dispositivo di protezione UEFI
- Dispositivo KES
- Dispositivo MDM iOS
- Dominio di trasmissione
- Epidemia di virus
- File chiave
- Finestra Kaspersky Security Network (KSN)
- Gateway di connessione
- Gestione centralizzata delle applicazioni
- Gestione diretta delle applicazioni
- Gruppo di amministrazione
- Gruppo di applicazioni concesse in licenza

Guida all'hardening

HTTPS

IAM (Identity and Access Management)

Impostazioni attività

Impostazioni del programma

Installazione forzata

Installazione locale

Installazione manuale

Installazione remota

Istanza Amazon EC2

JavaScript

Kaspersky Private Security Network (KPSN)

Kaspersky Security Center System Health Validator (SHV)

Lightweight Nagent (LWNGT)

Livello di criticità di un evento

Livello di importanza patch

Negozio applicazioni

Network Agent

Network Location Awareness (NLA)

Operatore di Kaspersky Security Center

Pacchetto di installazione

Periodo licenza

Plug-in di gestione

Profilo di configurazione

Profilo di provisioning

Profilo MDM iOS

Proprietario dispositivo

Protezione anti-virus della rete

Provider di servizi di protezione anti-virus

Punto di distribuzione

Rete perimetrale (DMZ)

Ripristino

Ripristino dei dati di Administration Server

Ruolo IAM

Server degli aggiornamenti Kaspersky

Server per dispositivi mobili

Server per dispositivi mobili MDM iOS

Server Web di Kaspersky Security Center

Soglia di attività virus

SSL

Stato della protezione della rete

Stato protezione

Upgrade di Kaspersky Security Center

Utente IAM

Utenti interni

Vulnerabilità

Windows Server Update Services (WSUS)

Workstation dell'amministratore
Informazioni sul codice di terze parti
Note relative ai marchi registrati
Problemi noti

Guida di Kaspersky Security Center 15.1

	**Novità** Informazioni sulle novità della versione più recente dell'applicazione.		**Configurazione della protezione di rete** Gestire la protezione dell'organizzazione.
	**Requisiti hardware e software** Controllare i sistemi operativi e le versioni delle applicazioni supportati.		**Applicazioni Kaspersky. Aggiornamento dei database e dei moduli del software** Gestire l'affidabilità del sistema di protezione.
	**Distribuzione e configurazione iniziale** Pianificare l'utilizzo delle risorse, installare l'Administration Server, installare Network Agent e le applicazioni di protezione nei dispositivi client e consolidare i dispositivi in gruppi di amministrazione.		**Monitoraggio e generazione dei rapporti** Visualizzare l'infrastruttura, lo stato della protezione e le statistiche. Gestire l'accesso ai servizi cloud utilizzando Cloud Discovery.
	**Individuazione dei dispositivi nella rete** Individuare i dispositivi nuovi ed esistenti nella rete dell'organizzazione.		**Sostituzione di applicazioni di protezione di terzi** Informazioni sui metodi per la disinstallazione delle applicazioni incompatibili.
	**Applicazioni Kaspersky. Distribuzione centralizzata** Distribuire applicazioni Kaspersky.		**Regolazione di punti di distribuzione e gateway di connessione** Configurare i punti di distribuzione.
	**Upgrade di Kaspersky Security Center da una versione precedente** Upgrade di Kaspersky Security Center 15.1 da una versione precedente.		**Procedure consigliate per i provider di servizi (solo Guida in linea)** Raccomandazioni relative alla distribuzione, alla configurazione e all'utilizzo dell'applicazione e indicazioni per risolvere i problemi più comuni che possono verificarsi durante l'esecuzione dell'applicazione.
	**Applicazioni Kaspersky. Licensing e attivazione** Attivare le applicazioni Kaspersky in pochi passaggi.		**Guida per il dimensionamento (solo Guida in linea)** Per prestazioni ottimali in diverse condizioni, tenere conto del numero di dispositivi in rete, della topologia della rete e del set di funzionalità di Kaspersky Security Center richiesto.
	**Esportazione di eventi nei sistemi SIEM** Configurare l'esportazione degli eventi nei sistemi SIEM per l'analisi.		**Vulnerability e patch management** Individuare e correggere le vulnerabilità del software di terze parti.
	**Utilizzo di un ambiente cloud** Distribuire Kaspersky Security Center in ambienti cloud: Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.		**Domande frequenti (solo in inglese)** Trovare le istruzioni su come risolvere i problemi comuni.
	**Guida introduttiva di Kaspersky Endpoint Security for Business** Introduzione a Kaspersky Endpoint Security for Business: installare e configurare questa soluzione. È anche possibile esaminare il confronto tra le funzionalità di Kaspersky Security Center, per scegliere il modo più appropriato di gestire la sicurezza della rete.		

Novità

Kaspersky Security Center 15.1 Aggiornamento 2

Kaspersky Security Center 15.1 Aggiornamento 2 è incentrato sulla risoluzione dei problemi segnalati dagli utenti e dal team di test:

- Le attività ora vengono eseguite correttamente per l'ambito dei dispositivi gestiti basati su Linux specificati tramite l'importazione di un file TXT.
- Adesso, quando un'applicazione Kaspersky viene installata utilizzando un'attività di installazione remota creata in un Administration Server virtuale, i pacchetti di installazione vengono trasmessi ai dispositivi gestiti utilizzando gli strumenti del sistema operativo solo tramite il punto di distribuzione gestito da tale Administration Server virtuale.
- È stato risolto un problema per cui un Administration Server secondario non riusciva a riconnettersi all'Administration Server primario dopo la rotazione del certificato del server secondario.
- Risolti problemi che interessano le connessioni TLS.
- È stato risolto un problema che causava più errori "Typecast non valido" durante l'accesso dell'utente.
- Kaspersky Security Center ora invia correttamente le notifiche degli eventi tramite e-mail.
- È stato risolto un problema relativo all'aggiunta della cartella *Aggiornamenti* alla copia di backup durante l'upgrade di Kaspersky Security Center dalla versione 14.2 alla versione 15.1.
- La data di scadenza della licenza dell'applicazione Kaspersky ora è visualizzata correttamente in Kaspersky Security Center Web Console.
- I comandi **Localizza dispositivo mobile** e **Recupera cronologia posizioni dispositivo** ora funzionano correttamente.
- È stato risolto un problema per cui i pacchetti di installazione con certificati mobili non venivano eliminati automaticamente un'ora dopo il download o 24 ore dopo essere rimasti inutilizzati.
- Il profilo criterio attivato da un tag specifico ora viene applicato correttamente ai dispositivi le cui descrizioni contengono tale contenitore.
- È stato risolto un problema per cui i messaggi di errore del database PostgreSQL venivano visualizzati nel registro eventi.
- L'esclusione di un account dalla verifica in due passaggi ora funziona correttamente.
- È stato risolto un problema per cui la disconnessione da Kaspersky Security Center Web Console non funzionava correttamente durante l'utilizzo dell'autenticazione del dominio con Identity and Access Manager abilitato.
- A questo punto, durante l'aggiornamento di un plug-in Web di gestione, facendo clic sul collegamento con la versione del plug-in richiesta viene avviato il download.

- Problemi risolti nei rapporti:
  - Quando si crea un'attività di invio per i rapporti sulle minacce e sugli aggiornamenti e si imposta la pianificazione dell'attività su **Mensile**, i rapporti vengono compilati correttamente con i dati.
  - Nel modello *Rapporto sullo stato dei componenti dell'applicazione*, i filtri in base al nome del componente sono stati applicati correttamente.
  - Adesso il *rapporto sulla distribuzione della protezione* può essere filtrato in modo da visualizzare solo i dispositivi in cui non sono installate le applicazioni Kaspersky. Questo aiuta a visualizzare il numero di dispositivi in cui devono essere installate le applicazioni.
- Il widget **Cloud Discovery** viene visualizzato correttamente indipendentemente dal fatto che si disponga del diritto **Execute** nell'area **Funzionalità generali: Funzionalità di base**.
- Prestazioni migliorate delle procedure memorizzate e delle operazioni sui database.
- È stato risolto un problema per cui i certificati scaduti collegati a utenti inesistenti causavano l'arresto del processo di rinnovo per tutti gli utenti.
- Risolti problemi che influivano sulla corretta gestione dei certificati.
- Dopo l'upgrade di Kaspersky Security Center dalla versione 14.2 alla 15.1, il download di un pacchetto di installazione indipendente da un Administration Server virtuale secondario in Administration Console ora funziona correttamente.
- Risolto un problema in Kaspersky Security Center Web Console, in cui quando si abilitava l'utilizzo di Kaspersky Security Network (KSN) nel criterio dell'applicazione Kaspersky, l'accettazione dell'Informativa KSN non era disponibile per le seguenti applicazioni: Kaspersky Endpoint Security for Linux versione 12.2 o precedenti, Kaspersky Industrial CyberSecurity for Linux Nodes versione 1.5 o precedenti, Kaspersky Security for Virtualization Light Agent versione 6.0 e 6.1, Kaspersky Embedded Systems Security for Linux versione 3.3 e Kaspersky Security for Windows Server versione 11.0.1.897.
- È stato risolto un problema per cui un profilo criterio non veniva applicato ai dispositivi basati su Linux inclusi in un gruppo di dominio Active Directory.
- È stato risolto un problema che si verificava durante i tentativi di connessione da diversi Administration Server secondari di secondo livello all'Administration Server primario.

Kaspersky Security Center 15.1

Kaspersky Security Center 15.1 prevede diversi miglioramenti e nuove funzionalità:

- Cloud Discovery. Si tratta di una nuova funzionalità consente di monitorare i tentativi di utilizzo dei servizi cloud nei dispositivi gestiti in cui viene eseguito Windows e di bloccare l'accesso ai servizi cloud considerati indesiderati. Questa funzionalità è disponibile solo in Kaspersky Security Center Web Console.
- Il polling del controller di dominio ora consente di eseguire il polling di un controller di dominio Samba tramite un punto di distribuzione basato su Linux. Sono stati apportati ulteriori miglioramenti per supportare il polling di domini di grandi dimensioni.
- Diagnostica remota ottimizzata dei dispositivi gestiti basati su Linux.
- Inventario hardware esteso dei dispositivi macOS. Network Agent in un dispositivo macOS invia l'indirizzo MAC e il numero di serie del dispositivo ad Administration Server.

- È ora possibile verificare la connessione a un sistema SIEM.
- La lunghezza massima della password per un utente interno è stata aumentata a 256 caratteri.
- Quando si esegue la migrazione da Kaspersky Security Center Windows a Kaspersky Security Center Linux, ora è possibile impostare i dispositivi gestiti in modo che siano sotto la gestione di Kaspersky Security Center Linux ripristinando il certificato e la chiave privata di Administration Server da una copia di backup.
- Quando si esegue lo strumento Cleaner o l'utilità klmover per rimuovere un Network Agent protetto da password, viene richiesto di immettere la password di disinstallazione.
- L'upgrade da Kaspersky Security for Windows Server a Kaspersky Endpoint Security for Windows ora non richiede più il riavvio del dispositivo di destinazione.
- A un utente può essere assegnato il ruolo di proprietario dispositivo durante o dopo l'installazione di Network Agent in un dispositivo client in Linux.
- È ora possibile ricevere un rapporto sull'installazione remota quando si installa il software nei dispositivi gestiti tramite script personalizzati.
- Quando si eseguono diversi script personalizzati in un dispositivo gestito, è possibile impostare la priorità di ciascuno script per definire l'ordine di esecuzione. Gli script verranno eseguiti da quello con la priorità più alta a quello con la priorità più bassa.
- Controllo esteso dei criteri. È ora possibile visualizzare il contenuto della revisione di un criterio e salvare la revisione del criterio in un file. Al momento, queste funzionalità sono disponibili solo per il criterio di Administration Server e per il criterio di Network Agent.
- Miglioramenti dell'esperienza utente, tra cui:
  - Personalizzazione del menu principale bloccando le sezioni di Kaspersky Security Center Web Console per un rapido accesso dalla sezione **Bloccato**.
  - Lavoro ottimizzato con le tabelle. La visualizzazione predefinita di ogni tabella ora contiene le colonne utilizzate più di frequente. Inoltre, ora è possibile selezionare tutti gli elementi nella pagina corrente o nell'intera tabella, nonché ordinare gli elementi nell'intera tabella.
  - Configurazione migliorata per l'invio dei rapporti. È ora possibile specificare fino a 20 indirizzi e-mail a cui inviare il rapporto e la pianificazione dell'invio del rapporto.
- È possibile revocare i diritti di amministratore locale dagli account nei dispositivi gestiti basati su Linux. Ciò fornisce un ulteriore livello di controllo degli account utente. Ad esempio, è possibile revocare i diritti di amministratore locale al termine di un'assegnazione una tantum.
- È possibile modificare la password dell'account locale sui dispositivi gestiti basati su Linux, ad esempio quando un utente dimentica la password dell'account locale o per eseguire una modifica pianificata della password.
- Nella sottosezione **User certificates management**, è possibile specificare quali certificati radice installare. Questi certificati possono essere utilizzati, ad esempio, per verificare l'autenticità di siti Web o server Web.
- Il Rapporto sugli attacchi di rete ora include l'indirizzo MAC e la porta del dispositivo responsabile dell'attacco.
- Una nuova opzione per forzare un utente interno a modificare una password al successivo tentativo di accesso a Kaspersky Security Center Web Console.

- Una licenza commerciale non viene più selezionata quando si esportano gli eventi in un sistema SIEM nei formati CEF o LEEF.
- Quando si esegue la migrazione da un'applicazione Kaspersky a un'altra e l'applicazione corrente è protetta da password, è ora possibile specificare la password di disinstallazione nell'attività di installazione remota.
- Exchange ActiveSync non è più supportato.

Kaspersky Security Center 14.2

Kaspersky Security Center 14.2 prevede diversi miglioramenti e nuove funzionalità:

- È stata rilasciata una nuova Guida all'hardening. Si consiglia vivamente di leggere attentamente la guida e di attenersi ai suggerimenti sulla protezione per configurare Kaspersky Security Center e l'infrastruttura di rete.

  Inoltre, installare l'ultimo aggiornamento per Kaspersky Security Center. Questo aggiornamento include funzionalità di protezione dell'infrastruttura come la verifica in due passaggi degli account utente e altri miglioramenti.
- L'accesso ai server di Kaspersky viene ora verificato automaticamente. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza il DNS pubblico.
- I diritti utente su un Administration Server virtuale sono disponibili per la configurazione in qualsiasi momento, indipendentemente dall'Administration Server primario. Inoltre, è possibile assegnare agli utenti del server primario i diritti per gestire un server virtuale.
- Kaspersky Security Center ora supporta l'utilizzo dei seguenti DBMS:
  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (tutte le edizioni)
  - Postgres Pro 14.x (tutte le edizioni)
  - MariaDB 10.1, 10.4, 10.5
- È possibile utilizzare Kaspersky Security Center Web Console per esportare criteri e attività in un file, e quindi importare i criteri e le attività in Kaspersky Security Center Windows o Kaspersky Security Center Linux.
- L'opzione **Non utilizzare il server proxy** è stata rimossa dalle seguenti attività:
  - *Scarica aggiornamenti nell'archivio dell'Administration Server*
  - *Scarica aggiornamenti negli archivi dei punti di distribuzione*
- Per proteggere i dispositivi client in un ambiente cloud, è possibile distribuire Kaspersky Endpoint Security for Windows anziché Kaspersky Security for Windows Server. Questa funzionalità è disponibile dopo il rilascio di Kaspersky Endpoint Security 12.0 for Windows.
- L'utilizzo delle chiavi di criptaggio è ora limitato dai diritti di accesso per l'area funzionale **Caratteristiche generali**: **Gestione delle chiavi di criptaggio**. Gli utenti di Kaspersky Security Center ora possono esportare le chiavi di criptaggio se dispongono del diritto di **lettura** e possono importare le chiavi di criptaggio se dispongono del diritto di **scrittura**.

Kaspersky Security Center 14

Kaspersky Security Center 14 prevede diversi miglioramenti e nuove funzionalità:

- È possibile installare gli aggiornamenti e correggere le vulnerabilità del software di terzi (escluso il software Microsoft) in una rete isolata. Tali reti includono Administration Server e dispositivi gestiti senza accesso a Internet. Per correggere le vulnerabilità in questo tipo di rete, è necessario scaricare gli aggiornamenti richiesti utilizzando un Administration Server con accesso a Internet, quindi trasmettere le patch agli Administration Server isolati.

- Sono stati aggiunti i profili di connessione per gli utenti fuori sede per i dispositivi macOS. Utilizzando i profili di connessione, è possibile configurare le regole per i Network Agent sui dispositivi macOS per la connessione allo stesso Administration Server o ad Administration Server diversi, a seconda della posizione del dispositivo.

- Network Agent ora può essere installato nei dispositivi in cui viene eseguito Microsoft Windows 10 IoT Enterprise.

- Nel **Rapporto sulle minacce** adesso è possibile filtrare l'elenco delle minacce per visualizzare solo le minacce rilevate dalla sandbox cloud.

- Kaspersky Security Center ora supporta Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 come applicazione gestita.

Kaspersky Security Center Web Console prevede diversi miglioramenti e nuove funzionalità:

- È possibile configurare la modalità Solo dashboard per i dipendenti che non gestiscono la rete ma che desiderano visualizzare le statistiche di protezione della rete in Kaspersky Security Center (ad esempio un Top Manager). Quando per un utente è abilitata questa modalità, viene visualizzato solo un dashboard con un set predefinito di widget. L'utente può quindi monitorare le statistiche specificate nei widget, ad esempio lo stato della protezione di tutti i dispositivi gestiti, il numero di minacce rilevate di recente o l'elenco delle minacce più frequenti nella rete.

- Kaspersky Security Center Web Console ora supporta Kaspersky Security for iOS come applicazione di protezione.

- Nelle proprietà dell'attività, è possibile specificare se si desidera applicare o meno l'attività a sottogruppi e Administration Server secondari (inclusi quelli virtuali).

- Kaspersky Security Center ora supporta Kaspersky Industrial CyberSecurity for Linux Nodes 1.3 come applicazione gestita.

Kaspersky Security Center 13.2

Kaspersky Security Center 13.2 prevede diversi miglioramenti e nuove funzionalità:

- Adesso è possibile installare Administration Server, Administration Console, Kaspersky Security Center 13.2 Web Console e Network Agent nei nuovi sistemi operativi illustrati di seguito (vedere i requisiti software per ulteriori dettagli):
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2 (aggiornamento di ottobre 2021)
  - Windows Server 2022
- È possibile utilizzare MySQL 8.0 come database.
- È possibile distribuire Kaspersky Security Center in un cluster di failover Kaspersky Security Center per garantire l'elevata disponibilità di Kaspersky Security Center.
- Kaspersky Security Center adesso funziona sia con gli indirizzi IPv6 che con gli indirizzi IPv4. Administration Server può eseguire il polling delle reti che hanno dispositivi con indirizzi IPv6.

Kaspersky Security Center 13.2 Web Console prevede diversi miglioramenti e nuove funzionalità:

- Adesso è possibile gestire i dispositivi mobili che eseguono Android tramite Kaspersky Security Center 13.2 Web Console.
- Kaspersky Marketplace è disponibile come nuova sezione del menu: è possibile cercare un'applicazione Kaspersky tramite Kaspersky Security Center 13.2 Web Console.
- Kaspersky Security Center adesso supporta le seguenti applicazioni Kaspersky:
  - Kaspersky Endpoint Detection and Response Optimum 2.0
  - Kaspersky Sandbox 2.0
  - Kaspersky Industrial CyberSecurity for Networks 3.1

Kaspersky Security Center 13.1

Kaspersky Security Center 13.1 prevede diversi miglioramenti e nuove funzionalità:

- L'integrazione con i sistemi SIEM è stata migliorata. Adesso è possibile esportare gli eventi nei sistemi SIEM tramite il canale criptato (TLS). La funzionalità è disponibile per Kaspersky Security Center Web Console e Administration Console basata su MMC.
- Adesso è possibile ricevere patch per Administration Server come pacchetto di distribuzione, che è possibile utilizzare per aggiornamenti futuri alle versioni successive.
- In Kaspersky Security Center 13.1 Web Console è stata aggiunta una nuova sezione, **Avvisi**, per Kaspersky Endpoint Detection and Response Optimum. Sono inoltre stati aggiunti diversi nuovi widget per gestire le minacce rilevate da Kaspersky Endpoint Detection and Response Optimum.

- In Kaspersky Security Center 13.1 Web Console adesso è possibile ricevere notifiche sulle licenze in scadenza per le applicazioni Kaspersky.

- Il tempo di risposta per Kaspersky Security Center 13.1 Web Console è stato ridotto.

Kaspersky Security Center 13

Sono state aggiunte le seguenti funzionalità a Kaspersky Security Center 13 Web Console:

- È stata implementata la verifica in due passaggi. È possibile abilitare la verifica in due passaggi per ridurre il rischio di accesso non autorizzato a Kaspersky Security Center 13 Web Console.

- È stata implementata l'autenticazione del dominio utilizzando i protocolli NTLM e Kerberos (Single Sign-On). La funzionalità Single Sign-On consente a un utente Windows di abilitare l'autenticazione sicura in Kaspersky Security Center 13 Web Console senza dover reinserire la password nella rete aziendale.

- Adesso è possibile configurare un plug-in per il funzionamento con Kaspersky Managed Detection and Response. È possibile utilizzare questa integrazione per visualizzare gli incidenti e gestire le workstation.

- Adesso è possibile specificare le impostazioni per Kaspersky Security Center 13 Web Console nell'installazione guidata di Administration Server.

- Vengono visualizzate le notifiche sulle nuove versioni di aggiornamenti e patch. È possibile installare un aggiornamento subito o successivamente in qualsiasi momento. Adesso è possibile installare le patch per Administration Server tramite Kaspersky Security Center 13 Web Console.

- Quando si utilizzano le tabelle, adesso è possibile specificare l'ordine e la larghezza delle colonne, ordinare i dati e specificare le dimensioni della pagina.

- Adesso è possibile aprire qualsiasi rapporto facendo clic sul nome.

- Kaspersky Security Center 13 Web Console adesso è disponibile in coreano.

- Nel menu **Monitoraggio e generazione dei rapporti** è disponibile la nuova sezione Annunci Kaspersky. Questa sezione consente di rimanere informati fornendo informazioni relative alla versione in uso di Kaspersky Security Center e alle applicazioni gestite installate nei dispositivi gestiti. Kaspersky Security Center aggiorna periodicamente le informazioni in questa sezione rimuovendo gli annunci obsoleti e aggiungendo nuove informazioni. È tuttavia possibile disabilitare gli annunci Kaspersky se lo si desidera.

- È stata implementata un'autenticazione aggiuntiva dopo la modifica delle impostazioni di un account utente. È possibile abilitare la protezione di un account utente dalle modifiche non autorizzate. Se questa opzione è abilitata, la modifica delle impostazioni dell'account utente richiede l'autorizzazione da parte di un utente con diritti di modifica.

Sono state aggiunte le seguenti funzionalità a Kaspersky Security Center 13:

- È stata implementata la verifica in due passaggi. È possibile abilitare la verifica in due passaggi per ridurre il rischio di accesso non autorizzato ad Administration Console. Se questa opzione è abilitata, la modifica delle impostazioni dell'account utente richiede l'autorizzazione dell'utente con i diritti di modifica. Adesso è possibile abilitare o disabilitare la verifica in due passaggi per i dispositivi KES.

- È possibile inviare messaggi ad Administration Server tramite HTTP. Sono ora disponibili una guida di riferimento e una libreria Python per utilizzare OpenAPI di Administration Server.

- È possibile emettere un certificato di riserva da utilizzare nei profili MDM iOS, per garantire il passaggio immediato dei dispositivi iOS gestiti dopo la scadenza del certificato del server per dispositivi mobili MDM iOS.
- La cartella delle applicazioni multi-tenancy non è più visualizzata in Administration Console.

Informazioni su Kaspersky Security Center

Questa sezione contiene informazioni sulla funzione di Kaspersky Security Center, sui relativi componenti e funzionalità principali e sulle modalità di acquisto di Kaspersky Security Center.

Le informazioni fornite nella Guida in linea possono variare rispetto alle informazioni contenute nei documenti dell'applicazione. In tal caso, la Guida in linea viene considerata aggiornata. È possibile accedere alla Guida in linea facendo clic sui collegamenti nell'interfaccia dell'applicazione o facendo clic sul collegamento Guida in linea nei documenti. La Guida in linea può essere aggiornata senza preavviso. Se necessario, è possibile passare dalla Guida in linea alla Guida offline.

Kaspersky Security Center è progettato per l'esecuzione centralizzata delle attività di base di amministrazione e manutenzione nella rete di un'organizzazione. L'applicazione consente all'amministratore di accedere a informazioni dettagliate sul livello di protezione della rete dell'organizzazione e permette di configurare tutti i componenti della protezione utilizzando le applicazioni Kaspersky.

L'applicazione Kaspersky Security Center è destinata agli amministratori di reti aziendali e ai dipendenti responsabili della protezione dei dispositivi in un'ampia gamma di organizzazioni.

Utilizzando Kaspersky Security Center è possibile eseguire quanto segue:

- Creare una gerarchia di Administration Server per gestire la rete dell'organizzazione, nonché le reti di filiali remote o organizzazioni client.

  Un'*organizzazione client* è un'organizzazione la cui protezione anti-virus viene assicurata da un provider di servizi.

- Creare una gerarchia di gruppi di amministrazione per gestire una selezione di dispositivi client come una singola unità.
- Gestire un sistema di protezione anti-virus basato sulle applicazioni Kaspersky.
- Creare immagini dei sistemi operativi e distribuirle nei dispositivi client in rete, nonché eseguire l'installazione remota delle applicazioni Kaspersky e di altri produttori di software.
- Gestire in remoto le applicazioni Kaspersky e di altri produttori installate nei dispositivi client. Installare gli aggiornamenti, individuare e correggere le vulnerabilità.
- Eseguire la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi client, monitorarne l'utilizzo e rinnovare le licenze.
- Ricevere statistiche e rapporti sull'esecuzione delle applicazioni e dei dispositivi.
- Ricevere notifiche relative agli eventi critici durante l'esecuzione delle applicazioni Kaspersky.
- Gestire i dispositivi mobili.
- Gestire il criptaggio delle informazioni archiviate nei dischi rigidi di dispositivi e unità rimovibili e l'accesso degli utenti ai dati criptati.

- Eseguire l'inventario dell'hardware connesso alla rete dell'organizzazione.
- Gestire in modo centralizzato il file spostati in Quarantena o Backup dalle applicazioni di protezione, nonché gestire i file per cui l'elaborazione da parte delle applicazioni di protezione è stata rimandata.

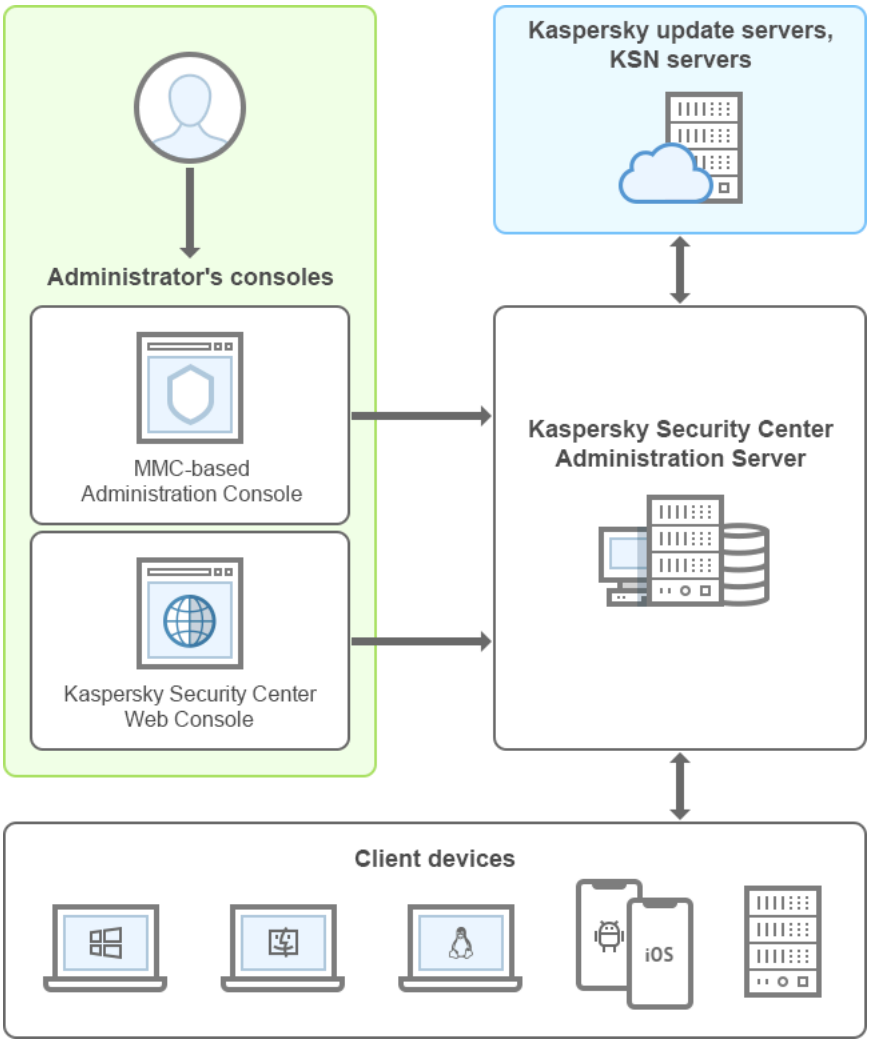
È possibile acquistare Kaspersky Security Center tramite Kaspersky (ad esempio, all'indirizzo https://www.kaspersky.it) o tramite aziende partner.

Se Kaspersky Security Center viene acquistato tramite Kaspersky, è possibile copiare l'applicazione dal nostro sito Web. Le informazioni richieste per l'attivazione dell'applicazione vengono inviate tramite e-mail una volta elaborato il pagamento.

Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Architettura

Questa sezione fornisce una descrizione dei componenti di Kaspersky Security Center e la relativa interazione.



Architettura di Kaspersky Security Center

Kaspersky Security Center include i seguenti componenti di base:

- *Administration Console* (denominato anche *console*). Fornisce un'interfaccia utente per i servizi di amministrazione di Administration Server e Network Agent. Administration Console è implementato come uno snap-in di Microsoft Management Console (MMC). Administration Console consente una connessione remota ad Administration Server via Internet.
- *Kaspersky Security Center Web Console*. Offre un'interfaccia Web per la creazione e la manutenzione del sistema di protezione di una rete di un'organizzazione client gestita tramite Kaspersky Security Center.
- *Kaspersky Security Center Administration Server* (denominato anche *Server*). Centralizza l'archiviazione delle informazioni sulle applicazioni installate nella rete aziendale e sulla relativa gestione.
- *Server di aggiornamento Kaspersky*. I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.
- *Server KSN*. Server che contengono un database Kaspersky con informazioni sempre aggiornate sulla reputazione di file, risorse Web e software. Kaspersky Security Network assicura una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora l'efficacia di alcuni componenti della protezione e riduce la probabilità di falsi positivi.
- *Dispositivi client*. Dispositivi client dell'azienda protetti da Kaspersky Security Center. Ogni dispositivo che deve essere protetto deve avere una delle applicazioni di protezione Kaspersky installate.

Requisiti hardware e software

- Requisiti di Administration Server
- Requisiti di Web Console
- Requisiti dei server mobili
- Requisiti di Administration Console
- Requisiti di Network Agent

Requisiti di Administration Server

Requisiti hardware minimi:

- CPU: con frequenza operativa di 1 GHz o superiore. Per un sistema operativo a 64 bit, la frequenza minima della CPU è di 1.4 GHz.
- RAM: 4 GB.
- Spazio disponibile su disco: 10 GB. Quando si utilizza Vulnerability e patch management, è necessario disporre di almeno 100 GB di spazio disponibile su disco.

Per la distribuzione in ambienti cloud, i requisiti per Administration Server e il server database sono gli stessi di quelli per Administration Server fisico (a seconda del numero di dispositivi che si desidera gestire).

Requisiti software:

- Microsoft® Data Access Components (MDAC) 2.8
- Microsoft Windows® DAC 6.0
- Microsoft Windows Installer 4.5

Sono supportati i seguenti sistemi operativi:

- Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 bit
- Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Installation Option) (LTSB) 64 bit
- Windows Server 2019 Standard/Datacenter/Core 64 bit
- Windows Server 2022 Standard/Datacenter/Core 64 bit
- Windows Server 2025 Standard/Datacenter/Core 64 bit
- Windows Storage Server 2019 64 bit

Sono supportate le seguenti piattaforme di virtualizzazione:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Microsoft Hyper-V Server 2019 64 bit
- Microsoft Hyper-V Server 2022 64 bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x

Sono supportati i seguenti server di database (può essere installato su un dispositivo diverso):

- Microsoft SQL Server 2016 (tutte le edizioni) 64 bit
- Microsoft SQL Server 2017 (tutte le edizioni) in Windows/Linux 64 bit
- Microsoft SQL Server 2019 (tutte le edizioni) in Windows/Linux 64 bit (richiede azioni aggiuntive)
- Microsoft SQL Server 2022 (tutte le edizioni) in Windows/Linux 64 bit
- MySQL 5.7 Community 32 bit/64 bit
- MySQL Standard Edition 8.0 (versione 8.0.20 e successive) 32 bit/64 bit

- MySQL Enterprise Edition 8.0 (versione 8.0.20 e successive) 32 bit/64 bit
- MariaDB 10.5 (build 10.5.27 e versioni successive) 32 bit/64 bit
- Cluster MariaDB Galera 10.3 a 32 bit/64 bit con motore di archiviazione InnoDB
- PostgreSQL 13.x 64 bit
- PostgreSQL 14.x 64 bit
- PostgreSQL 15.x 64 bit
- Postgres Pro 13.x Windows/Linux 64 bit
- Postgres Pro 14.x Windows/Linux 64 bit

Fare riferimento al seguente argomento per dettagli e limitazioni: Selezione di un DBMS.

SIEM e altri sistemi di gestione delle informazioni:

- HP (Micro Focus) ArcSight ESM 7.0
- IBM QRadar 7.3
- Splunk 7.1

Requisiti di Web Console

Kaspersky Security Center Web Console Server

Requisiti hardware minimi:

- CPU: 4 core, frequenza operativa di 2.5 GHz
- RAM: 8 GB
- Spazio disponibile su disco: 40 GB

Requisiti minimi per il certificato di Administration Server:

- Algoritmo della firma del certificato SHA-2
- Lunghezza minima della chiave 2048

Se è necessario riemettere il certificato, fare riferimento alla Knowledge Base di Kaspersky Security Center.

Sistemi operativi. Microsoft Windows (solo versioni a 64 bit)	Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials/Server Core Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Installation Option) (LTSB) Windows Server 2019 Standard/Datacenter/Core Windows Server 2022 Standard/Datacenter/Core Windows Server 2025 Standard/Datacenter/Core Windows Storage Server 2019
Piattaforme di virtualizzazione	VMware vSphere 6.7 VMware vSphere 7.0 VMware vSphere 8.0 Citrix XenServer 7.1 LTSR Citrix XenServer 8.x Parallels Desktop 18 Oracle VM VirtualBox 7.x

Dispositivi client

Per un dispositivo client, l'utilizzo di Kaspersky Security Center Web Console richiede solo un browser.

La risoluzione minima dello schermo è 1366x768 pixel.

I requisiti hardware e software relativi al dispositivo sono identici a quelli del browser utilizzato per Kaspersky Security Center Web Console.

Browser:

- Google Chrome 128.0.6613.120 o versioni successive
- Microsoft Edge 128.0.2739.67 o successiva
- Safari 17.6 su macOS
- "Yandex" Browser 24.7.3.1081 o versione successiva
- Mozilla Firefox Extended Support Release 115.14.0 o versione successiva

Requisiti dei server mobili

Server MDM iOS (Mobile Device Management iOS)

Requisiti hardware:

- CPU: con frequenza operativa di 1 GHz o superiore. Per un sistema operativo a 64 bit, la frequenza minima della CPU è di 1.4 GHz.
- RAM: 2 GB.
- Spazio disponibile su disco: 2 GB.

Requisiti software: Microsoft Windows (la versione del sistema operativo supportato è definita dai requisiti di Administration Server).

Requisiti di Administration Console

Requisiti hardware:

- CPU: con frequenza operativa di 1 GHz o superiore. Per un sistema operativo a 64 bit, la frequenza minima della CPU è di 1.4 GHz.
- RAM: 512 MB.
- Spazio disponibile su disco: 1 GB.

Requisiti software:

- Sistema operativo Microsoft Windows (la versione supportata del sistema operativo è determinata dai requisiti per Administration Server):
  - Windows Server 2012 R2 Standard/Datacenter/Foundation/Essentials 64 bit
  - Windows Server 2016 Standard/Datacenter/Essentials (LTSB) 64 bit
  - Windows Server 2019 Standard/Datacenter 64 bit
  - Windows Server 2022 Standard/Datacenter 64 bit
  - Windows Server 2025 Standard/Datacenter/Core 64 bit
  - Windows Storage Server 2019 64 bit
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 11.0 eseguito in:
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows Storage Server 2019
- Microsoft Edge eseguito in Microsoft Windows Server 2022 Standard

Requisiti di Network Agent

Requisiti hardware minimi:

- CPU: con frequenza operativa di 1 GHz o superiore. Per un sistema operativo a 64 bit, la frequenza minima della CPU è di 1.4 GHz.
- RAM: 512 MB.
- Spazio disponibile su disco: 1 GB.

Requisito software per dispositivi basati su Linux: è necessario installare l'interprete Perl versione 5.10 o successiva.

Sistemi operativi. Microsoft Windows	Windows Embedded POSReady 2009 con il Service Pack più recente 32 bit Windows Embedded 7 Standard con Service Pack 1 32 bit/64 bit Windows Embedded 8.1 Industry Pro 32 bit/64 bit Windows 10 Enterprise 2015 LTSB 32 bit/64 bit Windows 10 Enterprise 2016 LTSB 32 bit/64 bit Windows 10 IoT Enterprise 2015 LTSB 32 bit/64 bit Windows 10 IoT Enterprise 2016 LTSB 32 bit/64 bit Windows 10 Enterprise 2019 LTSC 32 bit/64 bit Windows 10 IoT Enterprise version 1703 32 bit/64 bit Windows 10 IoT Enterprise versione 1709 32 bit/64 bit Windows 10 IoT Enterprise versione 1803 32 bit/64 bit Windows 10 IoT Enterprise versione 1809 32 bit/64 bit Windows 10 20H2 IoT Enterprise 32 bit/64 bit Windows 10 21H2 IoT Enterprise 32 bit/64 bit Windows 10 IoT Enterprise 32 bit/64 bit Windows 10 IoT Enterprise versione 1909 32 bit/64 bit Windows 10 IoT Enterprise LTSC 2021 32 bit/64 bit Windows 10 IoT Enterprise versione 1607 32 bit/64 bit Windows 10 TH1 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 TH2 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 RS1 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 RS2 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 RS3 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 RS4 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 RS5 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 RS6 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 19H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 19H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 20H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 20H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 21H1 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 21H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 10 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 32 bit/64 bit Windows 11 Home/Pro/Pro for Workstations/Enterprise/Education 64 bit Windows 11 22H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 bit Windows 11 23H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 bit Windows 11 24H2 Home/Pro/Pro for Workstations/Enterprise/Education 64 bit Windows 8 Pro/Enterprise 32 bit/64 bit Windows 8.1 Pro/Enterprise 32 bit/64 bit Windows 7 Home/Pro/Enterprise/Ultimate con Service Pack 1 32 bit/64 bit Microsoft Windows XP Professional con Service Pack 2 32 bit/64 bit (supportato solo da Network Agent versione 10.5.1781, che è possibile richiedere tramite l'Assistenza tecnica) Windows XP Professional con Service Pack 3 e versioni successive 32 bit (supportato da Network Agent versione 14.0.0.20023) Windows XP Professional per sistemi integrati con Service Pack 3 32 bit (supportato da Network Agent versione 14.0.0.20023) Windows MultiPoint Server 2011 Standard/Premium 64 bit Windows Server 2003 SP1 32 bit/64 bit (supportato solo da Network Agent versione 10.5.1781) Windows Server 2003 SP2 Standard/Enterprise 32 bit/64 bit (supportato solo da Network Agent versione 10.5.1781) Windows Server 2003 R2 Standard/Enterprise con SP2 32 bit/64 bit (supportato solo da Network Agent versione 10.5.1781) Windows Server 2008 Standard/Enterprise/Datacenter/Foundation con Service Pack 2 32 bit/64 bit Windows Server 2008 R2 Standard/Datacenter/Enterprise/Foundation con Service Pack 1 e versioni successive 64 bit Windows Server 2012 Standard/Datacenter/Essentials/Foundation/Server Core 64 bit Windows Server 2012 R2 Standard/Datacenter/Essentials/Foundation/Server Core 64 bit Windows Server 2016 Standard/Datacenter/Essentials/Server Core (Installation Option) (LTSB) 64 bit

	Windows Server 2019 Standard/Datacenter/Core 64 bit Windows Server 2019 RS5 Standard/Essentials 64 bit Windows Server 2022 Standard/Datacenter/Core 64 bit Windows Server 2022 21H2 Standard/Datacenter 64 bit Windows Server 2025 Standard/Datacenter/Core 64 bit Windows Storage Server 2019 64 bit
Sistemi operativi. Linux	Debian GNU/Linux 10.x (Buster) 32 bit/64 bit Debian GNU/Linux 11.x (Bullseye) 32 bit/64 bit Debian GNU/Linux 12 (Bookworm) 32 bit/64 bit Ubuntu Server 18.04 LTS (Bionic Beaver) 64 bit Ubuntu Server 20.04 LTS (Focal Fossa) 64 bit Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bit Ubuntu Server 22.04 LTS ARM 64 bit Ubuntu Server 24.04 LTS (Noble Numbat) 64 bit CentOS 6.7 e versioni successive 32 bit CentOS 6.x (fino a 6.6) 32 bit/64 bit CentOS 7.x 64 bit CentOS Stream 8 64 bit CentOS Stream 9 64 bit CentOS Stream 9 ARM 64 bit Red Hat Enterprise Linux Server 6.x 32 bit/64 bit Red Hat Enterprise Linux Server 7.x 64 bit Red Hat Enterprise Linux Server 8.x 64 bit Red Hat Enterprise Linux Server 9.x 64 bit SUSE Linux Enterprise Server 12 (tutti i Service Pack) 64 bit SUSE Linux Enterprise Server 15 (tutti i Service Pack) 64 bit SUSE Linux Enterprise Server 15 (tutti i Service Pack) ARM 64 bit openSUSE 15 64 bit EulerOS 2.0 SP10 64 bit EulerOS 2.0 SP10 ARM 64 bit Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.5) 64 bit Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.6) 64 bit Astra Linux Special Edition RUSB.10015-16 (versione 1) (aggiornamento operativo 1.6) 64-bit Astra Linux Special Edition RUSB.10015-17 (aggiornamento operativo 1.7.3) 64 bit Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.7) 64 bit Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.8) 64 bit Astra Linux Special Edition RUSB.10015-37 (aggiornamento operativo 7.7) 64 bit Astra Linux Special Edition RUSB.10152-02 (aggiornamento operativo 4.7) ARM 64 bit Astra Linux Common Edition (aggiornamento operativo 2.12) 64 bit ALT Workstation 10.1 64 bit ALT Server 10.1 64 bit ALT Education 10.1 64 bit ALT SP Server 10 32 bit/64 bit ALT SP Server 10 ARM 64 bit ALT SP Workstation 10 32 bit/64 bit ALT SP Workstation 10 ARM 64 bit ALT Server 10 64 bit ALT Server 10 ARM 64 bit ALT Workstation 10 32 bit/64 bit ALT 8 SP Workstation (8.4) ARM 64 bit ALT 8 SP Server (8.4) ARM 64 bit ALT 8 SP Server (LKNV.11100-01) 32 bit/64 bit ALT 8 SP Server (LKNV.11100-02) 32 bit/64 bit ALT 8 SP Server (LKNV.11100-03) 32 bit/64 bit ALT 8 SP Workstation (LKNV.11100-01) 32 bit/64 bit ALT 8 SP Workstation (LKNV.11100-02) 32 bit/64 bit

	ALT 8 SP Workstation (LKNV.11100-03) 32 bit/64 bit Mageia 4 32 bit Oracle Linux 7 64 bit Oracle Linux 8 64 bit Oracle Linux 9 64 bit Linux Mint 20.x 64 bit Linux Mint 21.1 e versioni successive 64 bit AlterOS 7.5 e versioni successive 64 bit GosLinux IC6/7.17 64 bit GosLinux IC6/7.2 64 bit SberOS 3.3.1 64 bit Platform V SberLinux OS Server (SLO) 8.8 64 bit Platform V SberLinux OS Server (SLO) 8.9.2 64 bit RED OS 7.3 ARM 64 bit RED OS 7.3 Server 64 bit RED OS 7.3 Certified Edition 64 bit RED OS 8 Certified Edition 64 bit ROSA Enterprise Linux Server 7.9 64 bit ROSA Enterprise Linux Desktop 7.9 64 bit ROSA COBALT 7.9 64 bit ROSA CHROME 12 64 bit AlmaLinux 8 e versioni successive 64 bit AlmaLinux 9 e versioni successive 64 bit Rocky Linux 8 e versioni successive 64 bit Rocky Linux 9 e versioni successive 64 bit Atlant, build Alcyone, versione 2022.02 64 bit MSVSPHERE 9.2 SERVER 64 bit MSVSPHERE 9.2 ARM 64 bit SynthesisM Server 8.6 64 bit SynthesisM Client 8.6 64 bit OSnova 2.10 64 bit Kylin 10 64 bit EMIAS 1.0 64 bit Amazon Linux 2 a 64 bit MosOS 15.4 Arbat 64 bit OS MES (Moscow Electronic School) 64 bit
Sistemi operativi. macOS	Per l'elenco dei sistemi operativi supportati, fare riferimento alla Guida di Kaspersky Endpoint Security for Mac.

Per Network Agent è supportata anche l'architettura Apple Silicon (M1), così come Intel.

Sono supportate le seguenti piattaforme di virtualizzazione:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware vSphere 8.0
- Parallels Desktop 18
- Oracle VM VirtualBox 7.x
- Citrix XenServer 7.1 LTSR

- Citrix XenServer 8.x
- Macchina virtuale basata su kernel (tutti i sistemi operativi Linux supportati da Network Agent)

Nei dispositivi che eseguono Windows 10 versione RS4 o RS5, Kaspersky Security Center potrebbe non essere in grado di rilevare alcune vulnerabilità nelle cartelle in cui è abilitata la distinzione tra maiuscole e minuscole.

Prima di installare Network Agent nei dispositivi in cui viene eseguito Windows 7, Windows Server 2008 o Windows Server 2008 R2, assicurarsi di aver installato l'aggiornamento di sicurezza KB3063858 per il sistema operativo Windows (Aggiornamento di sicurezza per Windows 7 (KB3063858), Aggiornamento di sicurezza per Windows 7 per sistemi basati su x64 (KB3063858), Aggiornamento di sicurezza per Windows Server 2008 (KB3063858), Aggiornamento di sicurezza per Windows Server 2008 x64 Edition (KB3063858), Aggiornamento di sicurezza per Windows Server 2008 R2 x64 Edition (KB3063858).

In Microsoft Windows XP Network Agent non potrebbe eseguire correttamente alcune operazioni.

È possibile installare o aggiornare Network Agent for Windows XP solo in Microsoft Windows XP. Le edizioni supportate di Microsoft Windows XP e le versioni corrispondenti di Network Agent sono elencate nell'elenco dei sistemi operativi supportati. È possibile scaricare la versione richiesta di Network Agent per Microsoft Windows XP da questa pagina.

Si consiglia di installare la stessa versione di Network Agent di Kaspersky Security Center.

Kaspersky Security Center supporta Network Agent con versioni uguali o più recenti.

Network Agent per macOS viene fornito insieme all'applicazione di protezione Kaspersky per questo sistema operativo.

Applicazioni e soluzioni Kaspersky compatibili

Kaspersky Security Center supporta la distribuzione e la gestione centralizzate di tutte le applicazioni e soluzioni Kaspersky attualmente supportate. La tabella seguente mostra le applicazioni e soluzioni Kaspersky supportate da Administration Console basata su MMC e Kaspersky Security Center Web Console. Per conoscere le versioni delle applicazioni e delle soluzioni, consultare la pagina Web del ciclo di vita del supporto del prodotto.

Elenco delle soluzioni e delle applicazioni Kaspersky supportate da Kaspersky Security Center

Nome dell'applicazione o della soluzione Kaspersky	Supportato da Administration Console basata su MMC	Supportata da Kaspersky Security Center Web Console
Per workstation		
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓

Nome dell'applicazione o della soluzione Kaspersky	Supportato da Administration Console basata su MMC	Supportata da Kaspersky Security Center Web Console
Kaspersky Endpoint Security for Linux Elbrus Edition	✓	✓
Kaspersky Endpoint Security for Mac	✓	✓
Kaspersky Endpoint Agent	✓	✓
Kaspersky Embedded Systems Security for Windows	✓	✓
Kaspersky Embedded Systems Security for Linux	—	✓
Per soluzioni industriali		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (la distribuzione centralizzata non è supportata)	✓	✓
Per dispositivi mobili		
Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	—	✓
Per file server		
Kaspersky Security for Windows Server	✓	✓
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Per ambienti virtuali		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	—
Per i server di posta e di collaborazione		
Kaspersky Security for Microsoft Exchange Servers	✓	—
Per il rilevamento degli attacchi mirati		
Kaspersky Sandbox Server	—	✓
Kaspersky Endpoint Detection and Response Optimum	—	✓
Kaspersky Managed Detection and Response	—	✓
Per dispositivi KasperskyOS		
Kaspersky IoT Secure Gateway	—	✓
Kaspersky Thin Client	—	✓
Database di reputazione		
Kaspersky Private Security Network	—	✓

Licenze e funzionalità di Kaspersky Security Center 15.1

Kaspersky Security Center richiede una licenza per alcune funzionalità.

La seguente tabella mostra le funzionalità di Kaspersky Security Center incluse nelle varie licenze.

Per abilitare le funzionalità di Kaspersky Security Center, è necessario attivare Administration Server aggiungendo una chiave di licenza di Administration Server.

È necessario aggiungere manualmente una chiave di licenza per ogni Administration Server.

Licenze e funzionalità Kaspersky Security Center

Funzionalità di Kaspersky Security Center	Vulnerability e patch management di Kaspersky	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security for Business	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise	Kaspersky EDR Optimum
Valutazione vulnerabilità	✓	✓	✓	✓	✓	✓	✓
Gestione patch	✓	–	✓	✓	–	✓	✓
Controllo dell'accesso basato sui ruoli	✓	✓	✓	✓	✓	✓	✓
Installazione di sistemi operativi e applicazioni	✓	–	✓	✓	–	✓	✓
Mobile Device Management (gestione dei dispositivi iOS e Android degli utenti)	✓	✓	✓	✓	–	–	✓
Configura ambiente cloud per l'utilizzo in ambienti cloud come AWS, Microsoft Azure o Google Cloud	–	–	–	–	✓	✓	–
Esportazione di eventi nei sistemi SIEM: Syslog	✓	✓	✓	✓	✓	✓	✓
Esportazione di eventi nei sistemi SIEM: QRadar di IBM e ArcSight di Micro Focus	✓	✓	✓	✓	✓	✓	✓

Informazioni sulla compatibilità dei componenti di Kaspersky Security Center

Nella tabella seguente sono disponibili informazioni sulla compatibilità dei componenti di Kaspersky Security Center.

Compatibilità dei componenti di Kaspersky Security Center

Componente	Compatibile con
Kaspersky Security Center 15.1 Administration Server	• Kaspersky Security Center 15.1 Administration Console. • Kaspersky Security Center 15.1 Web Console. • Kaspersky Security Center Network Agent delle seguenti versioni: 16, 15.4, 15.1, 15, 14.2, 14.
Kaspersky Security Center 15.1 Web Console	Kaspersky Security Center Administration Server delle seguenti versioni: 15.1 e 14.2.
Kaspersky Security Center 15.1 Primary Administration Server	Administration Server secondari: • Kaspersky Security Center 14 Windows. • Kaspersky Security Center 14.2 Windows. • Kaspersky Security Center 15.1 Windows. • Kaspersky Security Center 14.2 Linux. • Kaspersky Security Center 15 Linux. • Kaspersky Security Center 15.1 Linux.
Administration Server secondario di Kaspersky Security Center 15.1	Administration Server primari: • Kaspersky Security Center 14 Windows. • Kaspersky Security Center 14.2 Windows. • Kaspersky Security Center 15.1 Windows. • Kaspersky Security Center 14.2 Linux. • Kaspersky Security Center 15 Linux. • Kaspersky Security Center 15.1 Linux.

Si consiglia di utilizzare la versione più recente sia di Kaspersky Security Center Administration Server che di Kaspersky Security Center Web Console. In caso contrario, la funzionalità di Kaspersky Security Center potrebbe essere limitata. È possibile installare e aggiornare Kaspersky Security Center Administration Server e Kaspersky Security Center Web Console in modo indipendente. In questo caso, è necessario assicurarsi che la versione installata di Kaspersky Security Center Web Console sia compatibile con la versione di Administration Server a cui ci si connette:

Se si dispone della versione più recente di Kaspersky Security Center Web Console e della versione precedente di Kaspersky Security Center e si verifica un errore durante l'autenticazione del dominio, il testo dell'errore conterrà un messaggio predefinito.

Confronto tra Kaspersky Security Center basato su Windows e basato su Linux

Kaspersky fornisce Kaspersky Security Center come soluzione locale per due piattaforme: Windows e Linux. Nella soluzione basata su Windows, Administration Server è installato in un dispositivo Windows. Nella soluzione basata su Linux, la versione di Administration Server è invece progettata per l'installazione in un dispositivo Linux. Questa Guida in linea contiene informazioni su Kaspersky Security Center Windows. Per informazioni dettagliate sulla soluzione basata su Linux, fare riferimento alla Guida in linea di Kaspersky Security Center Linux.

La seguente tabella consente di confrontare le caratteristiche principali di Kaspersky Security Center come soluzione basata su Windows e come soluzione basata su Linux.

Confronto delle funzionalità di Kaspersky Security Center come soluzione basata su Windows e soluzione basata su Linux

Funzionalità o proprietà	Kaspersky Security Center	
	Soluzione basata su Windows	Soluzione basata su Linux
Administration Server		
Posizione del DBMS (Database Management System)	In locale	In locale (Microsoft SQL non è supportato)
Sistema operativo in cui installare Administration Server	Windows	Linux
Gerarchia di Administration Server	✓	✓
Supporto per Administration Server virtuali	✓	✓
Utilizzo di SNMP per l'invio delle statistiche di Administration Server ad applicazioni di terzi	✓	Da implementare nel 2026
Server Web per la pubblicazione di pacchetti di installazione e altri file	✓	✓
Installazione di Administration Server in un cluster di failover di Windows Server	✓	—
Administration Console		
Tipo di Administration Console	Basato su MMC e basato sul Web	Basata sul Web
Sistema operativo in cui installare l'Administration Console basata sul Web	Windows o Linux	Linux
Accesso alla console utilizzando l'autenticazione del dominio	✓	✓ Single Sign-On non è supportato per le versioni 15.1-15.4 incluse
Gestione dei dispositivi client e dei gruppi di amministrazione		
Numero massimo di dispositivi gestiti (per un Administration Server)	100.000	50.000 (con PostgreSQL e Postgres Pro)
Polling della rete	✓	✓ A partire dalla versione 16, sono supportati il controller di dominio FreeIPA e ALD Pro
Protezione dei dispositivi gestiti Windows, macOS e Linux	✓	✓
Protezione dei dispositivi mobili	✓ Gestione di base dei dispositivi mobili	✓ MDM e utilizzo della funzionalità Kaspersky Secure Mobility Management (su licenza)
Gestione della protezione delle macchine virtuali	✓	✓
Protezione dell'infrastruttura cloud pubblica	✓	—
Connessione remota al desktop di un dispositivo client	✓	✓ A partire dalla versione 15.3
Criptaggio e protezione dei dati	✓	✓ Nei dispositivi gestiti basati su Windows con Kaspersky Endpoint Security for Windows o Kaspersky Endpoint Security for Mac installato
Distribuzione del cluster di failover Kaspersky Security Center	✓	✓
Supporto di cluster e array di server nei gruppi di amministrazione	✓	✓
Gerarchia di gruppi di amministrazione	✓	✓
Aggiunta di un gateway di connessione nella rete perimetrale come punto di distribuzione	✓ (Administration Console basata su MMC)	Da implementare nel 2026
Utilizzo degli utenti		
Creazione e gestione degli account utente	✓	✓

Funzionalità o proprietà	Kaspersky Security Center	
	Soluzione basata su Windows	Soluzione basata su Linux
Gestione delle applicazioni Kaspersky		
Criteri dell'applicazione	✓	✓
Attività per le applicazioni Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Proxy KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky	✓	✓
Diagnostica remota dei dispositivi client	✓	✓
Aggiornamento automatico delle applicazioni Kaspersky	✓	✓
Supporto di Controllo adattivo delle anomalie	✓	✓
Gestione della sicurezza incentrata sul dispositivo	✓	✓
Gestione della sicurezza incentrata sull'utente	✓	✓
Gestione dei sistemi		
Distribuzione di sistemi operativi nei dispositivi client	✓	—
Gestione di licenze di terzi	✓	—
Utilizzo di Administration Server come server WSUS	✓	✓ (Solo modalità di ricerca di Windows Update passiva)
Gestione delle applicazioni di terzi nei dispositivi client		
Installazione di aggiornamenti software di terze parti e correzione delle vulnerabilità del software di terze parti	✓	✓
Monitoraggio, generazione di rapporti e audit		
Gestione delle revisioni degli oggetti	✓	✓
Confronto tra le revisioni dei criteri	✓	Da implementare nel 2026
Visualizzazione e utilizzo degli avvisi rilevati da Kaspersky Endpoint Detection and Response Optimum	✓	✓
Notifiche sugli eventi che si sono verificati nei dispositivi gestiti	✓	✓
Monitoraggio dello stato dei criteri e dello stato delle attività	✓	✓
Integrazioni		
Integrazione con Kaspersky Managed Detection and Response	✓	✓
Integrazione con i sistemi SIEM	✓	✓ Utilizzando solo Syslog
Esportazione degli eventi tramite i formati CEF e LEEF	✓	Da implementare nel 2026

Informazioni di Kaspersky Security Center Cloud Console

Se utilizzato come applicazione locale, Kaspersky Security Center (comprensivo di Administration Server) viene installato in un dispositivo locale e il sistema di sicurezza di rete viene gestito tramite Administration Console basata su Microsoft Management Console (disponibile solo in Kaspersky Security Center Windows) o Kaspersky Security Center Web Console.

In alternativa, è tuttavia possibile utilizzare Kaspersky Security Center come servizio cloud. In questo caso Kaspersky Security Center viene automaticamente installato e gestito dagli esperti Kaspersky nell'ambiente cloud e Kaspersky fornisce l'accesso ad Administration Server come servizio. Il sistema di sicurezza di rete viene gestito tramite Administration Console basata su cloud, denominata Kaspersky Security Center Cloud Console. Questa console ha un'interfaccia simile all'interfaccia di Kaspersky Security Center Web Console.

L'interfaccia e la documentazione di Kaspersky Security Center Cloud Console sono disponibili nelle seguenti lingue:

- Inglese
- Francese
- Tedesco
- Italiano
- Giapponese
- Portoghese (Brasile)
- Russo
- Cinese semplificato
- Spagnolo
- Spagnolo (LATAM)
- Cinese tradizionale

Ulteriori informazioni su Kaspersky Security Center Cloud Console e sulle relative funzionalità sono disponibili nella documentazione di Kaspersky Security Center Cloud Console e nella documentazione di Kaspersky Endpoint Security for Business.

Kaspersky Security Center 15.1

Questa sezione fornisce informazioni sull'utilizzo di Kaspersky Security Center 15.1.

Le informazioni fornite nella Guida in linea possono variare rispetto alle informazioni contenute nei documenti dell'applicazione. In tal caso, la Guida in linea viene considerata aggiornata. È possibile accedere alla Guida in linea facendo clic sui collegamenti nell'interfaccia dell'applicazione o facendo clic sul collegamento Guida in linea nei documenti. La Guida in linea può essere aggiornata senza preavviso. Se necessario, è possibile passare dalla Guida in linea alla Guida offline.

Concetti di base

In questa sezione sono illustrati i concetti di base relativi a Kaspersky Security Center.

Administration Server

I componenti di Kaspersky Security Center consentono la gestione remota delle applicazioni Kaspersky installate nei dispositivi client.

I dispositivi in cui è installato il componente Administration Server sono denominati *Administration Server* (o semplicemente *server*). Gli Administration Server devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Administration Server viene installato nei dispositivi come un servizio con il seguente set di attributi:

- Con il nome "Kaspersky Security Center Administration Server"
- Impostato per l'avvio automatico all'avvio del sistema operativo
- Con l'account **LocalSystem** o l'account utente selezionato durante l'installazione di Administration Server

Administration Server esegue le seguenti funzioni:

- Memorizzazione della struttura dei gruppi di amministrazione
- Archiviazione di informazioni sulla configurazione dei dispositivi client
- Organizzazione degli archivi per i pacchetti di distribuzione dell'applicazione
- Installazione remota delle applicazioni nei dispositivi client e rimozione delle applicazioni
- Aggiornamento dei database e dei moduli software delle applicazioni Kaspersky
- Gestione di criteri e attività nei dispositivi client
- Archiviazione di informazioni sugli eventi che si sono verificati nei dispositivi client

- Generazione di rapporti sull'esecuzione delle applicazioni Kaspersky
- Distribuzione delle chiavi di licenza ai dispositivi client e archiviazione delle informazioni sulle chiavi di licenza
- Invio di notifiche sullo stato di avanzamento delle attività (ad esempio, il rilevamento di virus in un dispositivo client)

Denominazione degli Administration Server nell'interfaccia dell'applicazione

Nell'interfaccia di Administration Console basata su MMC e di Kaspersky Security Center Web Console gli Administration Server possono avere i seguenti nomi:

- Nome del dispositivo Administration Server, ad esempio: "*nome_dispositivo*" o "Administration Server: *nome_dispositivo*".
- Indirizzo IP del dispositivo Administration Server, ad esempio: "*Indirizzo_IP*" o "Administration Server: *Indirizzo_IP*".
- Gli Administration Server secondari e gli Administration Server virtuali hanno nomi personalizzati da specificare quando si connette un Administration Server virtuale o secondario all'Administration Server primario.
- Se si utilizza Kaspersky Security Center Web Console installata in un dispositivo Linux, l'applicazione visualizza i nomi degli Administration Server specificati come attendibili nel file di risposta.

È possibile connettersi ad Administration Server tramite Administration Console o Kaspersky Security Center Web Console.

Gerarchia di Administration Server

Gli Administration Server possono essere organizzati in una gerarchia. Ogni Administration Server può disporre di diversi Administration Server secondari (denominati *server secondari*) a diversi livelli di nidificazione della gerarchia. Non vi sono limiti per il livello di nidificazione dei server secondari. I gruppi di amministrazione dell'Administration Server primario includeranno i dispositivi client di tutti gli Administration Server secondari. In tal modo, è possibile gestire sezioni isolate e indipendenti di reti tramite differenti Administration Server che vengono a loro volta gestiti dal server primario.

Gli *Administration Server virtuali* sono casi particolari di Administration Server secondari.

La gerarchia degli Administration Server può essere utilizzata per le seguenti operazioni:

- Ridurre il carico su Administration Server (rispetto all'utilizzo di un singolo Administration Server installato per un'intera rete).
- Ridurre il traffico nella rete Intranet e semplificare il lavoro con le filiali remote. Non è necessario stabilire connessioni tra l'Administration Server primario e tutti i dispositivi della rete, che possono ad esempio essere collocati in altre aree geografiche. È sufficiente installare un Administration Server secondario in ogni segmento della rete, distribuire i dispositivi tra i gruppi di amministrazione dei server secondari e stabilire connessioni tra i server secondari e il server primario tramite canali di comunicazione ad alta velocità.

- Distribuire le responsabilità tra gli amministratori della protezione anti-virus. Tutte le capacità di monitoraggio e gestione centralizzati dello stato della protezione anti-virus nelle reti aziendali rimangono disponibili.

- Utilizzare Kaspersky Security Center dai provider di servizi. Un provider di servizi deve installare soltanto Kaspersky Security Center e Kaspersky Security Center Web Console. Per gestire numerosi dispositivi client di varie organizzazioni, un provider di servizi può aggiungere Administration Server secondari (inclusi i server virtuali) a una gerarchia di Administration Server.

Ogni dispositivo incluso nella gerarchia dei gruppi di amministrazione può essere connesso a un unico Administration Server. È necessario monitorare in modo indipendente la connessione dei dispositivi agli Administration Server. Utilizzare la funzionalità per la ricerca di dispositivi nei gruppi di amministrazione di differenti server in base agli attributi di rete.

Administration Server virtuale

Un Administration Server virtuale (denominato anche *server virtuale*) è un componente di Kaspersky Security Center progettato per la gestione della protezione anti-virus della rete di un'organizzazione client.

Un Administration Server virtuale è un particolare tipo di Administration Server secondario e presenta le seguenti limitazioni rispetto a un Administration Server fisico:

- Un Administration Server virtuale può essere creato solo in un Administration Server primario.

- L'Administration Server virtuale utilizza il database dell'Administration Server primario durante il relativo funzionamento. Le attività di backup e ripristino dei dati, nonché le attività di scansione e download degli aggiornamenti, non sono supportate in un Administration Server virtuale.

- Un server virtuale non supporta la creazione di Administration Server secondari (inclusi server virtuali).

L'Administration Server virtuale presenta inoltre le seguenti restrizioni:

- Nella finestra delle proprietà di Administration Server virtuale il numero delle sezioni è limitato.

- Per eseguire l'installazione delle applicazioni Kaspersky in remoto nei dispositivi client gestiti dall'Administration Server virtuale, è necessario verificare che Network Agent sia installato in uno dei dispositivi client per assicurare la comunicazione con l'Administration Server virtuale. Alla prima connessione con l'Administration Server virtuale, il dispositivo verrà automaticamente designato come punto di distribuzione e opererà come un gateway di connessione tra i dispositivi client e l'Administration Server virtuale.

- Un server virtuale può eseguire il polling della rete solo tramite i punti di distribuzione.

- Per riavviare un server virtuale che presenta un malfunzionamento, Kaspersky Security Center riavvia l'Administration Server primario e tutti gli Administration Server virtuali.

- Agli utenti creati in un server virtuale non può essere assegnato un ruolo in Administration Server.

L'amministratore di un Administration Server virtuale dispone di tutti i privilegi per lo specifico server virtuale.

Server per dispositivi mobili

Server per dispositivi mobili è un componente di Kaspersky Security Center che fornisce l'accesso ai dispositivi mobili e consente di gestirli tramite Administration Console. Il server per dispositivi mobili riceve informazioni sui dispositivi mobili e archivia i relativi profili.

Kaspersky Security Center include iOS MDM Server come Mobile Device Server o server per dispositivi mobili. Questo server per dispositivi mobili viene utilizzato per la gestione dei dispositivi mobili che supportano il servizio Apple® Push Notification (APNs).

I server per dispositivi mobili di Kaspersky Security Center consentono di gestire i seguenti oggetti:

- Un singolo dispositivo mobile.
- Più dispositivi mobili.
- Più dispositivi mobili connessi a un cluster di server simultaneamente. Dopo la connessione a un cluster di server, il server per dispositivi mobili installato in questo cluster viene visualizzato in Administration Console come un singolo server.

Server Web

Il *server Web* di Kaspersky Security Center (di seguito denominato anche *server Web*) è un componente di Kaspersky Security Center installato insieme ad Administration Server. Il server Web è progettato per la trasmissione tramite una rete di pacchetti di installazione indipendenti, profili MDM iOS e file da una cartella condivisa.

Quando si crea un pacchetto di installazione indipendente, questo viene automaticamente pubblicato nel server Web. Il collegamento per il download del pacchetto indipendente viene visualizzato nell'elenco dei pacchetti di installazione indipendenti creati. Se necessario, è possibile annullare la pubblicazione del pacchetto indipendente o pubblicarlo nuovamente sul server Web.

Quando si crea un profilo MDM iOS per il dispositivo mobile dell'utente, anche questo viene pubblicato automaticamente nel server Web. Il profilo pubblicato viene automaticamente eliminato dal server Web subito dopo l'installazione nel dispositivo mobile dell'utente.

La cartella condivisa è progettata come un'area di archiviazione per le informazioni disponibile per tutti gli utenti dei dispositivi gestiti tramite Administration Server. Se un utente non ha accesso diretto alla cartella condivisa, è possibile fornirgli le informazioni contenute nella cartella utilizzando il server Web.

Per fornire agli utenti le informazioni nella cartella condivisa utilizzando il server Web, l'amministratore deve creare una sottocartella denominata public nella cartella condivisa e incollare le informazioni in tale sottocartella.

La sintassi del collegamento per il trasferimento delle informazioni è la seguente:

```
https://<nome server Web>:<porta HTTPS>/public/<oggetto>
```

dove:

- `<Web Server name>` è il nome del server Web di Kaspersky Security Center.
- `<HTTPS port>` è una porta HTTPS del server Web definita dall'amministratore. La porta HTTPS può essere impostata nella sezione **Server Web** della finestra delle proprietà di Administration Server. Il numero di porta predefinito è 8061.
- `<object>` è la sottocartella o il file reso accessibile all'utente.

L'amministratore può inviare il nuovo collegamento all'utente con qualsiasi sistema (ad esempio, tramite e-mail).

Utilizzando questo collegamento, l'utente può scaricare le informazioni richieste in un dispositivo locale.

Network Agent

L'interazione tra Administration Server e i dispositivi viene eseguita dal componente *Network Agent* di Kaspersky Security Center. Network Agent deve essere installato in tutti i dispositivi in cui viene utilizzato Kaspersky Security Center per gestire applicazioni Kaspersky.

Network Agent viene installato nei dispositivi come un servizio con il seguente set di attributi:

- Con il nome "Kaspersky Security Center Network Agent"
- Impostato per l'avvio automatico all'avvio del sistema operativo
- Utilizzo dell'account LocalSystem

Un dispositivo con Network Agent installato è denominato *dispositivo gestito* o *dispositivo*.

È possibile installare Network Agent in un dispositivo Windows, Linux o Mac. È possibile ottenere il componente da una delle seguenti origini:

- Pacchetto di installazione nell'archivio dell'Administration Server (è necessario avere installato Administration Server)
- Pacchetto di installazione collocato nei server Web Kaspersky

Non è necessario installare Network Agent nel dispositivo in cui è installato Administration Server, perché la versione server di Network Agent viene installata automaticamente insieme ad Administration Server.

Il nome del processo avviato da Network Agent è *klnagent.exe*.

Network Agent sincronizza il dispositivo gestito con Administration Server. È consigliabile impostare l'intervallo di sincronizzazione (anche denominato *heartbeat*) su 15 minuti per 10.000 dispositivi gestiti.

Gruppi di amministrazione

Un *gruppo di amministrazione* (di seguito denominato anche *gruppo*) è un set logico di dispositivi gestiti combinati in base a una specifica caratteristica allo scopo di gestire i dispositivi raggruppati come una singola unità in Kaspersky Security Center.

Tutti i dispositivi gestiti all'interno di un gruppo di amministrazione sono configurati in modo da eseguire quanto segue:

- Utilizzare le stesse impostazioni dell'applicazione (che possono essere specificate nei criteri di gruppo).
- Utilizzare una modalità operativa comune per tutte le applicazioni grazie alla creazione di attività di gruppo con impostazioni specificate. Tramite le attività di gruppo è ad esempio possibile creare e installare un pacchetto di installazione comune, aggiornare i database e i moduli dell'applicazione, eseguire la scansione del dispositivo su richiesta e abilitare la protezione in tempo reale.

Un dispositivo gestito può appartenere a un solo gruppo di amministrazione.

È possibile creare gerarchie con qualsiasi livello di nidificazione per gli Administration Server e i gruppi. Un singolo livello della gerarchia può comprendere Administration Server secondari e virtuali, gruppi e dispositivi gestiti. È possibile spostare i dispositivi da un gruppo all'altro senza spostarli fisicamente. Ad esempio, se la posizione di un dipendente all'interno dell'azienda cambia da addetto alla contabilità a sviluppatore, è possibile spostare il dispositivo del dipendente dal gruppo di amministrazione Contabilità al gruppo di amministrazione Sviluppatori. Il dispositivo riceverà automaticamente le impostazioni dell'applicazione necessarie per gli sviluppatori.

Dispositivo gestito

Un *dispositivo gestito* è un dispositivo in cui viene eseguito Windows, Linux o macOS in cui è installato Network Agent o un dispositivo mobile in cui è installata un'applicazione di protezione Kaspersky. È possibile gestire tali dispositivi creando attività e criteri per le applicazioni installate nei dispositivi. È inoltre possibile ricevere rapporti dai dispositivi gestiti.

È possibile designare un dispositivo gestito non mobile come punto di distribuzione e come gateway di connessione.

Un dispositivo può essere gestito da un solo Administration Server. Un unico Administration Server può gestire fino a 100.000 dispositivi, compresi i dispositivi mobili.

Dispositivo non assegnato

Un *dispositivo non assegnato* è un dispositivo della rete che non è stato incluso in alcun gruppo di amministrazione. È possibile eseguire alcune azioni sui dispositivi non assegnati, ad esempio spostarli nei gruppi di amministrazione o installarvi applicazioni.

Quando viene individuato un nuovo dispositivo nella rete, questo dispositivo viene inserito nel gruppo di amministrazione **Dispositivi non assegnati**. È possibile configurare regole per lo spostamento automatico dei dispositivi in altri gruppi di amministrazione dopo il rilevamento.

Workstation dell'amministratore

La workstation dell'amministratore è un dispositivo in cui è installato Administration Console o utilizzato per aprire Kaspersky Security Center Web Console. Gli amministratori possono utilizzare tali dispositivi per la gestione remota centralizzata delle applicazioni Kaspersky installate nei dispositivi client.

In seguito all'installazione di Administration Console nel dispositivo, viene visualizzata la relativa icona, che consente di avviare Administration Console. È disponibile nel menu **Start** → **Programmi** → **Kaspersky Security Center**.

Non vi sono limitazioni per il numero di workstation dell'amministratore. Da qualsiasi workstation dell'amministratore è possibile gestire contemporaneamente i gruppi di amministrazione di diversi Administration Server in rete. Una workstation dell'amministratore può essere connessa a un Administration Server (fisico o virtuale) a qualsiasi livello di gerarchia.

È possibile includere una workstation dell'amministratore in un gruppo di amministrazione come dispositivo client.

All'interno dei gruppi di amministrazione di qualsiasi Administration Server, lo stesso dispositivo può operare come un client di Administration Server, un Administration Server o una workstation dell'amministratore.

Plug-in di gestione

Le applicazioni Kaspersky sono gestite tramite Administration Console utilizzando un componente dedicato denominato *plug-in di gestione*. Ciascuna applicazione Kaspersky che può essere gestita tramite Kaspersky Security Center include un plug-in di gestione.

Utilizzando il plug-in di gestione dell'applicazione, è possibile eseguire le seguenti azioni in Administration Console:

- Creare e modificare le impostazioni e i criteri dell'applicazione, nonché le impostazioni delle attività dell'applicazione.
- Ottenere informazioni sulle attività dell'applicazione, sugli eventi che si verificano durante l'esecuzione, oltre che sulle statistiche di esecuzione dell'applicazione ricevute dai dispositivi client.

È possibile scaricare i plug-in di gestione dalla pagina Web del Servizio di assistenza tecnica di Kaspersky.

Plug-in Web di gestione

Un componente speciale (il *plug-in Web di gestione*) viene utilizzato per l'amministrazione remota del software Kaspersky tramite Kaspersky Security Center Web Console. Da questo momento il plug-in Web di gestione verrà denominato anche *plug-in di gestione*. Il plug-in di gestione è un'interfaccia tra Kaspersky Security Center Web Console e un'applicazione Kaspersky specifica. Con un plug-in di gestione è possibile configurare le attività e i criteri per l'applicazione.

È possibile scaricare i plug-in Web di gestione dal sito Web di Kaspersky.

Il plug-in di gestione offre i seguenti elementi:

- Interfaccia per la creazione e la modifica di impostazioni e attività delle applicazioni
- Interfaccia per la creazione e la modifica di criteri e profili criterio per la configurazione centralizzata e remota dei dispositivi e delle applicazioni Kaspersky
- Trasmissione di eventi generati dall'applicazione
- Kaspersky Security Center Web Console consente di visualizzare eventi e dati relativi al funzionamento dell'applicazione e le statistiche trasmesse dai dispositivi client

Criteri

Un *criterio* è un set di impostazioni dell'applicazione Kaspersky che vengono applicate a un gruppo di amministrazione e ai relativi sottogruppi. È possibile installare diverse applicazioni Kaspersky nei dispositivi di un gruppo di amministrazione. Kaspersky Security Center fornisce un singolo criterio per ogni applicazione Kaspersky in un gruppo di amministrazione. Un criterio ha uno dei seguenti stati (vedere la seguente tabella):

Lo stato del criterio

Stato	Descrizione
Attivo	Il criterio corrente applicato al dispositivo. Può essere attivo un solo criterio per un'applicazione Kaspersky in ogni gruppo di amministrazione. I dispositivi applicano i valori delle impostazioni di un criterio attivo per un'applicazione Kaspersky.
Inattivo	Un criterio che non è attualmente applicato a un dispositivo.
Fuori sede	Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.

I criteri funzionano secondo le seguenti regole:

- È possibile configurare diversi criteri con differenti impostazioni per una singola applicazione.
- Un solo criterio può essere attivo per l'applicazione corrente.
- È possibile attivare un criterio inattivo quando si verifica un evento specifico. È ad esempio possibile applicare impostazioni di protezione anti-virus più rigide durante le epidemie di virus.
- Un criterio può avere criteri secondari.

In generale è possibile utilizzare i criteri in preparazione a situazioni di emergenza, come un attacco virus. Ad esempio in caso di attacco tramite unità flash, è possibile attivare un criterio che blocca l'accesso alle unità flash. In questo caso il criterio attivo corrente diventa automaticamente inattivo.

Per evitare di dover gestire più criteri, ad esempio quando diverse occasioni presuppongono solo la modifica di più impostazioni, è possibile utilizzare i profili criterio.

Un *profilo criterio* è un sottoinsieme denominato di valori delle impostazioni dei criteri che sostituisce i valori delle impostazioni di un criterio. Un profilo criterio influisce sulla creazione delle impostazioni ottimizzate in un dispositivo gestito. Per *impostazioni effettive* si intende un insieme di impostazioni dei criteri, impostazioni dei profili criterio e impostazioni delle applicazioni locali attualmente applicate nel dispositivo.

I profili criterio funzionano secondo le seguenti regole:

- Un profilo criterio assume validità quando si verifica una condizione di attivazione specifica.
- I profili criterio contengono valori delle impostazioni che differiscono dalle impostazioni dei criteri.
- L'attivazione di un profilo criterio modifica le impostazioni effettive del dispositivo gestito.
- Un criterio può includere al massimo 100 profili criterio.

Profili criterio

Talvolta può essere necessario creare più istanze di un singolo criterio per diversi gruppi di amministrazione; è inoltre possibile modificare le impostazioni di questi criteri in modo centralizzato. Le istanze potrebbero avere solo una o due impostazioni differenti. Ad esempio, a tutti gli addetti alla contabilità di un'azienda viene applicato lo stesso criterio, ma quelli di livello senior possono utilizzare unità flash, a differenza degli altri. In questo caso, l'applicazione dei criteri ai dispositivi solo tramite la gerarchia dei gruppi di amministrazione può essere poco pratica.

Per evitare di creare più istanze di un singolo criterio, Kaspersky Security Center consente di creare *profili criterio*. I profili criterio sono necessari per consentire l'esecuzione dei dispositivi all'interno di un unico gruppo di amministrazione con diverse impostazioni del criterio.

Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo nel dispositivo gestito. L'attivazione di un profilo modifica le impostazioni del criterio "di base" che erano inizialmente attive nel dispositivo. Le impostazioni modificate assumono i valori specificati nel profilo.

Attività

Kaspersky Security Center consente di gestire le applicazioni di protezione Kaspersky installate nei dispositivi creando ed eseguendo *attività*. Le attività sono necessarie per l'installazione, l'avvio e l'arresto delle applicazioni, la scansione dei file, l'aggiornamento dei database e dei moduli software, oltre che per eseguire altre azioni sulle applicazioni.

Le attività per un'applicazione specifica possono essere create solo se è installato il plug-in di gestione per tale applicazione.

Le attività possono essere eseguite nell'Administration Server e nei dispositivi.

Le seguenti attività vengono eseguite nell'Administration Server:

- Distribuzione automatica dei rapporti
- Download degli aggiornamenti nell'archivio di Administration Server
- Backup dei dati di Administration Server
- Manutenzione del database
- Sincronizzazione di Windows Update
- Creazione di un pacchetto di installazione basato su un'immagine del sistema operativo di un dispositivo di riferimento

I seguenti tipi di attività vengono eseguiti nei dispositivi:

- *Attività locali* - Attività eseguite in un dispositivo specifico

  Le attività locali possono essere modificate dall'amministratore utilizzando gli strumenti di Administration Console oppure dall'utente di un dispositivo remoto (ad esempio, attraverso l'interfaccia dell'applicazione di protezione). Se un'attività locale viene modificata contemporaneamente dall'amministratore e dall'utente di un dispositivo gestito, hanno effetto le modifiche apportate dall'amministratore perché hanno una priorità più alta.

- *Attività di gruppo* - Attività eseguite su tutti i dispositivi di un gruppo specifico

  A meno che non sia diversamente specificato nelle proprietà dell'attività, un'attività di gruppo si applica anche a tutti i sottogruppi del gruppo selezionato. Un'attività di gruppo influisce anche (facoltativamente) sui dispositivi connessi agli Administration Server secondari e virtuali distribuiti nel gruppo o in uno dei relativi sottogruppi.

- *Attività globali* - Attività eseguite su un set di dispositivi, indipendentemente dalla loro appartenenza a un gruppo

Per ogni applicazione è possibile creare attività di gruppo, attività globali o attività locali.

È possibile apportare modifiche alle impostazioni delle attività, visualizzarne l'avanzamento, copiarle, esportarle, importarle ed eliminarle.

Le attività vengono avviate in un dispositivo solo se l'applicazione per cui l'attività è stata creata è in esecuzione.

I risultati delle attività sono salvati nel registro eventi di Microsoft Windows e nel registro eventi di Kaspersky Security Center, sia in modo centralizzato in Administration Server che localmente in ogni dispositivo.

Non includere dati privati nelle impostazioni dell'attività. Ad esempio, non specificare la password dell'amministratore del dominio.

Ambito attività

L'*ambito di un'attività* è il set di dispositivi in cui viene eseguita l'attività. I tipi di ambito sono i seguenti:

- Per un'*attività locale*, l'ambito è il dispositivo stesso.
- Per un'*attività di Administration Server*, l'ambito è Administration Server.
- Per un'*attività di gruppo*, l'ambito è l'elenco dei dispositivi inclusi nel gruppo.

Durante la creazione di un'*attività globale*, è possibile utilizzare i seguenti metodi per specificare l'ambito:

- Specificare manualmente specifici dispositivi.

  È possibile utilizzare un indirizzo IP (o un intervallo IP), un nome NetBIOS o un nome DNS come indirizzo del dispositivo.

- Importare un elenco di dispositivi da un file TXT con gli indirizzi dei dispositivi da aggiungere (ogni indirizzo deve essere specificato su una riga distinta).

  Se si importa un elenco di dispositivi da un file o se ne crea uno manualmente e i dispositivi vengono identificati con i rispettivi nomi, l'elenco deve contenere solo dispositivi per cui sono già state immesse le informazioni nel database di Administration Server. Inoltre, le informazioni devono essere state immesse al momento della connessione dei dispositivi o durante la device discovery.

- Specificare una selezione dispositivi.

  Nel corso del tempo, l'ambito un'attività si modifica, perché il set di dispositivi inclusi nella selezione cambia. Una selezione di dispositivi può essere creata sulla base degli attributi dei dispositivi, incluso il software installato in un dispositivo, e utilizzando i tag assegnati ai dispositivi. Una selezione dispositivi è il modo più flessibile per specificare l'ambito di un'attività.

  Le attività per le selezioni dispositivi vengono sempre eseguite in base a una pianificazione da Administration Server. Queste attività non possono essere eseguite nei dispositivi che non dispongono di una connessione ad Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite direttamente nei dispositivi, pertanto non dipendono dalla connessione del dispositivo ad Administration Server.

  Le attività per le selezioni dispositivi non vengono eseguite in base all'ora locale di un dispositivo, ma in base all'ora locale di Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite in base all'ora locale di un dispositivo.

Relazioni tra impostazioni locali delle applicazioni e criteri

È possibile utilizzare i criteri per impostare valori identici delle impostazioni delle applicazioni per tutti i dispositivi nel gruppo.

I valori delle impostazioni specificati da un criterio possono essere ridefiniti per singoli dispositivi in un gruppo utilizzando le impostazioni locali delle applicazioni. È possibile impostare soltanto i valori delle impostazioni che il criterio consente di modificare, ovvero le impostazioni sbloccate.

Il valore di un'impostazione utilizzata da un'applicazione in un dispositivo client è determinato dalla posizione del lucchetto (🔒) per l'impostazione nel criterio:

- Se la modifica di un'impostazione è bloccata, viene utilizzato lo stesso valore definito nel criterio in tutti i dispositivi client.

- Se la modifica di un'impostazione è "sbloccata", l'applicazione utilizza in ogni dispositivo client il valore dell'impostazione locale invece di quello specificato nel criterio. Il valore del parametro può quindi essere modificato nelle impostazioni locali dell'applicazione.

In questo modo, quando l'attività viene eseguita in un dispositivo client, l'applicazione utilizza impostazioni definite in due modi diversi:

- tramite le impostazioni delle attività e le impostazioni locali delle applicazioni, se la modifica dell'impostazione nel criterio non è bloccata.

- tramite il criterio di gruppo, se la modifica dell'impostazione è bloccata.

Le impostazioni locali delle applicazioni vengono modificate dopo la prima applicazione del criterio in base alle relative impostazioni.

Punto di distribuzione

Per *punto di distribuzione* (prima noto come Update Agent) si intende un dispositivo in cui è installato Network Agent, utilizzato per la distribuzione degli aggiornamenti, l'installazione remota delle applicazioni e il recupero di informazioni sui dispositivi della rete. I punti di distribuzione accelerano la distribuzione degli aggiornamenti e riducono l'utilizzo di risorse di Administration Server.

Le funzionalità e i casi d'uso di Network Agent installato su un dispositivo utilizzato come punto di distribuzione variano a seconda del sistema operativo.

Un punto di distribuzione può eseguire le seguenti funzioni:

- Distribuire i file ricevuti da Administration Server ai dispositivi client nel gruppo (inclusa la distribuzione mediante il multicasting tramite UDP).

  L'elenco dei file che possono essere trasferiti dai punti di distribuzione include:

  - Aggiornamenti dei moduli software e database Kaspersky
  - Aggiornamenti software di terze parti
  - Pacchetti di installazione
  - Aggiornamenti di Windows quando si utilizza Administration Server come server WSUS

  Gli aggiornamenti possono essere ricevuti da Administration Server o dai server di aggiornamento Kaspersky. Nel secondo caso è necessario creare un'attività di aggiornamento per il punto di distribuzione. I dispositivi dei punti di distribuzione che eseguono macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky.

  Se uno o più dispositivi che eseguono macOS rientrano nell'ambito dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'attività viene completata con lo stato *Non riuscito*, anche se è stata completata correttamente in tutti i dispositivi Windows.

- Distribuire criteri e attività di gruppo attraverso il multicasting tramite UDP.
- Operare come gateway per la connessione ad Administration Server per i dispositivi di un gruppo di amministrazione.

  Se è impossibile stabilire una connessione diretta tra i dispositivi gestiti nel gruppo e Administration Server, il punto di distribuzione può essere utilizzato come gateway di connessione ad Administration Server per il gruppo. In questo caso, i dispositivi gestiti sono connessi al gateway di connessione, che a sua volta è connesso ad Administration Server.

  La presenza di un punto di distribuzione che opera come gateway di connessione non esclude la possibilità di una connessione diretta tra i dispositivi gestiti e Administration Server. Se il gateway di connessione non è disponibile, ma è tecnicamente possibile la connessione diretta ad Administration Server, i dispositivi gestiti vengono connessi direttamente ad Administration Server.

- Eseguire il polling della rete per rilevare nuovi dispositivi e aggiornare le informazioni sui dispositivi esistenti. Un punto di distribuzione può applicare gli stessi metodi di device discovery di Administration Server.

- Eseguire l'installazione remota di software di terzi e applicazioni Kaspersky utilizzando gli strumenti del sistema operativo del punto di distribuzione. Si noti che il punto di distribuzione può eseguire l'installazione nei dispositivi client senza Network Agent.

  Questa funzionalità consente di trasferire in remoto i pacchetti di installazione di Network Agent ai dispositivi client disponibili nelle reti a cui l'Administration Server non ha accesso diretto.

- Fungere da server proxy che partecipa a Kaspersky Security Network (KSN).

  È possibile abilitare il proxy KSN da parte del punto di distribuzione per fare in modo che il dispositivo abbia il ruolo di Proxy KSN. In questo caso, il servizio proxy KSN (ksnproxy) viene eseguito nel dispositivo.

I file vengono trasmessi da Administration Server a un punto di distribuzione tramite HTTP o, se la connessione SSL è abilitata, HTTPS. L'utilizzo di HTTP o HTTPS garantisce un livello di prestazioni superiore rispetto a SOAP, grazie alla riduzione del traffico.

Ai dispositivi in cui è installato Network Agent può essere assegnato il ruolo di punti di distribuzione manualmente (dall'amministratore) o automaticamente (da Administration Server). L'elenco completo dei punti di distribuzione per i gruppi di amministrazione specificati è visualizzato nel rapporto sull'elenco dei punti di distribuzione.

L'ambito di un punto di distribuzione è il gruppo di amministrazione a cui è stato assegnato dall'amministratore, nonché i relativi sottogruppi a tutti i livelli. Se sono stati assegnati più punti di distribuzione nella gerarchia dei gruppi di amministrazione, Network Agent nel dispositivo gestito si connette al punto di distribuzione più vicino nella gerarchia.

L'ambito dei punti di distribuzione può anche essere un percorso di rete. Il percorso di rete viene utilizzato per la creazione manuale di un set di dispositivi in cui il punto di distribuzione distribuirà gli aggiornamenti. È possibile determinare il percorso di rete solo per i dispositivi con sistema operativo Windows.

Se i punti di distribuzione sono assegnati automaticamente da Administration Server, vengono assegnati in base ai domini di trasmissione anziché in base ai gruppi di amministrazione. Questo si verifica quando tutti i domini di trasmissione sono noti. Network Agent scambia messaggi con altri Network Agent nella stessa subnet e invia ad Administration Server informazioni su se stesso e su altri Network Agent. Administration Server può utilizzare tali informazioni per raggruppare i Network Agent in base ai domini di trasmissione. I domini di trasmissione diventano noti ad Administration Server in seguito al polling di oltre il 70% dei Network Agent nei gruppi di amministrazione. Administration Server esegue il polling dei domini di trasmissione ogni due ore. In seguito all'assegnazione in base ai domini di trasmissione, i punti di distribuzione non possono essere riassegnati in base ai gruppi di amministrazione.

Se l'amministratore assegna manualmente i punti di distribuzione, questi possono essere assegnati a gruppi di amministrazione o posizioni di rete.

I Network Agent con un profilo di connessione attivo non partecipano al rilevamento dei domini di trasmissione.

Kaspersky Security Center assegna a ciascun Network Agent un indirizzo IP multicast univoco diverso da tutti gli altri indirizzi. Questo consente di evitare il sovraccarico della rete che potrebbe verificarsi a causa di sovrapposizioni IP.

Se due o più punti di distribuzione vengono assegnati in un'unica area di rete o in un singolo gruppo di amministrazione, uno di loro diventa il punto di distribuzione attivo, mentre gli altri diventano punti di distribuzione standby. Il punto di distribuzione attivo scarica gli aggiornamenti e i pacchetti di installazione direttamente da Administration Server, mentre i punti di distribuzione standby ricevono gli aggiornamenti solo dal punto di distribuzione attivo. In questo caso, i file vengono scaricati una sola volta da Administration Server e in seguito distribuiti tra i punti di distribuzione. Se il punto di distribuzione attivo diventa non disponibile per qualsiasi motivo, uno dei punti di distribuzione standby diventa attivo. Administration Server assegna automaticamente a un punto di distribuzione il ruolo di standby.

Lo stato di un punto di distribuzione (*Attivo*/*Standby*) è visualizzato con una casella di controllo nel rapporto di klnagchk.

Un punto di distribuzione richiede almeno 4 GB di spazio disponibile sul disco. Se lo spazio disponibile sul disco del punto di distribuzione è inferiore a 2 GB, Kaspersky Security Center crea un problema di sicurezza con il livello di importanza *Avviso*. Il problema di sicurezza sarà pubblicato nelle proprietà del dispositivo, nella sezione **Problemi di sicurezza**.

L'esecuzione delle attività di installazione remota in un dispositivo assegnato come punto di distribuzione richiede ulteriore spazio libero su disco. Il volume di spazio disponibile sul disco deve essere superiore alle dimensioni totali di tutti i pacchetti di installazione da installare.

L'esecuzione di attività di aggiornamento (installazione delle patch) e di correzione vulnerabilità in un dispositivo con il ruolo di punto di distribuzione richiede ulteriore spazio libero su disco. Il volume di spazio disponibile sul disco deve essere almeno il doppio rispetto alle dimensioni totali di tutte le patch da installare.

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Gateway di connessione

Un *gateway di connessione* è un Network Agent che funziona in modalità speciale. Un gateway di connessione accetta le connessioni da altri Network Agent e le trasmette ad Administration Server tramite la propria connessione con il server. A differenza di un normale Network Agent, un gateway di connessione attende le connessioni da Administration Server anziché stabilire connessioni ad Administration Server.

Un gateway di connessione può ricevere connessioni da un massimo di 10.000 dispositivi.

Sono disponibili due opzioni per utilizzare i gateway di connessione:

- È consigliabile installare un gateway di connessione in una rete perimetrale. Per altri Network Agent installati in dispositivi fuori sede è necessario configurare appositamente una connessione ad Administration Server tramite il gateway di connessione.

  Un gateway di connessione non modifica o elabora in alcun modo i dati trasmessi dai Network Agent ad Administration Server. Inoltre, non scrive questi dati in alcun buffer e non può quindi accettare dati da un Network Agent e in seguito inoltrarli ad Administration Server. Se Network Agent tenta di connettersi ad Administration Server tramite il gateway di connessione, ma il gateway di connessione non riesce a connettersi ad Administration Server, Network Agent percepisce Administration Server come inaccessibile. Tutti i dati rimangono in Network Agent (non nel gateway di connessione).

  Un gateway di connessione non può connettersi ad Administration Server tramite un altro gateway di connessione. Network Agent non può quindi essere contemporaneamente un gateway di connessione e utilizzare un gateway di connessione per connettersi ad Administration Server.

  Tutti i gateway di connessione sono inclusi nell'elenco dei punti di distribuzione nelle proprietà di Administration Server.

- È inoltre possibile utilizzare gateway di connessione all'interno della rete. I punti di distribuzione assegnati automaticamente diventano ad esempio anche gateway di connessione nel proprio ambito. Tuttavia, all'interno di una rete interna, i gateway di connessione non offrono vantaggi considerevoli. Riducono il numero di connessioni di rete ricevute da Administration Server, ma non riducono il volume dei dati in entrata. Anche senza gateway di connessione tutti i dispositivi potrebbero comunque connettersi ad Administration Server.

Scenario di installazione principale

In base a questo scenario è possibile distribuire Administration Server, nonché installare Network Agent e le applicazioni di protezione nei dispositivi della rete. È possibile utilizzare questo scenario sia per un approfondimento sull'applicazione sia per l'installazione dell'applicazione per un ulteriore utilizzo.

L'installazione di Kaspersky Security Center consistono nei seguenti passaggi:

1. Operazioni preliminari
2. Installazione di Kaspersky Security Center e di un'applicazione di protezione Kaspersky nel dispositivo di Administration Server
3. Distribuzione centralizzata delle applicazioni di protezione Kaspersky nei dispositivi client

La distribuzione di Kaspersky Security Center negli ambienti cloud e la distribuzione di Kaspersky Security Center per i provider di servizi sono descritte in altre sezioni della Guida.

È consigliabile assegnare almeno un'ora per l'installazione di Administration Server e un minimo di un giorno lavorativo per il completamento dello scenario. È inoltre consigliabile installare un'applicazione di protezione, ad esempio Kaspersky Security for Windows Server o Kaspersky Endpoint Security, nel dispositivo che opererà come Kaspersky Security Center Administration Server.

Al completamento dello scenario, la protezione verrà distribuita nella rete dell'organizzazione nel seguente modo:

- Il DBMS verrà installato per l'Administration Server.
- Kaspersky Security Center Administration Server verrà installato.

- Tutte le attività e i criteri richiesti verranno creati e verranno specificate le impostazioni predefinite di criteri e attività.
- Le applicazioni di protezione (ad esempio Kaspersky Endpoint Security for Windows) e Network Agent verranno installati nei dispositivi gestiti.
- I gruppi di amministrazione verranno creati (possibilmente in combinazione con una gerarchia).
- Se necessario, la protezione dei dispositivi mobili verrà distribuita.
- Se necessario, i punti di distribuzione verranno assegnati.

L'installazione di Kaspersky Security Center comprende le seguenti fasi:

Operazioni preliminari

1. **Acquisizione dei file necessari**

   Assicurarsi di disporre di una chiave di licenza (codice di attivazione) per Kaspersky Security Center o di chiavi di licenza (codici di attivazione) per le applicazioni di protezione Kaspersky.

   Decomprimere l'archivio ricevuto dal produttore. Questo archivio contiene le chiavi di licenza (file chiave), i codici di attivazione e l'elenco delle applicazioni Kaspersky che possono essere attivate da ciascuna chiave di licenza.

   Se si desidera provare prima Kaspersky Security Center è possibile ottenere una prova gratuita di 30 giorni nel sito Web di Kaspersky.

   Per informazioni dettagliate sulle licenze delle applicazioni di protezione Kaspersky che non sono incluse in Kaspersky Security Center, fare riferimento alla documentazione di tali applicazioni.

2. **Selezione di una struttura per la protezione di un'organizzazione**

   Ulteriori informazioni sui componenti di Kaspersky Security Center. Selezionare la struttura di protezione e la configurazione di rete più adatte all'organizzazione. In base alla configurazione di rete e al throughput dei canali di comunicazione, definire il numero di Administration Server da utilizzare e come devono essere distribuiti tra le varie sedi (se si esegue una rete distribuita).

   Per ottenere e mantenere prestazioni ottimali in diverse condizioni operative, tenere conto del numero di dispositivi in rete, della topologia della rete e del set di funzionalità di Kaspersky Security Center richiesto (per informazioni dettagliate, consultare la Guida per il dimensionamento di Kaspersky Security Center).

   Definire se utilizzare o meno una gerarchia di Administration Server nell'organizzazione. A tale scopo, è necessario valutare se è possibile e conveniente coprire tutti i dispositivi client con un singolo Administration Server o se è necessario creare una gerarchia di Administration Server. Può inoltre essere necessario creare una gerarchia di Administration Server che corrisponda perfettamente alla struttura organizzativa dell'organizzazione per cui si desidera proteggere la rete.

   Se è necessario garantire la protezione dei dispositivi mobili, eseguire tutte le azioni preliminari necessarie per la configurazione di un iOS MDM Server.

   Verificare che i dispositivi selezionati come Administration server, nonché quelli per l'installazione di Administration Console, soddisfino tutti i requisiti hardware e software.

3. **Preparazione per l'utilizzo dei certificati personalizzati**

   Se l'infrastruttura a chiave pubblica (PKI) dell'organizzazione richiede l'utilizzo di certificati personalizzati emessi da un'autorità di certificazione specifica, preparare tali certificati e assicurarsi che soddisfino tutti i requisiti.

4. **Preparazione per la gestione delle licenze di Kaspersky Security Center**

Se si prevede di utilizzare una versione di Kaspersky Security Center con il supporto per Mobile Device Management, Integrazione con i sistemi SIEM e/o Vulnerability e patch management, assicurarsi di disporre di un file chiave o di un codice di attivazione per la gestione delle licenze dell'applicazione.

5. **Preparazione per la gestione delle licenze delle applicazioni di protezione gestite**

   Durante la distribuzione della protezione è necessario fornire a Kaspersky le chiavi di licenza attive per le applicazioni da gestire tramite Kaspersky Security Center (visualizzare l'elenco delle applicazioni di protezione gestibili). Per informazioni dettagliate sulla gestione delle licenze di una qualsiasi applicazione di protezione, è possibile fare riferimento alla documentazione di questa applicazione.

6. **Selezione della configurazione hardware dell'Administration Server e del DBMS**

   Pianificare la configurazione hardware per il DBMS e Administration Server, tenendo conto del numero di dispositivi della rete.

7. **Selezione di un DBMS**

   Durante la selezione di un DBMS, tenere conto del numero di dispositivi gestiti da coprire con questo Administration Server. Se la rete include meno di 10.000 dispositivi e non si prevede di incrementare questo numero, è possibile scegliere un DBMS gratuito, come SQL Express o MySQL, e installarlo nello stesso dispositivo di Administration Server. In alternativa, è possibile scegliere il DBMS MariaDB che consente di gestire fino a 20.000 dispositivi. Se la rete include più di 10.000 dispositivi (o se si prevede di espandere la rete fino a oltrepassare questo numero di dispositivi), è consigliabile scegliere un DBMS SQL a pagamento e installarlo in un dispositivo dedicato. Un DBMS a pagamento può essere utilizzato con più Administration Server, mentre un DBMS gratuito può supportarne uno solo.

   Se si seleziona SQL Server DBMS, tenere presente che è possibile migrare i dati archiviati nel database nel DBMS di MySQL, MariaDB o Azure SQL. Per eseguire la migrazione, eseguire il backup dei dati e ripristinarli nel nuovo DBMS.

8. **Installazione del DBMS e creazione del database**

   È possibile ottenere ulteriori informazioni sugli account per l'utilizzo con il DBMS e installare il DBMS.

   Prima dell'installazione, scegliere un DBMS supportato. È possibile selezionare, ad esempio, PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL o MariaDB.

   Per informazioni su come installare il DBMS selezionato, consultare la relativa documentazione.

   Se si installa MariaDB, MySQL, PostgreSQL o PostgresPro, utilizzare le impostazioni consigliate per garantire il corretto funzionamento del DBMS.

   Annotare e salvare le impostazioni del DBMS poiché saranno necessarie durante l'installazione di Administration Server. Queste impostazioni includono il nome SQL Server, il numero della porta utilizzata per la connessione a SQL Server, il nome dell'account e la password per l'accesso a SQL Server.

   > Se si decide di installare il DBMS di PostgreSQL o Postgres Pro, assicurarsi di aver specificato una password per il l'utente con privilegi avanzati. Se la password non viene specificata, Administration Server potrebbe non essere in grado di connettersi al database.

   Per impostazione predefinita, il programma di installazione di Kaspersky Security Center crea il database per l'archiviazione delle informazioni di Administration Server, ma è possibile scegliere di non creare il database e utilizzare un database diverso. In questo caso verificare che il database sia stato creato, di conoscere il relativo nome e che l'account con cui Administration Server otterrà l'accesso a questo database disponga del ruolo db_owner attinente.

   Se necessario, contattare l'amministratore del DBMS per ulteriori informazioni.

9. **Configurazione delle porte**

   Verificare che tutte le porte necessarie siano aperte per l'interazione tra i componenti in base della struttura di protezione selezionata.

Se è necessario concedere ad Administration Server l'accesso a Internet, configurare le porte e specificare le impostazioni di connessione, a seconda della configurazione di rete.

10. **Controllo degli account**

    Verificare di disporre di tutti i diritti di amministratore locale richiesti per l'installazione di Kaspersky Security Center Administration Server e per la conseguente distribuzione della protezione nei dispositivi. I diritti di amministratore locale nei dispositivi client sono richiesti per l'installazione di Network Agent in tali dispositivi. Dopo l'installazione di Network Agent, è possibile utilizzarlo per installare le applicazioni nei dispositivi in remoto, senza utilizzare l'account con i diritti di amministratore del dispositivo.

    Per impostazione predefinita, nel dispositivo selezionato per l'installazione di Administration Server, il programma di installazione di Kaspersky Security Center crea tre account locali con cui verranno eseguiti Administration Server e i servizi di Administration Server:

    - KL-AK-*: account del servizio di Administration Server
    - NT Service/KSC*: account per altri servizi del pool di Administration Server
    - KlPxeUser: account per la distribuzione dei sistemi operativi

    È possibile scegliere di non creare account per i servizi di Administration Server e altri servizi. È possibile utilizzare gli account esistenti, ad esempio account di dominio, se si intende installare Administration Server in un cluster di failover o se per qualche motivo si intende utilizzare gli account di dominio anziché gli account locali. In questo caso, assicurarsi che gli account destinati all'esecuzione di Administration Server e dei servizi di Kaspersky Security Center siano stati creati, siano privi di privilegi e dispongano di tutte le autorizzazioni necessarie per l'accesso al DBMS. Se si pianifica una distribuzione successiva dei sistemi operativi nei dispositivi tramite Kaspersky Security Center, non rinunciare alla creazione degli account.

Installazione di Kaspersky Security Center e di un'applicazione di protezione Kaspersky nel dispositivo di Administration Server

1. **Installazione di Administration Server, Administration Console, Kaspersky Security Center Web Console e plug-in di gestione per le applicazioni di protezione**

    Scaricare Kaspersky Security Center dal sito Web Kaspersky. È possibile scaricare il pacchetto completo, solo Web Console o solo Administration Console.

    Installare Administration Server nel dispositivo selezionato (o più dispositivi se è necessario utilizzare più Administration Server). È possibile selezionare l'installazione standard o personalizzata di Administration Server. Administration Console verrà installato insieme ad Administration Server. È consigliabile installare Administration Server in un server dedicato anziché in un controller di dominio.

    L'installazione standard è consigliabile se si desidera provare a utilizzare Kaspersky Security Center, ad esempio verificandone il funzionamento in un'area delimitata all'interno della rete. Durante l'installazione standard, è possibile esclusivamente configurare il database. È inoltre possibile installare solo il set predefinito di plug-in di gestione delle applicazioni Kaspersky. È inoltre possibile utilizzare l'installazione standard se si dispone già di una certa esperienza nell'utilizzo di Kaspersky Security Center in modo da poter specificare tutte le impostazioni pertinenti dopo l'installazione standard.

    L'installazione personalizzata è consigliabile se si intende modificare le impostazioni di Kaspersky Security Center, ad esempio il percorso della cartella condivisa, gli account e le porte per la connessione ad Administration Server, nonché le impostazioni del database. L'installazione personalizzata consente di specificare quali plug-in di gestione di Kaspersky installare. Se necessario, è possibile avviare l'installazione personalizzata in modalità automatica.

    Administration Console e la versione del server di Network Agent vengono installate insieme ad Administration Server. È anche possibile scegliere di installare Kaspersky Security Center Web Console durante l'installazione.

    Se si desidera, è possibile installare Administration Console e/o Kaspersky Security Center Web Console nella workstation dell'amministratore separatamente per gestire Administration Server dalla rete.

2 Configurazione iniziale e licensing

Quando l'installazione di Administration Server è completa, alla prima connessione ad Administration Server viene avviato automaticamente l'Avvio rapido guidato. Eseguire la configurazione iniziale di Administration Server in base ai requisiti esistenti. Durante la fase di configurazione iniziale, la procedura guidata utilizza le impostazioni predefinite per creare i criteri e le attività necessari per la distribuzione della protezione. Le impostazioni predefinite potrebbero tuttavia non essere ottimali per le esigenze dell'organizzazione. Se necessario, è possibile modificare le impostazioni di criteri e attività (Configurazione della protezione nella rete di un'organizzazione client, Scenario: Configurazione della protezione di rete).

Se si prevede di utilizzare funzionalità esterne alla funzionalità di base, concedere la licenza all'applicazione. È possibile eseguire questa operazione in uno dei passaggi dell'Avvio rapido guidato.

3 Controllo della corretta installazione di Administration Server

Quando tutti i passaggi precedenti sono completi, Administration Server viene installato ed è pronto all'uso.

Accertarsi che Administration Console funzioni e che sia possibile connettersi ad Administration Server tramite Administration Console. Verificare inoltre che in Administration Server sia disponibile l'attività Scarica gli aggiornamenti nell'archivio dell'Administration Server (nella cartella **Attività** della struttura della console), nonché il criterio per Kaspersky Endpoint Security (nella cartella **Criteri** della struttura della console).

Dopo aver completato la verifica, procedere come segue.

Distribuzione centralizzata delle applicazioni di protezione Kaspersky nei dispositivi client

1 Individuazione dei dispositivi nella rete

Questo passaggio fa parte dell'Avvio rapido guidato. È inoltre possibile avviare manualmente la device discovery. Kaspersky Security Center riceve gli indirizzi e i nomi di tutti i dispositivi rilevati nella rete. È quindi possibile utilizzare Kaspersky Security Center per installare le applicazioni Kaspersky e software di altri produttori nei dispositivi rilevati. Kaspersky Security Center avvia periodicamente la device discovery, pertanto eventuali nuove istanze che compaiono nella rete verranno rilevate automaticamente.

2 Installazione di Network Agent e di applicazioni di protezione nei dispositivi in rete

La distribuzione della protezione (Configurazione della protezione nella rete di un'organizzazione client, Scenario: Configurazione della protezione di rete) della rete di un'organizzazione implica l'installazione di Network Agent e delle applicazioni di protezione (ad esempio Kaspersky Endpoint Security) nei dispositivi rilevati da Administration Server durante la device discovery.

Le applicazioni di protezione proteggono i dispositivi da virus e/o da altri programmi che costituiscono una minaccia. Network Agent garantisce la comunicazione tra il dispositivo e Administration Server. Le impostazioni di Network Agent vengono configurate automaticamente per impostazione predefinita.

È possibile installare Network Agent in modalità automatica con un file di risposta o senza un file di risposta.

Prima di iniziare a installare Network Agent e le applicazioni di protezione nei dispositivi nella rete, verificare che questi dispositivi siano accessibili (e quindi attivati). È possibile installare Network Agent in macchine virtuali e in dispositivi fisici.

Le applicazioni di protezione e Network Agent possono essere installati in locale o in remoto.

Installazione remota: utilizzando la Distribuzione guidata della protezione, è possibile installare in remoto l'applicazione di protezione (ad esempio Kaspersky Endpoint Security for Windows) e Network Agent nei dispositivi rilevati da Administration Server nella rete dell'organizzazione. In genere, l'attività Installazione remota distribuisce correttamente la protezione nella maggior parte dei dispositivi in rete. Tuttavia, l'attività può restituire un errore in alcuni dispositivi se, ad esempio, un dispositivo è spento o non è accessibile per qualche motivo. In tal caso, è consigliabile connettersi al dispositivo manualmente e utilizzare l'installazione locale.

L'installazione locale—Viene utilizzata nei dispositivi di rete in cui non è stato possibile distribuire la protezione tramite un'attività di installazione remota. Per installare la protezione in tali dispositivi, creare un pacchetto di installazione indipendente da eseguire localmente in tali dispositivi.

L'installazione di Network Agent nei dispositivi che eseguono sistemi operativi Linux e macOS è descritta nella documentazione per Kaspersky Endpoint Security for Linux e Kaspersky Endpoint Security for Mac, rispettivamente. Sebbene i dispositivi con sistemi operativi Linux e macOS siano considerati meno vulnerabili rispetto ai dispositivi che eseguono Windows, è comunque consigliabile installare applicazioni di protezione in tali dispositivi.

Dopo l'installazione, accertarsi che l'applicazione di protezione sia installata nei dispositivi gestiti. Eseguire un rapporto sulla versione del software Kaspersky e visualizzarne i risultati.

3. **Distribuzione delle chiavi di licenza ai dispositivi client**

   Distribuire le chiavi di licenza ai dispositivi client per attivare applicazioni di protezione gestite in tali dispositivi.

4. **Configurazione della protezione dei dispositivi mobili**

   Questo passaggio fa parte dell'Avvio rapido guidato.

   Se si desidera gestire i dispositivi mobili aziendali, eseguire i passaggi necessari per la preparazione e la distribuzione di Mobile Device Management.

5. **Creazione di una struttura di gruppi di amministrazione**

   In alcuni casi, la distribuzione della protezione nei dispositivi della rete nel modo più immediato può richiedere la suddivisione dell'intero pool di dispositivi in gruppi di amministrazione, tenendo conto della struttura dell'organizzazione. È possibile creare regole di spostamento al fine di distribuire i dispositivi tra i gruppi oppure distribuire manualmente i dispositivi. È possibile assegnare attività di gruppo per i gruppi di amministrazione, definire l'ambito dei criteri e assegnare i punti di distribuzione.

   Verificare che tutti i dispositivi gestiti siano stati assegnati correttamente ai gruppi di amministrazione appropriati e che non siano più presenti dispositivi non assegnati nella rete.

6. **Assegnazione dei punti di distribuzione**

   Kaspersky Security Center assegna automaticamente i punti di distribuzione ai gruppi di amministrazione ma è possibile assegnarli manualmente, se necessario. È consigliabile utilizzare i punti di distribuzione nelle reti su vasta scala per ridurre il carico su Administration Server e nelle reti con una struttura distribuita per consentire ad Administration Server di accedere ai dispositivi (o ai gruppi di dispositivi) tramite canali a basso throughput. È possibile utilizzare dispositivi che eseguono Linux come punti di distribuzione, nonché dispositivi che eseguono Windows.

Porte utilizzate da Kaspersky Security Center

Le tabelle seguenti mostrano le porte predefinite utilizzate dagli Administration Server e dai dispositivi client. È possibile modificare i numeri di porta predefiniti.

Se si installa Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL, la porta 1433 per Microsoft SQL Server o la porta 5432 per PostgreSQL e Postgres Pro). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

Porte utilizzate dall'Administration Server

Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta	Ambito
8060	klcsweb	TCP	Trasmissione dei pacchetti di installazione pubblicati ai dispositivi client	Pubblicazione dei pacchetti di installazione. È possibile modificare il numero di porta predefinito nella sezione **Web Server** della finestra delle proprietà di Administration Server in Administration Console o in Kaspersky Security Center Web Console. Questa porta è facoltativa. Per motivi di sicurezza, si consiglia di utilizzare la porta TCP 8061.
8061	klcsweb	TCP (TLS)	Trasmissione dei pacchetti di installazione pubblicati ai dispositivi client	Pubblicazione dei pacchetti di installazione. È possibile modificare il numero di porta predefinito nella sezione **Web Server** della finestra delle proprietà di Administration Server in Administration Console o in Kaspersky Security Center Web Console.
13000	klserver	TCP (TLS)	Ricezione delle connessioni dai Network Agent e dagli Administration Server secondari; utilizzata anche negli Administration Server secondari per la ricezione delle connessioni dall'Administration Server primario (ad esempio, se l'Administration Server secondario è nella rete perimetrale)	Gestione dei dispositivi client e degli Administration Server secondari. È possibile modificare il numero di porta predefinito per la ricezione delle connessioni dai Network Agent durante la configurazione delle porte di connessione; è possibile modificare il numero di porta predefinito per la ricezione delle connessioni dagli Administration Server secondari durante la creazione di una gerarchia di Administration Server in Administration Console o in Kaspersky Security Center Web Console.
13000	klserver	UDP	Ricezione di informazioni sui dispositivi che sono stati spenti dai Network Agent	Gestione dei dispositivi client. È possibile modificare il numero di porta predefinito nelle impostazioni del criterio di Network Agent in Administration Console o in Kaspersky Security Center Web Console.
13291	klserver	TCP (TLS)	Ricezione delle connessioni da Administration Console ad Administration Server	Gestione di Administration Server. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server in Administration Console.
13299	klserver	TCP (TLS)	Ricezione delle connessioni da Kaspersky Security Center Web Console ad Administration Server; ricezione delle connessioni ad Administration Server tramite OpenAPI	Kaspersky Security Center Web Console, OpenAPI. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server (sezione **Impostazioni di connessione di Administration Server** → sottosezione **Porte di connessione**) in Administration Console o durante la creazione di una gerarchia di Administration Server in Administration Console o in Kaspersky Security Center Web Console.
14000	klserver	TCP	Ricezione delle connessioni dai Network Agent	Gestione dei dispositivi client. È possibile modificare il numero di porta predefinito durante la configurazione delle porte di connessione nel corso dell'installazione di Kaspersky Security Center o durante la connessione manuale di un dispositivo client ad Administration Server. Questa porta è facoltativa. Per motivi di sicurezza, si consiglia di utilizzare la porta TCP 13000.
13111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	ksnproxy	TCP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server.
15111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	ksnproxy	UDP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server.

Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta	Ambito
17000	klactprx	TCP (TLS)	Ricezione delle connessioni per l'attivazione dell'applicazione dai dispositivi gestiti (ad eccezione dei dispositivi mobili)	Server proxy di attivazione utilizzato da dispositivi non mobili per attivare le applicazioni Kaspersky con codici di attivazione. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server.
17100 (solo se si gestiscono dispositivi mobili)	klactprx	TCP (TLS)	Ricezione delle connessioni per l'attivazione dell'applicazione dai dispositivi mobili	Server proxy di attivazione per i dispositivi mobili. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server.
19170	klserver	HTTPS (TLS)	Tunneling delle connessioni ai dispositivi gestiti tramite l'utilità klsctunnel	Connessione remota ai dispositivi gestiti tramite Kaspersky Security Center Web Console. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server solo in Administration Console (sezione**Impostazioni di connessione di Administration Server** → sottosezione **Porte di connessione** → **opzione Apri porta RDP per Kaspersky Security Center Web Console**).
13292 (solo se si gestiscono dispositivi mobili)	klserver	TCP (TLS)	Ricezione delle connessioni dai dispositivi mobili	Mobile Device Management. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server in Administration Console o in Kaspersky Security Center Web Console.
13294 (solo se si gestiscono dispositivi mobili)	klserver	TCP (TLS)	Ricezione delle connessioni dai dispositivi di protezione UEFI	Gestione dei dispositivi client di protezione UEFI. È possibile modificare il numero di porta predefinito quando si connettono i dispositivi mobili o successivamente nella finestra delle proprietà di Administration Server (sezione **Impostazioni di connessione di Administration Server** → sottosezione **Porte di connessione**) in Administration Console o in Kaspersky Security Center Web Console.
13296	klserver	TCP (TLS)	Pubblicazione delle metriche di Kaspersky Security Center per Prometheus	Pubblicazione delle metriche di Kaspersky Security Center che saranno ulteriormente ottenute da Prometheus. È possibile visualizzare le metriche tramite il seguente collegamento: https://<`indirizzo_server`>:13296/metrics. In <`indirizzo_server`>, specificare l'indirizzo IP o il nome di dominio dell'Administration Server. È possibile modificare il numero di porta predefinito nella finestra delle proprietà di Administration Server in Administration Console.
30522, 30523 (porte sull'interfaccia localhost)	klnagent	TCP	Ricezione degli aggiornamenti delle applicazioni Kaspersky da Administration Server tramite il componente FileTransferBridge	Il dispositivo Administration Server che riceve gli aggiornamenti delle applicazioni Kaspersky.

La tabella seguente mostra la porta utilizzata dal server per dispositivi mobili MDM iOS (solo se si gestiscono dispositivi mobili).

Porta utilizzata dal server per dispositivi mobili MDM iOS

Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta	Ambito
443	kliosmdmservicesrv	TCP (TLS)	Ricezione delle connessioni dai dispositivi mobili iOS	Mobile Device Management. È possibile modificare il numero di porta predefinito durante l'installazione del server per dispositivi mobili MDM iOS.

Nella tabella seguente viene mostrata la porta utilizzata dal server Kaspersky Security Center Web Console. Può trattarsi dello stesso dispositivo in cui è installato Administration Server o di un dispositivo diverso.

Porta utilizzata da Kaspersky Security Center Web Console Server

Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta	Ambito
8080	Node.js: Server-side JavaScript	TCP (TLS)	Ricezione delle connessioni dal browser a Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. È possibile modificare il numero di porta predefinito durante l'installazione di Kaspersky Security Center Web Console in un dispositivo che esegue Windows o su una piattaforma Linux. Se si installa Kaspersky Security Center Web Console nel sistema operativo Linux ALT, è necessario specificare un numero di porta diverso da 8080, poiché la porta 8080 è utilizzata dal sistema operativo.

La tabella seguente mostra la porta utilizzata dai dispositivi gestiti in cui è installato Network Agent.

Porte utilizzate da Network Agent

Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta	Ambito
15000	klnagent	UDP	Segnali di gestione da Administration Server o dal punto di distribuzione ai Network Agent	Gestione dei dispositivi client. È possibile modificare il numero di porta predefinito nelle impostazioni del criterio di Network Agent in Administration Console o in Kaspersky Security Center Web Console.
15000	klnagent	Trasmissione UDP	Ottenimento dei dati su altri Network Agent all'interno dello stesso dominio di trasmissione (i dati vengono quindi inviati ad Administration Server)	Distribuzione degli aggiornamenti e dei pacchetti di installazione.
15001	klnagent	UDP	Ricezione di richieste multicast da un punto di distribuzione (se in uso)	Ricezione di aggiornamenti e pacchetti di installazione da un punto di distribuzione. È possibile modificare il numero di porta predefinito nella finestra delle proprietà del punto di distribuzione in Administration Console o in Kaspersky Security Center Web Console.
30522, 30523 (porte sull'interfaccia localhost)	klnagent	TCP	Ricezione degli aggiornamenti delle applicazioni Kaspersky da Administration Server tramite il componente FileTransferBridge	Dispositivi gestiti che ricevono gli aggiornamenti delle applicazioni Kaspersky dall'Administration Server specificato come sorgente degli aggiornamenti del database.
161	klnagent	SNMP	Monitoraggio e rilevamento dei dispositivi in rete.	Rilevabilità dei dispositivi.

Si noti che il processo klnagent può anche richiedere porte libere dall'intervallo di porte dinamiche del sistema operativo di un endpoint. Queste porte vengono assegnate automaticamente al processo klnagent dal sistema operativo, quindi il processo klnagent può utilizzare alcune porte usate da un altro software. Se il processo klnagent influisce sulle operazioni del software, modificare le impostazioni delle porte in questo software o modificare l'intervallo di porte dinamiche predefinito nel sistema operativo per escludere la porta utilizzata dal software interessato.

Tenere inoltre presente che i suggerimenti sulla compatibilità di Kaspersky Security Center con il software di terze parti sono descritti solo come riferimento e potrebbero non essere applicabili alle nuove versioni del software di terze parti. I suggerimenti descritti per la configurazione delle porte si basano sull'esperienza dell'Assistenza tecnica e sulle nostre best practice.

La tabella seguente mostra le porte utilizzato da un dispositivo gestito in cui è installato Network Agent con il ruolo di punto di distribuzione. Oltre alle porte utilizzate dai Network Agent, anche le porte elencate sono utilizzate dai dispositivi del punto di distribuzione (vedere la tabella sopra).

Porte utilizzate da Network Agent con il ruolo di punto di distribuzione

Numero di porta	Nome del processo che apre la porta	Protocollo	Ambito della porta	Ambito
13000	klnagent	TCP (TLS)	Ricezione di connessioni dai Network Agent e da Kaspersky Security Center quando il punto di distribuzione funge da gateway di connessione nella rete perimetrale. Se un dispositivo con Administration Server installato è specificato come punto di distribuzione, per impostazione predefinita viene utilizzata la porta 13001 per la connessione SSL anziché 13000.	Gestione dei dispositivi client, distribuzione degli aggiornamenti e dei pacchetti di installazione. Per informazioni dettagliate, vedere il seguente argomento: Administration Server, un gateway di connessione in un segmento di rete e un dispositivo client. È possibile modificare il numero di porta predefinito nella finestra delle proprietà del punto di distribuzione in Administration Console o in Kaspersky Security Center Web Console.
13111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	ksnproxy	TCP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN. È possibile modificare il numero di porta predefinito nella finestra delle proprietà del punto di distribuzione in Administration Console o in Kaspersky Security Center Web Console.
15111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	ksnproxy	UDP	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN. È possibile modificare il numero di porta predefinito nella finestra delle proprietà del punto di distribuzione in Administration Console o in Kaspersky Security Center Web Console.
17111 (solo se il servizio proxy KSN è in esecuzione nel dispositivo)	ksnproxy	HTTPS	Ricezione delle richieste dai dispositivi gestiti al server proxy KSN	Server proxy KSN. È possibile modificare il numero di porta predefinito nella finestra delle proprietà del punto di distribuzione in Administration Console o in Kaspersky Security Center Web Console.
13295 (solo se si utilizza il punto di distribuzione come server push)	klnagent	TCP (TLS)	Ricezione delle connessioni dai dispositivi client	Server push. È possibile modificare il numero di porta predefinito nella finestra delle proprietà del punto di distribuzione in Administration Console o in Kaspersky Security Center Web Console.

La tabella seguente mostra le porte utilizzate da un dispositivo controller di dominio.

Porte utilizzate da un dispositivo controller di dominio

Numero di porta	Protocollo	Ambito della porta	Ambito
389	LDAP su TCP o UDP	Connessione a un server LDAP	Polling del controller di dominio
636	LDAP su TLS	Connessione a un server LDAP	Polling del controller di dominio

Certificati per l'utilizzo di Kaspersky Security Center

Questa sezione contiene le informazioni sui certificati Kaspersky Security Center e descrive come emettere un certificato personalizzato per Administration Server.

Informazioni sui certificati di Kaspersky Security Center

Kaspersky Security Center utilizza i seguenti tipi di certificati per consentire un'interazione sicura tra i componenti dell'applicazione:

- Certificato di Administration Server
- Certificato mobile
- Certificato del server per dispositivi mobili MDM iOS
- Certificato del server Web di Kaspersky Security Center
- Certificato di Kaspersky Security Center Web Console

Per impostazione predefinita, Kaspersky Security Center utilizza certificati autofirmati (ovvero emessi da Kaspersky Security Center stesso), ma è possibile sostituirli con certificati personalizzati per soddisfare al meglio i requisiti della rete dell'organizzazione e rispettare gli standard di sicurezza. Quando Administration Server verifica che un certificato personalizzato soddisfa tutti i requisiti applicabili, il certificato assume lo stesso ambito funzionale di un certificato autofirmato. L'unica differenza è che un certificato personalizzato non viene riemesso automaticamente alla scadenza. È possibile sostituire i certificati con quelli personalizzati tramite l'utilità klsetsrvcert o la sezione delle proprietà di Administration Server in Administration Console, a seconda del tipo di certificato. Quando si utilizza l'utilità klsetsrvcert, è necessario specificare un tipo di certificato utilizzando uno dei seguenti valori:

- C: certificato comune per le porte 13000 e 13291.
- CR: certificato di riserva comune per le porte 13000 e 13291.
- M: certificato mobile per la porta 13292.
- MR: certificato di riserva mobile per la porta 13292.
- MCA: autorità di certificazione mobile per certificati utente generati automaticamente.

> Non è necessario scaricare l'utilità klsetsrvcert. È inclusa nel kit di distribuzione di Kaspersky Security Center. L'utilità non è compatibile con le versioni precedenti di Kaspersky Security Center.

Il periodo di validità massimo di qualsiasi certificato di Administration Server non deve superare i 397 giorni.

Certificati di Administration Server

È necessario un certificato di Administration Server per l'autenticazione di Administration Server, nonché per l'interazione sicura tra Administration Server e Network Agent nei dispositivi gestiti o tra l'Administration Server primario e gli Administration Server secondari. Quando si connette Administration Console ad Administration Server per la prima volta, viene richiesto di confermare l'utilizzo del certificato di Administration Server corrente. Tale conferma è richiesta anche ogni volta che il certificato di Administration Server viene sostituito, dopo ogni reinstallazione di Administration Server e quando si collega un Administration Server secondario all'Administration Server primario. Questo certificato è denominato comune ("C").

Il certificato comune ("C") viene creato automaticamente durante l'installazione del componente Administration Server. Il certificato si compone di due parti:

- file klserver.cer; per impostazione predefinita, si trova nel dispositivo in cui è installato il componente Administration Server nella cartella C:\ProgramData\KasperskyLab\adminkit\1093\cert.
- Chiave segreta situata nell'archivio protetto di Windows.

Esiste inoltre un certificato di riserva comune ("CR"). Kaspersky Security Center genera automaticamente questo certificato 90 giorni prima della scadenza del certificato comune. Il certificato di riserva comune viene successivamente utilizzato per la sostituzione immediata del certificato di Administration Server. Quando il certificato comune sta per scadere, il certificato di riserva comune viene utilizzato per gestire la connessione con le istanze di Network Agent installate nei dispositivi gestiti. A tale scopo, il certificato di riserva comune diventa automaticamente il nuovo certificato comune 24 ore prima della scadenza del certificato comune precedente.

È inoltre possibile eseguire il backup del certificato di Administration Server separatamente dalle altre impostazioni di Administration Server per spostare Administration Server da un dispositivo all'altro senza perdite di dati.

Certificati mobili

Per l'autenticazione di Administration Server nei dispositivi mobili è richiesto un certificato mobile ("M"). L'utilizzo del certificato mobile viene configurato nel passaggio dedicato dell'Avvio rapido guidato.

Esiste inoltre un certificato di riserva mobile ("MR"): viene utilizzato per la sostituzione immediata del certificato mobile. Kaspersky Security Center genera automaticamente questo certificato 60 giorni prima della scadenza del certificato comune. Quando il certificato mobile sta per scadere, il certificato di riserva mobile viene utilizzato per gestire la connessione con le istanze di Network Agent installate nei dispositivi mobili gestiti. A tale scopo, il certificato di riserva mobile diventa automaticamente il nuovo certificato mobile 24 ore prima della scadenza del certificato mobile precedente.

Se lo scenario di connessione richiede l'utilizzo di un certificato client nei dispositivi mobili (connessione che implica l'autenticazione SSL bidirezionale), è possibile generare tali certificati tramite l'autorità di certificazione per i certificati utente generati automaticamente ("MCA"). L'Avvio rapido guidato consente inoltre di iniziare a utilizzare certificati client personalizzati emessi da un'autorità di certificazione diversa, mentre l'integrazione con l'infrastruttura a chiave pubblica (PKI) del dominio dell'organizzazione consente di emettere certificati client tramite l'autorità di certificazione del dominio.

Certificato del server per dispositivi mobili MDM iOS

È necessario un certificato del server per dispositivi mobili MDM iOS per l'autenticazione di Administration Server nei dispositivi mobili che eseguono il sistema operativo iOS. L'interazione con questi dispositivi viene eseguita tramite il protocollo MDM (Mobile Device Management) di Apple che non coinvolge Network Agent. È invece necessario installare uno speciale profilo MDM iOS contenente un certificato client in ogni dispositivo, per garantire l'autenticazione SSL bidirezionale.

L'Avvio rapido guidato consente inoltre di iniziare a utilizzare certificati client personalizzati emessi da un'autorità di certificazione diversa, mentre l'integrazione con l'infrastruttura a chiave pubblica (PKI) del dominio dell'organizzazione consente di emettere certificati client tramite l'autorità di certificazione del dominio.

I certificati client vengono trasmessi ai dispositivi iOS quando si scaricano i profili MDM iOS. Un certificato client del server per dispositivi mobili MDM iOS è univoco per ogni dispositivo iOS gestito. Tutti i certificati client del server per dispositivi mobili MDM iOS vengono generati tramite l'autorità di certificazione per i certificati utente generati automaticamente ("MCA").

Certificato del server Web di Kaspersky Security Center

Server Web di Kaspersky Security Center (di seguito denominato server Web), un componente di Kaspersky Security Center Administration Server, utilizza un tipo speciale di certificato. Questo certificato è necessario per pubblicare i pacchetti di installazione di Network Agent scaricati successivamente nei dispositivi gestiti, nonché per pubblicare profili MDM iOS, app iOS e pacchetti di installazione di Kaspersky Security for Mobile. A tale scopo, Server Web può utilizzare diversi certificati.

Se il supporto dei dispositivi mobili è disabilitato, Server Web utilizza uno dei seguenti certificati, in ordine di priorità:

1. Certificato Server Web personalizzato specificato manualmente tramite Administration Console
2. Certificato di Administration Server comune ("C")

Se il supporto dei dispositivi mobili è abilitato, Server Web utilizza uno dei seguenti certificati, in ordine di priorità:

1. Certificato Server Web personalizzato specificato manualmente tramite Administration Console
2. Certificato mobile personalizzato
3. Certificato mobile autofirmato ("M")
4. Certificato di Administration Server comune ("C")

Certificato di Kaspersky Security Center Web Console

Kaspersky Security Center Web Console Server (di seguito denominato Web Console) dispone di un proprio certificato. Quando si apre un sito Web, un browser verifica se la connessione è attendibile. Il certificato di Web Console consente di autenticare Web Console e viene utilizzato per criptare il traffico tra un browser e Web Console.

Quando si apre Web Console, il browser potrebbe informare che la connessione a Web Console non è privata e il certificato Web Console non è valido. Questo avviso viene visualizzato perché il certificato di Web Console è autofirmato e generato automaticamente da Kaspersky Security Center. Per rimuovere questo avviso è possibile eseguire una delle seguenti operazioni:

- Sostituire il certificato di Web Console con uno personalizzato (opzione consigliata). Creare un certificato attendibile nella propria infrastruttura e che soddisfi i requisiti per i certificati personalizzati.
- Aggiungere il certificato di Web Console all'elenco dei certificati del browser attendibili. È consigliabile utilizzare questa opzione solo se non è possibile creare un certificato personalizzato.

Informazioni sul certificato di Administration Server

Vengono eseguite due operazioni in base al *certificato di Administration Server:* l'autenticazione di Administration Server durante la connessione di Administration Console e lo scambio dei dati con i dispositivi. Il certificato è inoltre utilizzato per l'autenticazione durante la connessione degli Administration Server primari agli Administration Server secondari.

Certificato rilasciato da Kaspersky

Il certificato di Administration Server viene creato automaticamente durante l'installazione del componente Administration Server e viene archiviato nella cartella %ALLUSERSPROFILE%\Application Data\KaspersкyLab\adminkit\1093\cert.

Il certificato di Administration Server è valido per cinque anni, se è stato generato da Administration Server versione 12.2 o precedente. In caso contrario il periodo di validità del certificato è limitato a 397 giorni. Un nuovo certificato viene generato da Administration Server come certificato di riserva 90 giorni prima della data di scadenza del certificato corrente. Successivamente, il nuovo certificato sostituisce automaticamente il certificato corrente un giorno prima della data di scadenza. Tutti i Network Agent nei dispositivi client vengono riconfigurati automaticamente per l'autenticazione di Administration Server con il nuovo certificato.

Certificati personalizzati

Se necessario, è possibile assegnare un certificato personalizzato per Administration Server. Questo può ad esempio essere necessario per una migliore integrazione con l'infrastruttura PKI esistente dell'azienda o per la configurazione personalizzata dei campi dei certificati.

Il periodo di validità massimo di qualsiasi certificato di Administration Server non deve superare i 397 giorni.

Quando si sostituisce il certificato, tutti i Network Agent che sono stati precedentemente connessi ad Administration Server tramite SSL perderanno la connessione e restituiranno un errore di autenticazione di Administration Server. Per eliminare l'errore, sarà necessario ripristinare la connessione dopo la sostituzione del certificato.

In caso di smarrimento del certificato di Administration Server, è necessario reinstallare il componente Administration Server e ripristinare i dati per recuperarlo.

Se si apre Kaspersky Security Center Web Console in browser diversi e si scarica il file del certificato dell'Administration Server nella finestra delle proprietà dell'Administration Server, i file scaricati hanno nomi diversi.

Requisiti per i certificati personalizzati utilizzati in Kaspersky Security Center

La seguente tabella visualizza i requisiti per i certificati personalizzati specificati per i diversi componenti di Kaspersky Security Center.

Tipo di certificato	Requisiti	Commenti
Certificato comune, certificato di riserva comune ("C", "CR")	Lunghezza minima della chiave: 2048. Vincoli di base: • Vincolo lunghezza percorso: nessuno Utilizzo chiave: • Firma digitale • Firma del certificato • Criptaggio chiavi • Firma CRL Utilizzo chiavi esteso (opzionale): autenticazione del server, autenticazione del client.	Il parametro Utilizzo chiavi esteso è facoltativo. Il valore Vincolo lunghezza percorso può essere un valore intero diverso da "Nessuno", ma non inferiore a 1.
Certificato mobile, certificato di riserva mobile ("M", "MR")	Lunghezza minima della chiave: 2048. Vincoli di base: • CA: true • Vincolo lunghezza percorso: nessuno Utilizzo chiave: • Firma digitale • Firma del certificato • Criptaggio chiavi • Firma CRL Utilizzo chiavi esteso (opzionale): autenticazione del server.	Il parametro Utilizzo chiavi esteso è facoltativo. Il valore Vincolo lunghezza percorso può essere un valore intero diverso da "Nessuno" se il certificato comune ha un valore Vincolo lunghezza percorso non inferiore a 1.
CA certificato per certificati utente generati automaticamente ("MCA")	Lunghezza minima della chiave: 2048. Vincoli di base: • CA: true • Vincolo lunghezza percorso: nessuno Utilizzo chiave: • Firma digitale • Firma del certificato • Criptaggio chiavi • Firma CRL Utilizzo chiavi esteso (opzionale): autenticazione del server, autenticazione del client.	Il parametro Utilizzo chiavi esteso è facoltativo. Il valore Vincolo lunghezza percorso può essere un valore intero diverso da "Nessuno" se il certificato comune ha un valore Vincolo lunghezza percorso non inferiore a 1.
Certificato Server Web	Utilizzo chiavi esteso: autenticazione del server. Il contenitore PKCS #12 / PEM da cui viene specificato il certificato include l'intera catena di chiavi pubbliche. È presente il Nome alternativo soggetto del certificato; quindi il valore del campo `subjectAltName` è valido. Il certificato soddisfa i requisiti effettivi dei browser imposti ai certificati del server, nonché gli attuali requisiti di base del CA/Browser Forum.	—
Certificato di Kaspersky Security Center Web Console	Il contenitore PEM da cui viene specificato il certificato include l'intera catena di chiavi pubbliche. È presente il Nome alternativo soggetto del certificato; quindi il valore del campo `subjectAltName` è valido. Il certificato soddisfa i requisiti effettivi dei browser per i certificati del server, nonché gli attuali requisiti di base del CA/Browser Forum.	I certificati criptati non sono supportati da Kaspersky Security Center Web Console.

Scenario: Specificazione del certificato di Administration Server personalizzato

È possibile assegnare il certificato di Administration Server personalizzato, ad esempio per una migliore integrazione con l'infrastruttura a chiave pubblica (PKI) esistente dell'azienda o per la configurazione personalizzata dei campi del certificato. È consigliabile sostituire il certificato subito dopo l'installazione di Administration Server e prima del completamento dell'Avvio rapido guidato.

Il periodo di validità massimo di qualsiasi certificato di Administration Server non deve superare i 397 giorni.

Prerequisiti

Devono essere soddisfatte le seguenti condizioni:

- Il nuovo certificato deve essere creato nel formato PKCS#12 (ad esempio tramite il PKI dell'organizzazione).
- Per il nuovo certificato devono essere soddisfatti i requisiti elencati nella tabella di seguito.

  Nella tabella seguente, prestare attenzione al requisito "CA: true", che significa che il nuovo certificato deve essere emesso da un'autorità di certificazione (CA) attendibile. Il nuovo certificato con il requisito "CA: true" deve includere l'intera catena di attendibilità e una chiave privata, che deve essere archiviata nel file con estensione pfx o p12.

  Requisiti per i certificati di Administration Server

Tipo di certificato	Requisiti
Certificato comune, certificato di riserva comune ("C", "CR")	Lunghezza minima della chiave: 2048. Vincoli di base: • Vincolo lunghezza percorso: nessuno Il valore Vincolo lunghezza percorso può essere un valore intero diverso da "Nessuno", ma non inferiore a 1. Utilizzo chiave: • Firma digitale • Firma del certificato • Criptaggio chiavi • Firma CRL EKU (Extended Key Usage): autenticazione del server e autenticazione del client. Il parametro EKU è facoltativo, ma se il certificato lo contiene, i dati di autenticazione del server e del client devono essere specificati nell'EKU.
Certificato mobile, certificato di riserva mobile ("M", "MR")	Lunghezza minima della chiave: 2048. Vincoli di base: • CA: true • Vincolo lunghezza percorso: nessuno Il valore Vincolo lunghezza percorso può essere un valore intero diverso da "Nessuno" se il certificato comune ha un valore Vincolo lunghezza percorso non inferiore a 1. Utilizzo chiave: • Firma digitale • Firma del certificato • Criptaggio chiavi • Firma CRL EKU (Extended Key Usage): autenticazione del server. L'EKU è facoltativo, ma se il certificato lo contiene, i dati di autenticazione del server devono essere specificati nell'EKU.
CA certificato per certificati utente generati automaticamente ("MCA")	Lunghezza minima della chiave: 2048. Vincoli di base: • CA: true • Vincolo lunghezza percorso: nessuno Il valore Vincolo lunghezza percorso può essere un valore intero diverso da "Nessuno" se il certificato comune ha un valore Vincolo lunghezza percorso non inferiore a 1. Utilizzo chiave: • Firma digitale • Firma del certificato • Criptaggio chiavi • Firma CRL EKU (Extended Key Usage): autenticazione del client. L'EKU è facoltativo, ma se il certificato lo contiene, i dati di autenticazione del client devono essere specificati nell'EKU.

I certificati rilasciati da un'autorità di certificazione pubblica non dispongono dell'autorizzazione di firma del certificato. Per utilizzare tali certificati, assicurarsi di aver installato Network Agent versione 13 o successiva nei punti di distribuzione o nei gateway di connessione della rete. In caso contrario, non sarà possibile utilizzare i certificati senza l'autorizzazione di firma.

Passaggi

Sono necessari alcuni passaggi per specificare il certificato di Administration Server:

1. **Sostituzione del certificato di Administration Server**

   A tale scopo, utilizzare la riga di comando utilità klsetsrvcert.

2. **Specificazione di un nuovo certificato e ripristino della connessione dei Network Agent ad Administration Server**

   Quando il certificato viene sostituito, tutti i Network Agent precedentemente connessi ad Administration Server tramite SSL perdono la connessione e restituiscono un errore di autenticazione di Administration Server. Per specificare il nuovo certificato e ripristinare la connessione, utilizzare l'utilità klmover della riga di comando.

3. **Specifica di un nuovo certificato nelle impostazioni di Kaspersky Security Center Web Console**

   Dopo aver sostituito il certificato, specificarlo nelle impostazioni di Kaspersky Security Center Web Console. In caso contrario, Kaspersky Security Center Web Console non sarà in grado di connettersi all'Administration Server.

Risultati

Al termine dello scenario, il certificato di Administration Server viene sostituito e il server viene autenticato dai Network Agent nei dispositivi gestiti.

Sostituzione del certificato di Administration Server con l'utilità klsetsrvcert

Per sostituire il certificato di Administration Server:

Dalla riga di comando eseguire la seguente utilità:

```
klsetsrvcert [-t <tipo di certificato> {-i <percorso del nuovo certificato> [-p
<password>] [-o <parametri>] | -g <nome dns>}][-f <ora della sostituzione>][-r
<certificati radice>][-l <percorso file di log>]
```

Non è necessario scaricare l'utilità klsetsrvcert. È inclusa nel kit di distribuzione di Kaspersky Security Center. Non è compatibile con le versioni precedenti di Kaspersky Security Center.

La descrizione dei parametri dell'utilità klsetsrvcert è contenuta nella seguente tabella.

Valori dei parametri dell'utilità klsetsrvcert

Parametro	Valore
`-t <tipo di certificato>`	Tipo del certificato da sostituire. Possibili valori del parametro `<tipo di certificato>`: • `C` – Sostituire il certificato comune per le porte 13000 e 13291. • `CR` – Sostituire il certificato di riserva comune per le porte 13000 e 13291. • `M` – Sostituire il certificato per i dispositivi mobili sulla porta 13292. • `MR` – Sostituire il certificato di riserva mobile per la porta 13292. • `MCA` – Mobile Client CA per certificati utente generati automaticamente.
`-f <ora della sostituzione>`	Pianificazione per la modifica del certificato, utilizzando il formato "GG-MM-AAAA hh:mm" (per le porte 13000 e 13291). Utilizzare questo parametro se si desidera sostituire il certificato comune con il certificato di riserva comune prima della scadenza del certificato comune. Specificare l'ora in cui i dispositivi gestiti devono sincronizzarsi con Administration Server in un nuovo certificato.

Parametro	Valore
`-i <percorso del nuovo certificato>`	Contenitore con il certificato e una chiave privata nel formato PKCS#12 (file con estensione p12 o pfx).
`-p <password>`	Password utilizzata per la protezione del contenitore p12. Il certificato e una chiave privata vengono archiviati nel contenitore, pertanto è necessaria la password per decriptare il file con il contenitore.
`-o <parametri di convalida>`	Parametri di convalida del certificato (separati da punto e virgola). Per utilizzare un certificato personalizzato senza l'autorizzazione di firma, specificare `-o NoCA` nell'utilità klsetsrvcert. Questo è utile per i certificati rilasciati da un'autorità di certificazione pubblica. Per modificare la lunghezza della chiave di criptaggio per i tipi di certificato C o CR, specificare `-o RsaKeyLen:<hezza della chiave>` nell'utilità klsetsrvcert, dove il parametro `<lunghezza della chiave>` è il valore della lunghezza della chiave richiesto. In caso contrario, viene utilizzata la lunghezza della chiave del certificato corrente.
`-g <nome dns>`	Verrà creato un nuovo certificato per il nome DNS specificato.
`-r <certificati radice>`	Elenco delle autorità di certificazione radice attendibili, formato PEM.
`-l <percorso file di registro>`	File di output dei risultati. Per impostazione predefinita, l'output viene reindirizzato nel flusso di output standard.

Per specificare il certificato personalizzato di Administration Server, utilizzare ad esempio il seguente comando:

```
klsetsrvcert -t C -i <percorso del nuovo certificato> -p <password> -o NoCA
```

Dopo la sostituzione del certificato, tutti i Network Agent connessi ad Administration Server tramite SSL perdono la connessione. Per ripristinarla, utilizzare l'utilità klmover della riga di comando.

Per evitare di perdere le connessioni di Network Agent, utilizzare i seguenti comandi:

1. Per installare il nuovo certificato,

   ```
   klsetsrvcert. exe -t CR -i <percorso del nuovo certificato> -p <password> -o NoCA
   ```

2. Per specificare la data in cui verrà applicato il nuovo certificato,

   ```
   klsetsrvcert.exe -f "DD-MM-YYYY hh:mm"
   ```

dove "`DD-MM-YYYY hh:mm`" è la data di 3-4 settimane successive alla data attuale. Lo slittamento temporale per la modifica del certificato in uno nuovo consentirà la distribuzione del nuovo certificato a tutti i Network Agent.

Connessione dei Network Agent ad Administration Server con l'utilità klmover

Dopo aver sostituito il certificato di Administration Server utilizzando l'utilità klsetsrvcert della riga di comando, è necessario stabilire la connessione SSL tra Network Agent e Administration Server in quanto la connessione è interrotta.

Per specificare il nuovo certificato di Administration Server e ripristinare la connessione:

Dalla riga di comando eseguire la seguente utilità:

```
klmover [-address <indirizzo server>] [-pn <numero porta>] [-ps <numero porta SSL>]
[-nossl] [-cert <percorso del file di certificato>]
```

I diritti di amministratore sono necessari per eseguire l'utilità.

Questa utilità viene copiata automaticamente nella cartella di installazione di Network Agent, quando Network Agent viene installato in un dispositivo client.

Per impedire agli intrusi di spostare i dispositivi fuori dal controllo di Administration Server, si consiglia di abilitare la protezione tramite password per l'esecuzione dell'utilità klmover. Per abilitare la protezione con password, selezionare l'opzione **Usa password di disinstallazione** nelle impostazioni dei criteri di Network Agent.

L'utilità klmover richiede i diritti di amministratore locale. La protezione tramite password per l'esecuzione dell'utilità klmover può essere omessa per i dispositivi utilizzati senza diritti di amministratore locale.

L'abilitazione dell'opzione **Usa password di disinstallazione** abilita anche la protezione con password per lo strumento Cleaner (cleaner.exe).

Non è possibile utilizzare l'utilità klmover per i dispositivi client connessi ad Administration Server tramite gateway di connessione. Per tali dispositivi è necessario riconfigurare Network Agent o reinstallarlo e specificare il gateway di connessione.

La descrizione dei parametri dell'utilità klmover è contenuta nella seguente tabella.

Valori dei parametri dell'utilità klmover

Parametro	Valore
`-address <indirizzo server>`	Indirizzo di Administration Server per la connessione. È possibile specificare un indirizzo IP, il nome NetBIOS o il nome DNS.
`-pn <numero di porta>`	Numero della porta tramite la quale viene stabilita la connessione non criptata ad Administration Server. Il numero di porta predefinito è 14000.
`-ps <numero di porta SSL>`	Numero della porta SSL tramite la quale viene stabilita la connessione criptata ad Administration Server utilizzando il protocollo SSL. Il numero di porta predefinito è 13000.
`-nossl`	Utilizza la connessione non criptata ad Administration Server. Se la chiave non è in uso, Network Agent è connesso ad Administration Server tramite il protocollo SSL criptato.
`-cert <percorso del file di certificato>`	Utilizzare il file di certificato specificato per l'autenticazione dell'accesso ad Administration Server.
`-virtserv`	Nome dell'Administration Server virtuale.
`-cloningmode`	Modalità di clonazione del disco di Network Agent Utilizzare uno dei seguenti parametri per configurare la modalità di clonazione del disco: • `-cloningmode`: richiede lo stato della modalità di clonazione del disco. • `-cloningmode 1`: abilita la modalità di clonazione del disco. • `-cloningmode 0`: disabilita la modalità di clonazione del disco.
`-nauninstpwd <password>`	Utilizzare questo parametro per specificare la password di disinstallazione di Network Agent. Il parametro non è obbligatorio.

Ad esempio, per connettere Network Agent ad Administration Server, eseguire il seguente comando:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Riemissione del certificato del server Web

Il certificato Server Web utilizzato in Kaspersky Security Center è necessario per pubblicare i pacchetti di installazione di Network Agent scaricati successivamente nei dispositivi gestiti, nonché per pubblicare profili MDM iOS, app iOS e pacchetti di installazione di Kaspersky Endpoint Security for Mobile. A seconda della configurazione dell'applicazione corrente, vari certificati possono funzionare come certificato del Server Web (per ulteriori dettagli, vedere Informazioni sui certificati di Kaspersky Security Center).

Potrebbe essere necessario riemettere il certificato del Server Web per soddisfare i requisiti di sicurezza specifici della propria organizzazione o per mantenere la connessione continua dei dispositivi gestiti prima di avviare l'aggiornamento dell'applicazione. Kaspersky Security Center offre due modi per riemettere il certificato del Server Web; la scelta tra i due metodi dipende dal fatto che si disponga di dispositivi mobili connessi e gestiti tramite protocollo mobile (ovvero utilizzando il certificato mobile).

Se non è stato mai specificato il certificato personalizzato come certificato del Server Web nella sezione **Server Web** della finestra delle proprietà di Administration Server, il certificato mobile funge da certificato del Server Web. In questo caso, la riemissione del certificato del Server Web viene eseguita attraverso la riemissione del protocollo mobile stesso.

Per riemettere il certificato del Server Web quando non si dispone di dispositivi mobili gestiti tramite il protocollo mobile:

1. Nella struttura della console fare clic con il pulsante destro del mouse sul nome dell'Administration Server pertinente e nel menu di scelta rapida selezionare **Proprietà**.

2. Nella finestra delle proprietà di Administration Server visualizzata, nel riquadro a sinistra selezionare la sezione **Impostazioni di connessione di Administration Server**.

3. Nell'elenco delle sottosezioni selezionare la sottosezione **Certificati**.

4. Se si prevede di continuare a utilizzare il certificato emesso da Kaspersky Security Center, procedere come segue:

   a. Nel riquadro di destra, nel gruppo di impostazioni **Autenticazione Administration Server da parte dei dispositivi mobili**, selezionare l'opzione **Certificato emesso tramite Administration Server** e fare clic sul pulsante **Riemetti**.

   b. Nella finestra **Riemetti certificato** visualizzata, nel gruppo di impostazioni **Indirizzo di connessione** e **Termine di attivazione**, selezionare le opzioni pertinenti e fare clic su **OK**.

   c. Nella finestra di conferma fare clic su **Sì**.

   In alternativa, se si prevede di utilizzare il proprio certificato personalizzato, procedere come segue:

   a. Verificare se il certificato personalizzato soddisfa i requisiti di Kaspersky Security Center e i requisiti per i certificati attendibili di Apple. Se necessario, modificare il certificato.

   b. Selezionare l'opzione **Altro certificato** e fare clic sul pulsante **Sfoglia**.

   c. Nella finestra **Certificato** visualizzata, nel campo **Tipo di certificato**, selezionare il tipo di certificato, quindi specificare le impostazioni e la posizione del certificato:

      - Se è stato selezionato **Contenitore PKCS #12**, fare clic sul pulsante **Sfoglia** accanto al campo **File di certificato** e specificare il file del certificato nel disco rigido. Se il file del certificato è protetto da password, immettere la password nel campo **Password (se presente)**.

      - Se è stato selezionato **Certificato X.509**, fare clic sul pulsante **Sfoglia** accanto al campo **Chiave privata (.prk, .pem)** e specificare la chiave privata nel disco rigido. Se la chiave privata è protetta da password, immettere la password nel campo **Password (se presente)**. Quindi fare clic sul pulsante **Sfoglia** accanto al campo **Chiave pubblica (.cer)** e specificare la chiave privata nel disco rigido.

   d. Nella finestra **Certificato** fare clic su **OK**.

   e. Nella finestra di conferma fare clic su **Sì**.

   Il certificato mobile viene riemesso per essere utilizzato come certificato del Server Web.

Per riemettere il certificato del Server Web quando si dispone di dispositivi mobili gestiti tramite il protocollo mobile:

1. Generare il certificato personalizzato e preparalo per l'utilizzo in Kaspersky Security Center. Verificare se il certificato personalizzato soddisfa i requisiti di Kaspersky Security Center e i requisiti per i certificati attendibili di Apple. Se necessario, modificare il certificato.

   È possibile utilizzare l'utilità kliossrvcertgen.exe per la generazione del certificato.

2. Nella struttura della console fare clic con il pulsante destro del mouse sul nome dell'Administration Server pertinente e nel menu di scelta rapida selezionare **Proprietà**.

3. Nel riquadro a sinistra della finestra delle proprietà di Administration Server visualizzata selezionare la sezione **Server Web**.

4. Nel menu **Tramite HTTPS** selezionare l'opzione **Specifica un altro certificato**.

5. Nel menu **Tramite HTTPS** fare clic sul pulsante **Cambia**.

6. Nella finestra **Certificato** visualizzata, nel campo **Tipo di certificato** selezionare il tipo di certificato:

   - Se è stato selezionato **Contenitore PKCS #12**, fare clic sul pulsante **Sfoglia** accanto al campo **File di certificato** e specificare il file del certificato nel disco rigido. Se il file del certificato è protetto da password, immettere la password nel campo **Password (se presente)**.

   - Se è stato selezionato **Certificato X.509**, fare clic sul pulsante **Sfoglia** accanto al campo **Chiave privata (.prk, .pem)** e specificare la chiave privata nel disco rigido. Se la chiave privata è protetta da password, immettere la password nel campo **Password (se presente)**. Quindi fare clic sul pulsante **Sfoglia** accanto al campo **Chiave pubblica (.cer)** e specificare la chiave privata nel disco rigido.

7. Nella finestra **Certificato** fare clic su **OK**.

8. Se necessario, nella finestra delle proprietà di Administration Server, nel campo **Porta HTTPS del server Web** modificare il numero della porta HTTPS per il Server Web. Fare clic su **OK**.

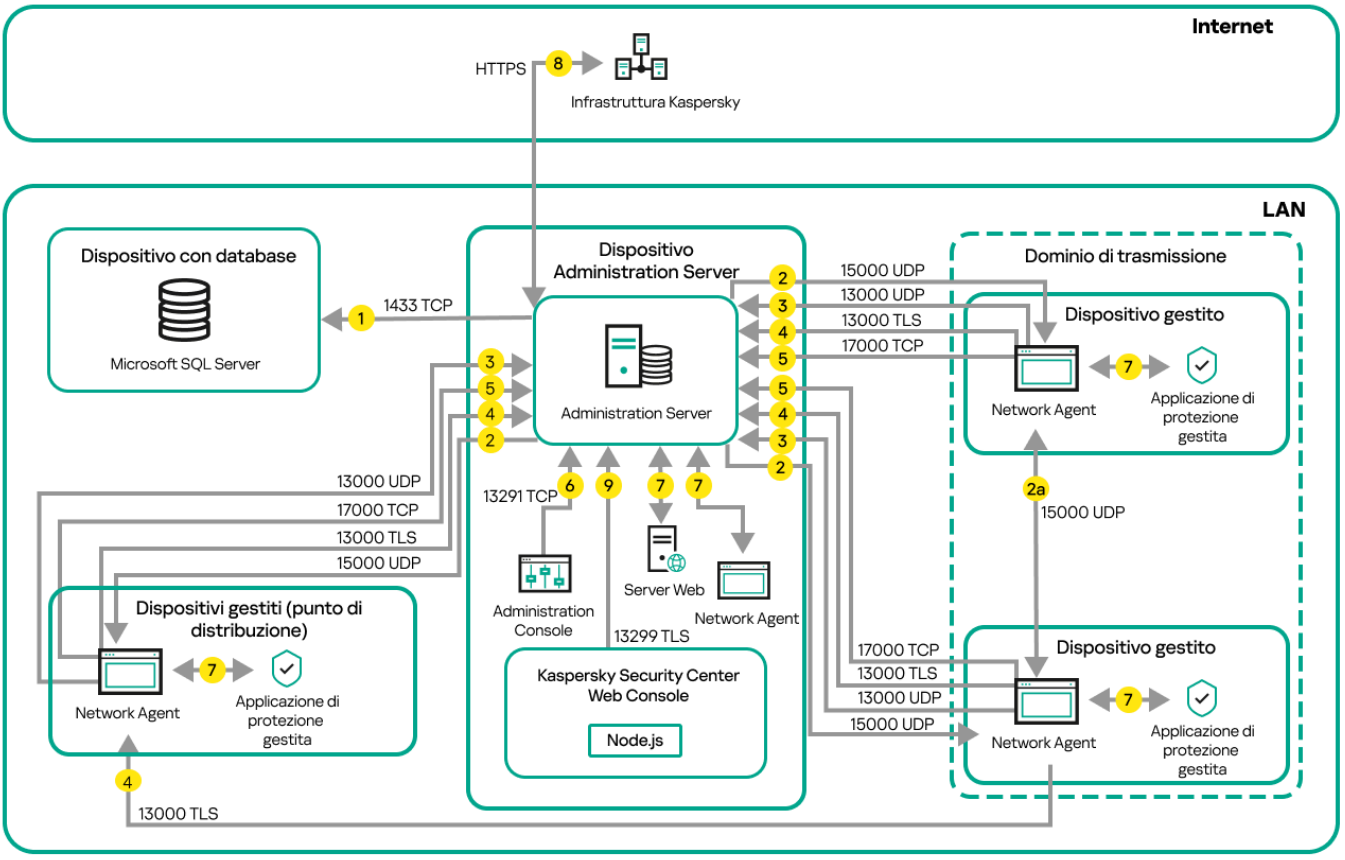
   Il certificato del Server Web viene riemesso.

Schemi per traffico dati e utilizzo delle porte

Questa sezione fornisce schemi per il traffico dati tra i componenti di Kaspersky Security Center, le applicazioni di protezione gestite e i server esterni in varie configurazioni. Gli schemi vengono forniti con i numeri delle porte che devono essere disponibili nei dispositivi locali.

Administration Server e dispositivi gestiti nella LAN

La figura di seguito mostra il traffico dati se Kaspersky Security Center è distribuito solo in una LAN (Local Area Network).



Administration Server e i dispositivi gestiti in una LAN (Local Area Network)

La figura illustra come diversi dispositivi gestiti si connettono all'Administration Server in modi differenti: direttamente o tramite un punto di distribuzione. I punti di distribuzione riducono il carico sull'Administration Server durante la distribuzione degli aggiornamenti e ottimizzano il traffico di rete. Tuttavia, i punti di distribuzione sono necessari solo se il numero di dispositivi gestiti è sufficientemente elevato. Se il numero di dispositivi gestiti è limitato, i dispositivi gestiti possono ricevere gli aggiornamenti direttamente dall'Administration Server.

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL o la porta 1433 per Microsoft SQL Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

   Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

   Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

   > Il punto di distribuzione era denominato "Update Agent" nelle versioni precedenti di Kaspersky Security Center.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. I dati dell'Administration Console basata su MMC vengono trasferiti ad Administration Server tramite la porta 13291. L'Administration Console può essere installata nello stesso dispositivo o in un altro dispositivo.

7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

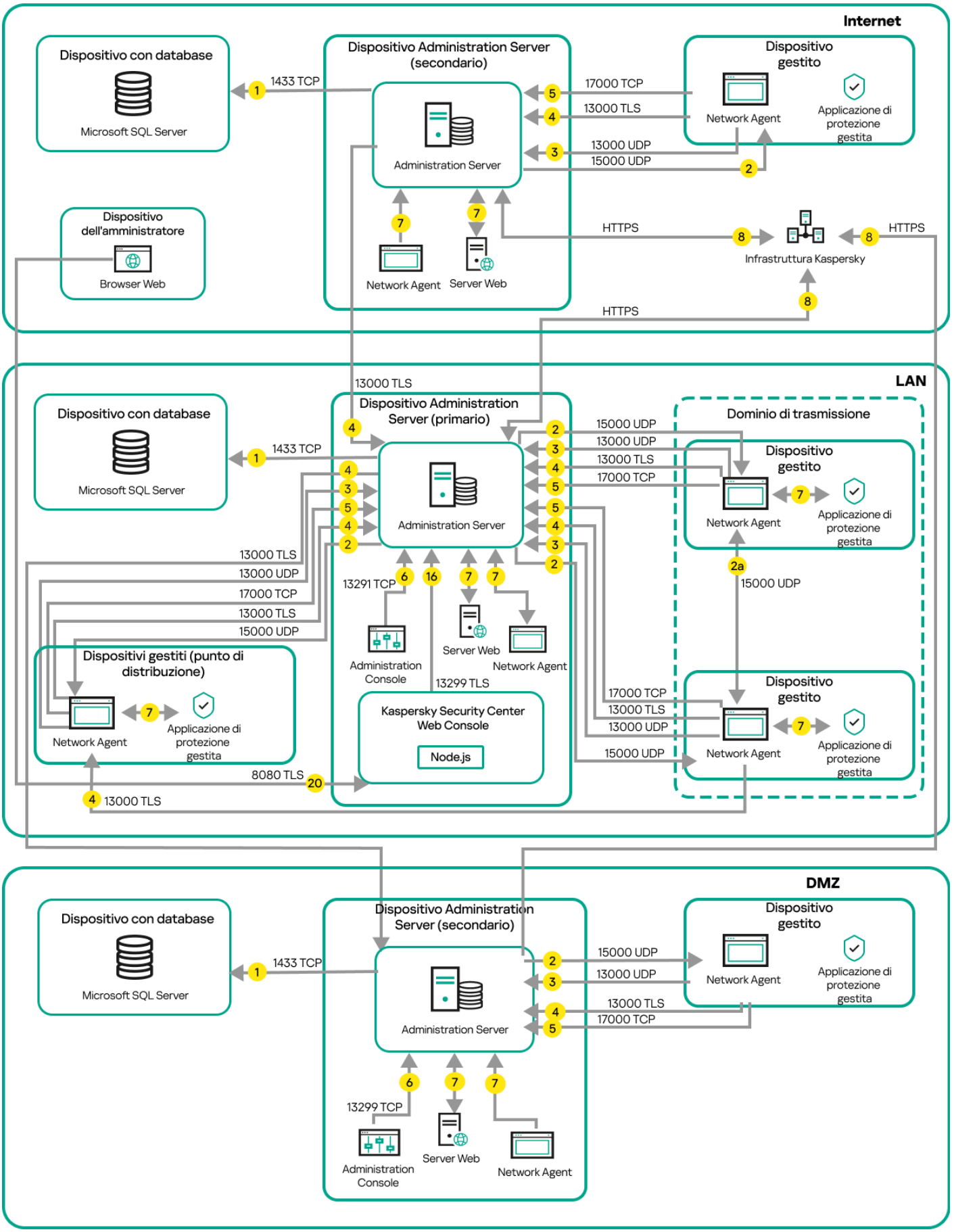
8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

9. Kaspersky Security Center Web Console Server invia i dati ad Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

Administration Server primario nella LAN e due Administration Server secondari

La figura di seguito mostra la gerarchia degli Administration Server: l'Administration Server primario si trova in una LAN. Un Administration Server secondario si trova in una rete perimetrale; un altro Administration Server secondario si trova in Internet.



Gerarchia degli Administration Server: Administration Server primario e due Administration Server secondari

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL o la porta 1433 per Microsoft SQL Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

   Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

   Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

   > Il punto di distribuzione era denominato "Update Agent" nelle versioni precedenti di Kaspersky Security Center.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. I dati dell'Administration Console basata su MMC vengono trasferiti ad Administration Server tramite la porta 13291. L'Administration Console può essere installata nello stesso dispositivo o in un altro dispositivo.

7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

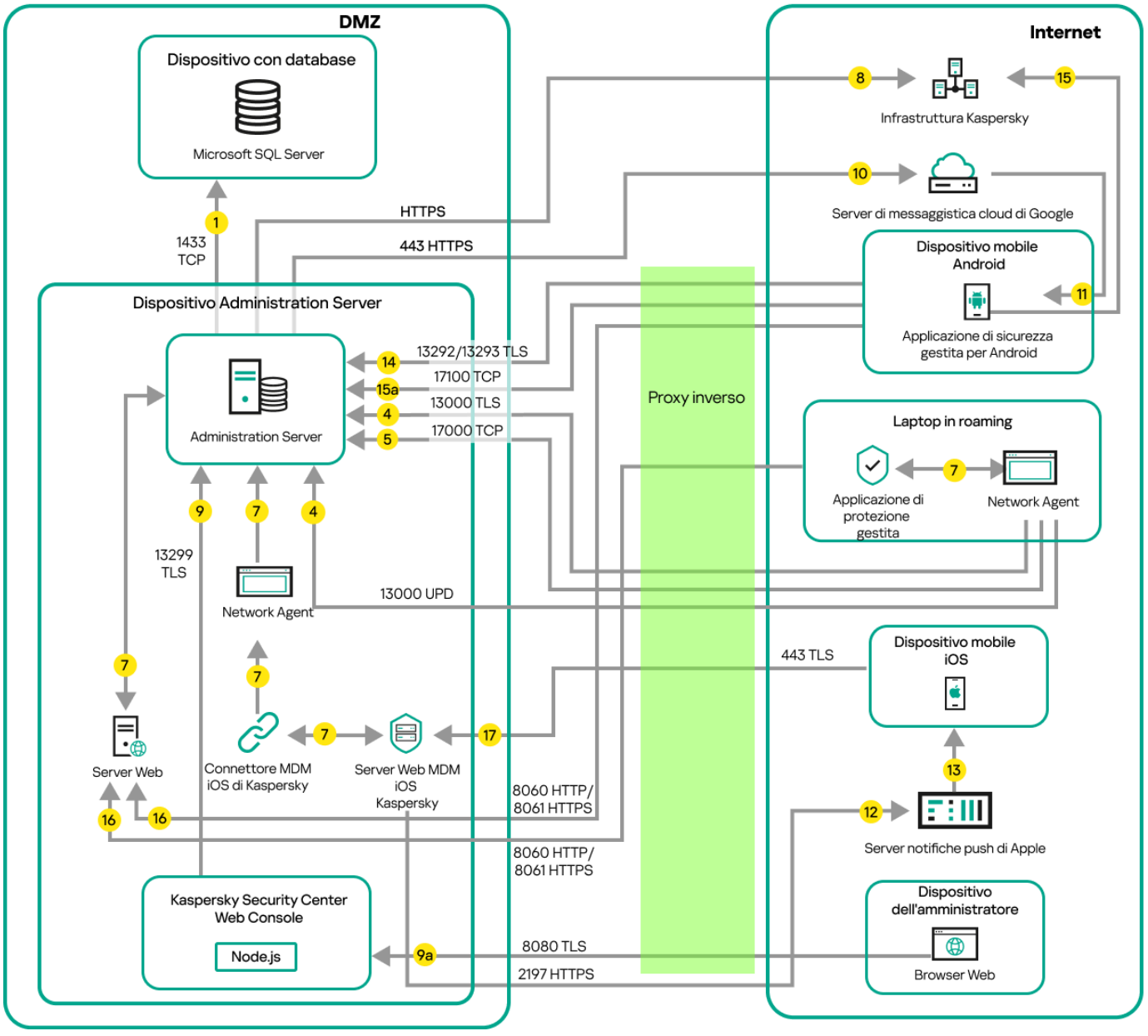
   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

9. Kaspersky Security Center Web Console Server invia i dati all'Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

   9a. I dati provenienti dal browser, installato in un altro dispositivo dell'amministratore, vengono trasferiti a Kaspersky Security Center Web Console Server tramite la porta TLS 8080. Kaspersky Security Center Web Console Server può essere installato in Administration Server o in un altro dispositivo.

Administration Server nella LAN, dispositivi gestiti in Internet, proxy inverso in uso

La figura di seguito mostra il traffico dati se Administration Server si trova all'interno di una LAN e i dispositivi gestiti, inclusi i dispositivi mobili, sono in Internet. In questa figura, è in uso un proxy inverso a scelta. Per informazioni dettagliate, fare riferimento alla documentazione dell'applicazione.



Administration Server in una LAN; i dispositivi gestiti si connettono all'Administration Server tramite un proxy inverso

Questo schema di distribuzione è consigliabile se non si desidera che i dispositivi mobili si connettano direttamente all'Administration Server e non si desidera assegnare un gateway di connessione nella rete perimetrale.

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL o la porta 1433 per Microsoft SQL Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

   Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

   Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

   > Il punto di distribuzione era denominato "Update Agent" nelle versioni precedenti di Kaspersky Security Center.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. I dati dell'Administration Console basata su MMC vengono trasferiti ad Administration Server tramite la porta 13291. L'Administration Console può essere installata nello stesso dispositivo o in un altro dispositivo.

7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

9. Kaspersky Security Center Web Console Server invia i dati all'Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

   9a. I dati provenienti dal browser, installato in un altro dispositivo dell'amministratore, vengono trasferiti a Kaspersky Security Center Web Console Server tramite la porta TLS 8080. Kaspersky Security Center Web Console Server può essere installato in Administration Server o in un altro dispositivo.

10. Solo per i dispositivi mobili Android: i dati provenienti dall'Administration Server vengono trasferiti ai server Google. Questa connessione viene utilizzata per segnalare ai dispositivi mobili Android che è necessaria la connessione all'Administration Server. Successivamente vengono inviate le notifiche push ai dispositivi mobili.

11. Solo per i dispositivi mobili Android: le notifiche push provenienti dai server Google vengono inviate al dispositivo mobile. Questa connessione viene utilizzata per segnalare ai dispositivi mobili che è necessaria la connessione all'Administration Server.

12. Solo per i dispositivi mobili iOS: i dati provenienti dal server per dispositivi mobili MDM iOS vengono trasferiti ai server per le notifiche push Apple. Successivamente vengono inviate le notifiche push ai dispositivi mobili.

13. Solo per i dispositivi mobili iOS: le notifiche push vengono inviate dai server Apple al dispositivo mobile. Questa connessione viene utilizzata per segnalare ai dispositivi mobili iOS che è necessaria la connessione all'Administration Server.

14. Solo per i dispositivi mobili: i dati provenienti dall'applicazione gestita vengono trasferiti ad Administration Server (o al gateway di connessione) tramite la porta TLS 13292 / 13293, direttamente o tramite un proxy inverso.

15. Solo per i dispositivi mobili: i dati provenienti dal dispositivo mobile vengono trasferiti all'infrastruttura Kaspersky.

    Se un dispositivo mobile non ha accesso a Internet, i dati vengono trasferiti all'Administration Server tramite la porta 17100 e l'Administration Server invia tali dati all'infrastruttura Kaspersky; tuttavia, questo scenario viene applicato molto raramente.

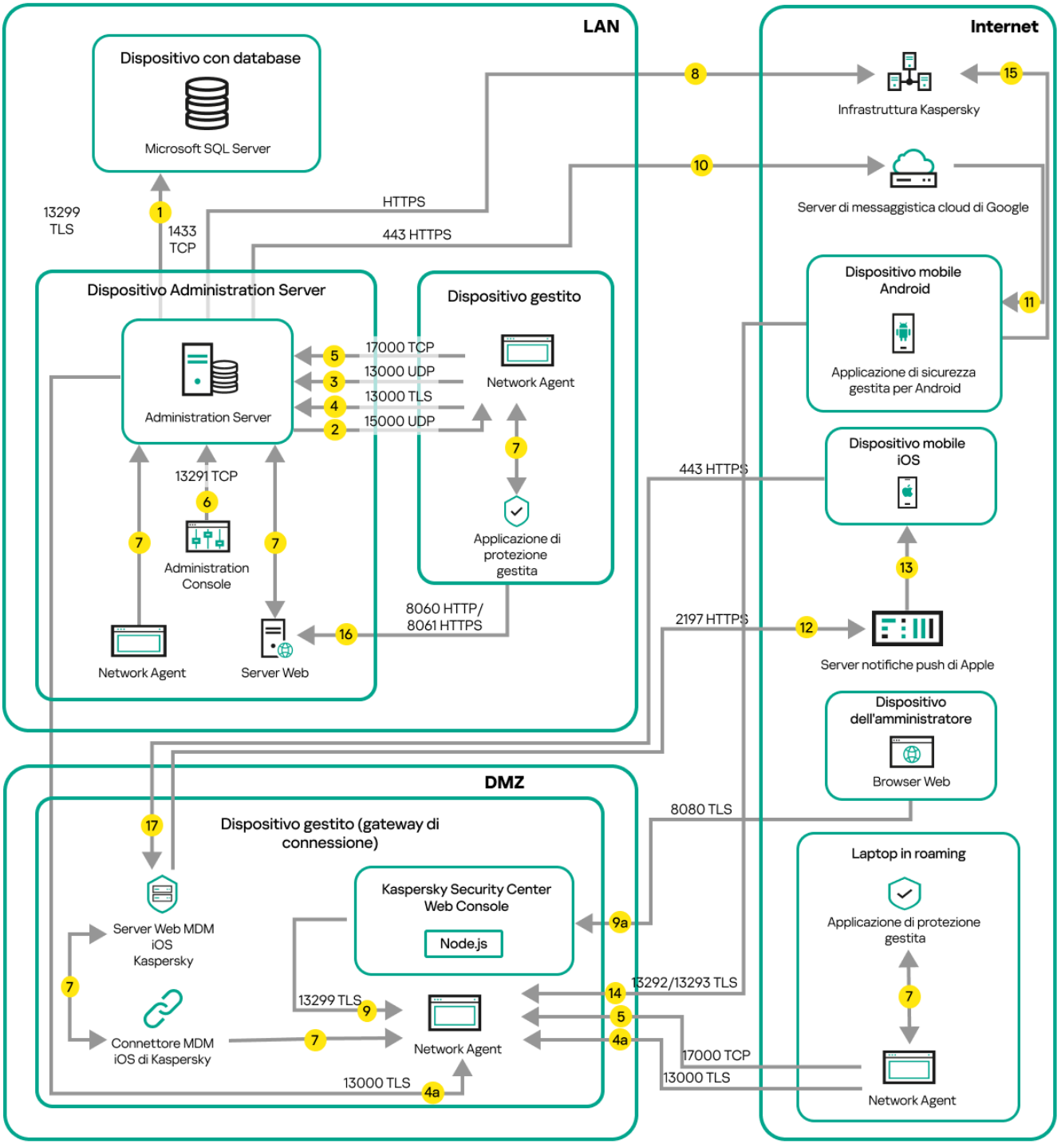
16. Le richieste di pacchetti provenienti dai dispositivi gestiti, inclusi i dispositivi mobili, vengono trasferite al server Web, che si trova nello stesso dispositivo in cui si trova Administration Server.

17. Solo per i dispositivi mobili iOS: i dati dal dispositivo mobile vengono trasferiti tramite la porta TLS 443 al server MDM iOS, che si trova sullo stesso dispositivo dell'Administration Server o sul gateway di connessione.

Administration Server nella LAN, dispositivi gestiti in Internet, gateway di connessione in uso

La figura di seguito mostra il traffico dati se Administration Server si trova all'interno di una LAN e i dispositivi gestiti, inclusi i dispositivi mobili, sono in Internet. È in uso un gateway di connessione.

Questo schema di distribuzione è consigliabile se non si desidera che i dispositivi mobili si connettano direttamente all'Administration Server e non si desidera utilizzare un proxy inverso o un firewall aziendale.



Dispositivi mobili gestiti connessi all'Administration Server tramite un gateway di connessione

In questa figura i dispositivi gestiti sono connessi all'Administration Server tramite un gateway di connessione che si trova nella rete perimetrale. Non è in uso alcun proxy inverso o firewall aziendale.

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL o la porta 1433 per Microsoft SQL Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

   Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

   Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

   > Il punto di distribuzione era denominato "Update Agent" nelle versioni precedenti di Kaspersky Security Center.

   4a. Anche un gateway di connessione nella rete perimetrale riceve la connessione da Administration Server tramite la porta TLS 13000. Dal momento che un gateway di connessione nella rete perimetrale non può raggiungere le porte di Administration Server, Administration Server crea e mantiene una connessione di segnale permanente con un gateway di connessione. La connessione di segnale non viene utilizzata per il trasferimento dei dati; viene utilizzata solo per inviare un invito all'interazione di rete. Quando deve connettersi al server, il gateway di connessione invia una notifica al server attraverso questa connessione di segnale, quindi il server crea la connessione richiesta per il trasferimento dei dati.

   Anche i dispositivi fuori sede si connettono al gateway di connessione tramite la porta TLS 13000.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. I dati dell'Administration Console basata su MMC vengono trasferiti ad Administration Server tramite la porta 13291. L'Administration Console può essere installata nello stesso dispositivo o in un altro dispositivo.

7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

9. Kaspersky Security Center Web Console Server invia i dati all'Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

   9a. I dati provenienti dal browser, installato in un altro dispositivo dell'amministratore, vengono trasferiti a Kaspersky Security Center Web Console Server tramite la porta TLS 8080. Kaspersky Security Center Web Console Server può essere installato in Administration Server o in un altro dispositivo.

10. Solo per i dispositivi mobili Android: i dati provenienti dall'Administration Server vengono trasferiti ai server Google. Questa connessione viene utilizzata per segnalare ai dispositivi mobili Android che è necessaria la connessione all'Administration Server. Successivamente vengono inviate le notifiche push ai dispositivi mobili.

11. Solo per i dispositivi mobili Android: le notifiche push provenienti dai server Google vengono inviate al dispositivo mobile. Questa connessione viene utilizzata per segnalare ai dispositivi mobili che è necessaria la connessione all'Administration Server.

12. Solo per i dispositivi mobili iOS: i dati provenienti dal server per dispositivi mobili MDM iOS vengono trasferiti ai server per le notifiche push Apple. Successivamente vengono inviate le notifiche push ai dispositivi mobili.

13. Solo per i dispositivi mobili iOS: le notifiche push vengono inviate dai server Apple al dispositivo mobile. Questa connessione viene utilizzata per segnalare ai dispositivi mobili iOS che è necessaria la connessione all'Administration Server.

14. Solo per i dispositivi mobili: i dati provenienti dall'applicazione gestita vengono trasferiti ad Administration Server (o al gateway di connessione) tramite la porta TLS 13292 / 13293, direttamente o tramite un proxy inverso.

15. Solo per i dispositivi mobili: i dati provenienti dal dispositivo mobile vengono trasferiti all'infrastruttura Kaspersky.

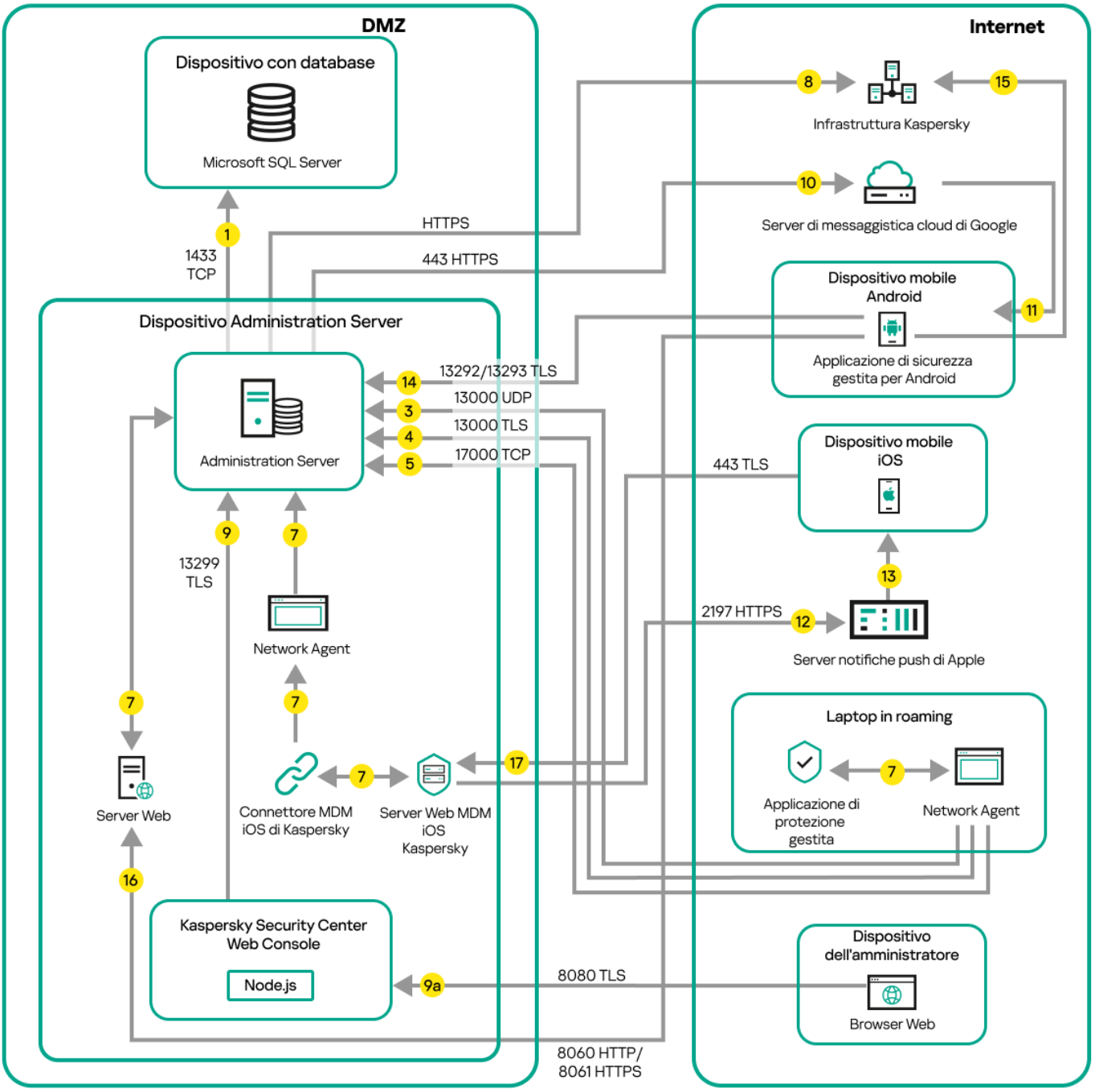
    Se un dispositivo mobile non ha accesso a Internet, i dati vengono trasferiti all'Administration Server tramite la porta 17100 e l'Administration Server invia tali dati all'infrastruttura Kaspersky; tuttavia, questo scenario viene applicato molto raramente.

16. Le richieste di pacchetti provenienti dai dispositivi gestiti, inclusi i dispositivi mobili, vengono trasferite al server Web, che si trova nello stesso dispositivo in cui si trova Administration Server.

17. Solo per i dispositivi mobili iOS: i dati dal dispositivo mobile vengono trasferiti tramite la porta TLS 443 al server MDM iOS, che si trova sullo stesso dispositivo dell'Administration Server o sul gateway di connessione.

Administration Server all'interno della rete perimetrale, dispositivi gestiti in Internet

La figura di seguito mostra il traffico dati se l'Administration Server si trova nella rete perimetrale (DMZ) e i dispositivi gestiti, inclusi i dispositivi mobili, sono in Internet.



Administration Server nella rete perimetrale, dispositivi mobili gestiti in Internet

In questa figura non è in uso alcun gateway di connessione: i dispositivi mobili si connettono direttamente all'Administration Server.

Le frecce indicano l'origine del traffico: ogni freccia punta da un dispositivo che avvia la connessione al dispositivo che "risponde" alla chiamata. Vengono forniti il numero della porta e il nome del protocollo utilizzato per il trasferimento dei dati. Ogni freccia ha un'etichetta numerica e i dettagli sul traffico dati corrispondente sono i seguenti:

1. Administration Server invia i dati al database. Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL o la porta 1433 per Microsoft SQL Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2. Le richieste di comunicazione provenienti da Administration Server vengono trasferite a tutti i dispositivi gestiti non mobili tramite la porta UDP 15000.

   I Network Agent inviano richieste reciproche con un solo dominio di trasmissione. I dati vengono quindi inviati ad Administration Server e utilizzati per definire i limiti del dominio di trasmissione e per l'assegnazione automatica dei punti di distribuzione (se questa opzione è abilitata).

   Se Administration Server non ha accesso diretto ai dispositivi gestiti, le richieste di comunicazione da Administration Server a questi dispositivi non vengono inviate direttamente.

3. Le informazioni sull'arresto dei dispositivi gestiti vengono trasferite dal Network Agent all'Administration Server tramite la porta UDP 13000.

4. Administration Server riceve la connessione dai Network Agent e dagli Administration Server secondari tramite la porta TLS 13000.

   Se è stata utilizzata una versione precedente di Kaspersky Security Center, l'Administration Server nella rete può ricevere la connessione dai Network Agent tramite la porta non TLS 14000. Kaspersky Security Center supporta la connessione dei Network Agent anche tramite la porta 14000, ma è consigliabile utilizzare la porta TLS 13000.

   > Il punto di distribuzione era denominato "Update Agent" nelle versioni precedenti di Kaspersky Security Center.

5. I dispositivi gestiti (ad eccezione dei dispositivi mobili) richiedono l'attivazione tramite la porta TCP 17000. Ciò non è necessario se il dispositivo dispone già dell'accesso a Internet; in tal caso il dispositivo invia i dati ai server Kaspersky direttamente via Internet.

6. I dati dell'Administration Console basata su MMC vengono trasferiti ad Administration Server tramite la porta 13291. L'Administration Console può essere installata nello stesso dispositivo o in un altro dispositivo.

7. Nelle applicazioni presenti in un singolo dispositivo avviene lo scambio di traffico locale (nell'Administration Server o in un dispositivo gestito). Non è necessaria l'apertura di porte esterne.

8. Il dati inviati dall'Administration Server ai server Kaspersky (ad esempio, i dati KSN o le informazioni sulle licenze) e i dati inviati dai server Kaspersky all'Administration Server (ad esempio, gli aggiornamenti delle applicazioni e dei database anti-virus) vengono trasferiti tramite il protocollo HTTPS.

   Se non si desidera concedere all'Administration Server l'accesso a Internet, è necessario gestire questi dati manualmente.

9. Kaspersky Security Center Web Console Server invia i dati all'Administration Server, che può essere installato nello stesso dispositivo o in un altro dispositivo, tramite la porta TLS 13299.

   9a. I dati provenienti dal browser, installato in un altro dispositivo dell'amministratore, vengono trasferiti a Kaspersky Security Center Web Console Server tramite la porta TLS 8080. Kaspersky Security Center Web Console Server può essere installato in Administration Server o in un altro dispositivo.

10. Solo per i dispositivi mobili Android: i dati provenienti dall'Administration Server vengono trasferiti ai server Google. Questa connessione viene utilizzata per segnalare ai dispositivi mobili Android che è necessaria la connessione all'Administration Server. Successivamente vengono inviate le notifiche push ai dispositivi mobili.

11. Solo per i dispositivi mobili Android: le notifiche push provenienti dai server Google vengono inviate al dispositivo mobile. Questa connessione viene utilizzata per segnalare ai dispositivi mobili che è necessaria la connessione all'Administration Server.

12. Solo per i dispositivi mobili iOS: i dati provenienti dal server per dispositivi mobili MDM iOS vengono trasferiti ai server per le notifiche push Apple. Successivamente vengono inviate le notifiche push ai dispositivi mobili.

13. Solo per i dispositivi mobili iOS: le notifiche push vengono inviate dai server Apple al dispositivo mobile. Questa connessione viene utilizzata per segnalare ai dispositivi mobili iOS che è necessaria la connessione all'Administration Server.

14. Solo per i dispositivi mobili: i dati provenienti dall'applicazione gestita vengono trasferiti ad Administration Server (o al gateway di connessione) tramite la porta TLS 13292 / 13293, direttamente o tramite un proxy inverso.

15. Solo per i dispositivi mobili: i dati provenienti dal dispositivo mobile vengono trasferiti all'infrastruttura Kaspersky.

    Se un dispositivo mobile non ha accesso a Internet, i dati vengono trasferiti all'Administration Server tramite la porta 17100 e l'Administration Server invia tali dati all'infrastruttura Kaspersky; tuttavia, questo scenario viene applicato molto raramente.

16. Le richieste di pacchetti provenienti dai dispositivi gestiti, inclusi i dispositivi mobili, vengono trasferite al server Web, che si trova nello stesso dispositivo in cui si trova Administration Server.

17. Solo per i dispositivi mobili iOS: i dati dal dispositivo mobile vengono trasferiti tramite la porta TLS 443 al server MDM iOS, che si trova sullo stesso dispositivo dell'Administration Server o sul gateway di connessione.

Interazione dei componenti di Kaspersky Security Center e delle applicazioni di protezione: ulteriori informazioni

In questa sezione vengono forniti gli schemi per l'interazione dei componenti di Kaspersky Security Center e delle applicazioni di protezione gestite. Gli schemi forniscono i numeri delle porte che devono essere disponibili e i nomi dei processi che aprono tali porte.

Convenzioni utilizzate negli schemi di interazione

Nella seguente tabella sono fornite le convenzioni utilizzate negli schemi.

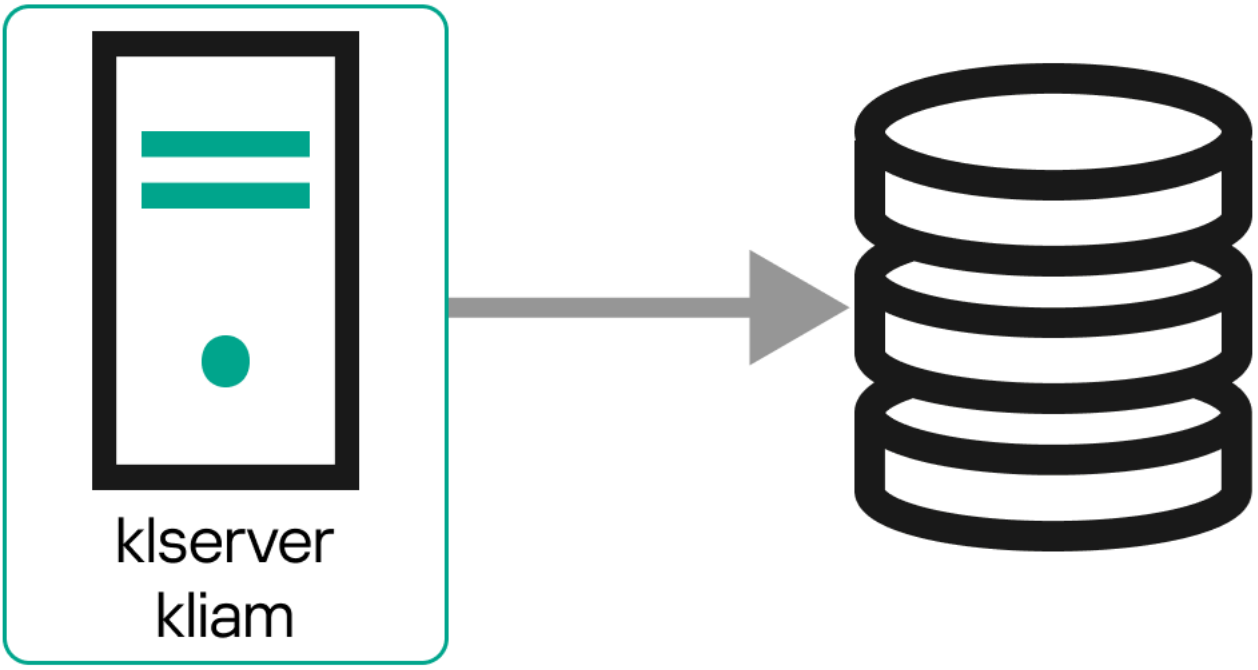
Convenzioni utilizzate nella documentazione

Icona	Significato
	Administration Server

	Administration Server secondario
	DBMS
	Dispositivo client (in cui sono installati Network Agent e un'applicazione della famiglia Kaspersky Endpoint Security o un'altra applicazione di protezione che può essere gestita da Kaspersky Security Center)
	Gateway di connessione
	Punto di distribuzione
	Dispositivo client mobile con Kaspersky Security for Mobile
	Browser nel dispositivo dell'utente
	Processo in esecuzione nel dispositivo e apertura di una porta
	Porta e relativo numero
	Traffico TCP (la direzione della freccia indica la direzione del flusso di traffico)
	Traffico UDP (la direzione della freccia indica la direzione del flusso di traffico)
	COM invoke
	Trasporto DBMS
	Limite della rete perimetrale

Administration Server e DBMS

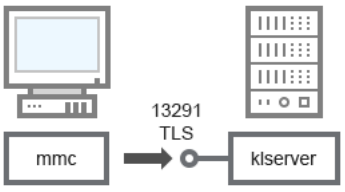
I dati di Administration Server vengono inseriti nel database SQL Server, MySQL o MariaDB.



Administration Server e DBMS

Se si installa l'Administration Server e il database in diversi dispositivi, è necessario rendere disponibili le porte necessarie nel dispositivo in cui si trova il database (ad esempio la porta 3306 per il server MySQL o la porta 1433 per Microsoft SQL Server). Fare riferimento alla documentazione DBMS per le informazioni attinenti.

Administration Server e Administration Console



Administration Server e Administration Console

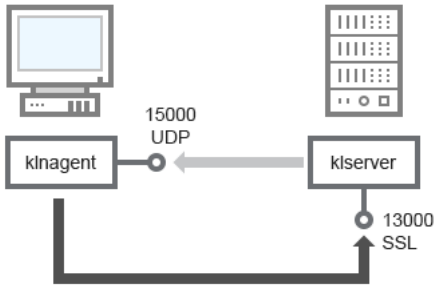
Per dettagli sullo schema, vedere la tabella di seguito.

Administration Server e Administration Console (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	TLS	Ambito della porta
Administration Server	13291	klserver	TCP	Sì	Ricezione delle connessioni da Administration Console

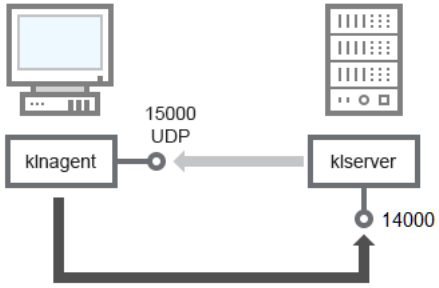
Administration Server e dispositivo client: gestione dell'applicazione di protezione

L'Administration Server riceve la connessione dai Network Agent tramite la porta SSL 13000 (vedere la figura seguente).



Administration Server e dispositivo client: gestione dell'applicazione di protezione, connessione tramite la porta 13000 (consigliata)

Se è stata utilizzata una versione precedente di Kaspersky Security Center, Administration Server nella rete può ricevere connessioni dai Network Agent tramite la porta non SSL 14000 (vedere la figura seguente). Anche Kaspersky Security Center 15.1 supporta la connessione dei Network Agent tramite la porta 14000, anche se è consigliabile utilizzare la porta SSL 13000.



Administration Server e dispositivo client: gestione dell'applicazione di protezione, connessione tramite la porta 14000 (protezione inferiore)

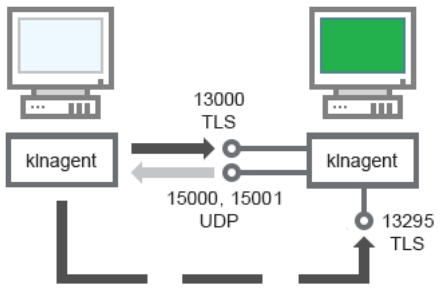
Per le spiegazioni degli schemi, vedere la tabella seguente.

Administration Server e dispositivo client: gestione dell'applicazione di protezione (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	TLS (solo per TCP)	Ambito della porta
Network Agent	15000	klnagent	UDP	Null	Multicasting per Network Agent
Administration Server	13000	klserver	TCP	Sì	Ricezione delle connessioni dai Network Agent
Administration Server	14000	klserver	TCP	No	Ricezione delle connessioni dai Network Agent

Upgrade del software in un dispositivo client tramite un punto di distribuzione

Il dispositivo client si connette al punto di distribuzione tramite la porta 13000 e, se si utilizza il punto di distribuzione come server push, anche tramite la porta 13295; il punto di distribuzione esegue la distribuzione multicast ai Network Agent tramite la porta 15000 (vedere la figura seguente). Gli aggiornamenti e i pacchetti di installazione vengono ricevuti da un punto di distribuzione tramite la porta 15001.



Upgrade del software in un dispositivo client tramite un punto di distribuzione

Per dettagli sullo schema, vedere la tabella di seguito.

Upgrade del software tramite un punto di distribuzione (traffico)

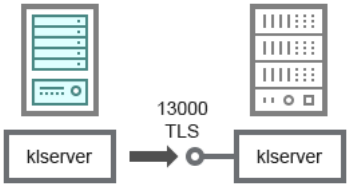
Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	TLS (solo per TCP)	Ambito della porta
Network Agent	15000	klnagent	UDP	Null	Multicasting per Network Agent
Network Agent	15001	klnagent	UDP	Null	Ricezione di aggiornamenti e pacchetti di installazione da un punto di distribuzione
Punto di distribuzione	13000	klnagent	TCP	Sì	Ricezione delle connessioni dai Network Agent
Punto di distribuzione	13295	klnagent	TCP	Sì	Ricezione delle connessioni dai dispositivi client (tramite il server push)

Gerarchia di Administration Server: Administration Server primario e Administration Server secondario

Lo schema (vedere la figura seguente) illustra come utilizzare la porta 13000 per garantire l'interazione tra più Administration Server combinati in una gerarchia.

Quando si combinano due Administration Server in una gerarchia, verificare che la porta 13291 sia accessibile in entrambi gli Administration Server. Administration Console si connette ad Administration Server tramite la porta 13291.

Successivamente, una volta che gli Administration Server sono combinati in una gerarchia, sarà possibile amministrarli entrambi utilizzando Administration Console connesso all'Administration Server primario. Di conseguenza, l'unico prerequisito è l'accessibilità della porta 13291 dell'Administration Server primario.



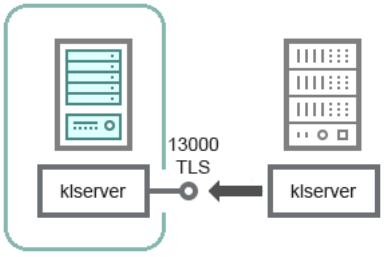
Gerarchia di Administration Server: Administration Server primario e Administration Server secondario

Per dettagli sullo schema, vedere la tabella di seguito.

Gerarchia di Administration Server (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	TLS	Ambito della porta
Administration Server primario	13000	klserver	TCP	Sì	Ricezione delle connessioni dagli Administration Server secondari

Gerarchia di Administration server con un Administration Server secondario nella rete perimetrale



Gerarchia di Administration server con un Administration Server secondario nella rete perimetrale

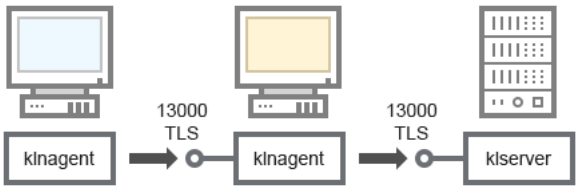
Lo schema illustra una gerarchia di Administration Server in cui l'Administration Server secondario disponibile nella rete perimetrale riceve una connessione dall'Administration Server primario (vedere la tabella seguente per le spiegazioni dello schema). Quando si combinano due Administration Server in una gerarchia, verificare che la porta 13291 sia accessibile in entrambi gli Administration Server. Administration Console si connette ad Administration Server tramite la porta 13291.

Successivamente, una volta che gli Administration Server sono combinati in una gerarchia, sarà possibile amministrarli entrambi utilizzando Administration Console connesso all'Administration Server primario. Di conseguenza, l'unico prerequisito è l'accessibilità della porta 13291 dell'Administration Server primario.

Gerarchia di Administration Server con un Administration Server secondario nella rete perimetrale (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	TLS	Ambito della porta
Administration Server secondario	13000	klserver	TCP	Sì	Ricezione delle connessioni dall'Administration Server primario

Administration Server, un gateway di connessione in un segmento di rete e un dispositivo client



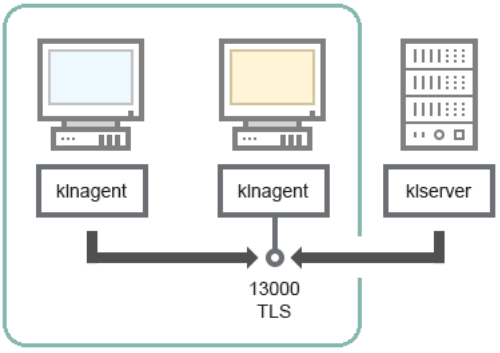
Administration Server, un gateway di connessione in un segmento di rete e un dispositivo client

Per dettagli sullo schema, vedere la tabella di seguito.

Administration Server, un gateway di connessione in un segmento di rete e un dispositivo client (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	TLS	Ambito della porta
Administration Server	13000	klserver	TCP	Sì	Ricezione delle connessioni dai Network Agent
Network Agent	13000	klnagent	TCP	Sì	Ricezione delle connessioni dai Network Agent

Administration Server e due dispositivi nella rete perimetrale: un gateway di connessione e un dispositivo client



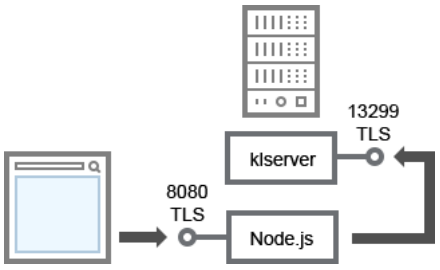
Administration Server con un gateway di connessione e un dispositivo client nella rete perimetrale

Per dettagli sullo schema, vedere la tabella di seguito.

Administration Server con un gateway di connessione in un segmento di rete e un dispositivo client (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	TLS	Ambito della porta
Network Agent	13000	klnagent	TCP	Sì	Ricezione delle connessioni dai Network Agent

Administration Server e Kaspersky Security Center Web Console



Administration Server e Kaspersky Security Center Web Console

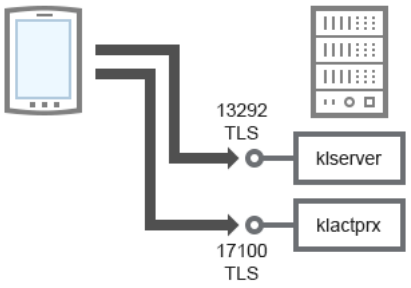
Per dettagli sullo schema, vedere la tabella di seguito.

Administration Server e Kaspersky Security Center Web Console (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	TLS	Ambito della porta
Administration Server	13299	klserver	TCP	Sì	Ricezione delle connessioni da Kaspersky Security Center Web Console ad Administration Server tramite OpenAPI
Kaspersky Security Center Web Console Server o Administration Server	8080	Node.js: Server-side JavaScript	TCP	Sì	Ricezione delle connessioni da Kaspersky Security Center Web Console

Kaspersky Security Center Web Console può essere installato in Administration Server o in un altro dispositivo.

Attivazione e gestione dell'applicazione di protezione in un dispositivo mobile



Attivazione e gestione dell'applicazione di protezione in un dispositivo mobile

Per dettagli sullo schema, vedere la tabella di seguito.

Attivazione e gestione dell'applicazione di protezione in un dispositivo mobile (traffico)

Dispositivo	Numero di porta	Nome del processo che apre la porta	Protocollo	TLS	Ambito della porta
Administration Server	13292	klserver	TCP	Sì	Ricezione delle connessioni da Administration Console ad Administration Server
Administration Server	17100	klactprx	TCP	Sì	Ricezione delle connessioni per l'attivazione dell'applicazione dai dispositivi mobili

Best practice per la distribuzione

Kaspersky Security Center è un'applicazione distribuita. Kaspersky Security Center include le seguenti applicazioni:

- Administration Server - Il componente principale, progettato per la gestione dei dispositivi di un'organizzazione e l'archiviazione dei dati in un sistema DBMS.
- Administration Console - Lo strumento di base per l'amministratore. Administration Console è distribuito insieme ad Administration Server, ma può anche essere installato singolarmente in uno o più dispositivi eseguiti dall'amministratore.
- Network Agent – Utilizzato per gestire l'applicazione di protezione installata in un dispositivo, nonché per ottenere informazioni sul dispositivo e per trasferire queste informazioni ad Administration Server. I Network Agent vengono installati nei dispositivi di un'organizzazione.

La distribuzione di Kaspersky Security Center nella rete di un'organizzazione viene eseguita come segue:

- Installazione di Administration Server
- Installazione di Administration Console nel dispositivo dell'amministratore
- Installazione di Network Agent e dell'applicazione di protezione nei dispositivi dell'organizzazione

Guida all'hardening

Kaspersky Security Center è progettato per l'esecuzione centralizzata delle attività di base di amministrazione e manutenzione nella rete di un'organizzazione. L'applicazione fornisce all'amministratore l'accesso a informazioni dettagliate sul livello di sicurezza della rete dell'organizzazione. Kaspersky Security Center consente di configurare tutti i componenti della protezione creati utilizzando le applicazioni Kaspersky.

Kaspersky Security Center Administration Server ha accesso completo alla gestione della protezione dei dispositivi client ed è il componente più importante del sistema di sicurezza dell'organizzazione. Pertanto, per Administration Server sono necessari metodi di protezione avanzati.

Prima della configurazione, creare una copia di backup di Kaspersky Security Center Administration Server utilizzando l'attività Backup dei dati di Administration Server o l'utilità klbackup e salvarla in una posizione sicura.

Nella Guida all'hardening, sono descritti i suggerimenti e le caratteristiche della configurazione di Kaspersky Security Center e dei suoi componenti, intesi a ridurre i rischi di compromissione.

La Guida all'hardening contiene le seguenti informazioni:

- Selezione dell'architettura di Administration Server
- Configurazione di una connessione sicura ad Administration Server
- Configurazione degli account per l'accesso ad Administration Server

- Gestione della protezione di Administration Server
- Gestione della protezione dei dispositivi client
- Configurazione della protezione per le applicazioni gestite
- Manutenzione di Administration Server
- Trasferimento di informazioni ad applicazioni di terzi
- Suggerimenti sulla sicurezza per i sistemi informativi di terze parti

Distribuzione di Administration Server

Architettura di Administration Server

In generale, la scelta di un'architettura di gestione centralizzata dipende dalla posizione dei dispositivi protetti, dall'accesso da reti adiacenti, dagli schemi di distribuzione degli aggiornamenti del database e così via.

Nella fase iniziale dello sviluppo dell'architettura, si consiglia di familiarizzare con i componenti di Kaspersky Security Center e con le modalità di interazione tra essi, così come con gli schemi per il traffico dati e l'utilizzo delle porte.

Sulla base di queste informazioni, è possibile formare un'architettura che specifichi:

- La posizione di Administration Server e le connessioni di rete
- L'organizzazione delle aree di lavoro dell'amministratore e i metodi di connessione ad Administration Server
- I metodi di distribuzione per Network Agent e il software di protezione
- L'utilizzo dei punti di distribuzione
- L'utilizzo di Administration Server virtuali
- L'utilizzo di una gerarchia di Administration Server
- Lo schema di aggiornamento del database anti-virus
- Altri flussi informativi

Selezione di un dispositivo per l'installazione di Administration Server

Si consiglia di installare Administration Server in un server dedicato nell'infrastruttura dell'organizzazione. Se nel server non è installato altro software di terzi, è possibile configurare le impostazioni di sicurezza in base ai requisiti di Kaspersky Security Center, senza dipendere dai requisiti del software di terzi.

È possibile distribuire Administration Server in un server fisico o in un server virtuale. Verificare che il dispositivo selezionato soddisfi i requisiti hardware e software.

Posizione dell'Administration Server

I dispositivi gestiti da Administration Server possono essere posizionati come segue:

- Su una rete locale (LAN)
- Su internet
- Nella zona perimetrale (DMZ)

Al contempo, Administration Server può trovarsi anche in diversi segmenti: industriale, aziendale e DMZ.

Se si utilizza Kaspersky Security Center per gestire la protezione di un segmento di rete isolato, si consiglia di distribuire Administration Server in un segmento della zona perimetrale (DMZ). In questo modo, è possibile organizzare una corretta segmentazione della rete e ridurre al minimo il flusso di traffico verso il segmento protetto, mantenendo al contempo le funzionalità di gestione completa e la distribuzione degli aggiornamenti.

Limitazione della distribuzione di Administration Server in un controller di dominio, un server terminal o un dispositivo utente

Si sconsiglia vivamente di installare Administration Server in un controller di dominio, un server terminal o un dispositivo utente.

Si consiglia di fornire la separazione funzionale dei nodi chiave di rete. Questo approccio consente di mantenere l'operatività di diversi sistemi quando un nodo si guasta o è compromesso. Al contempo, è possibile creare diversi criteri di sicurezza per ciascun nodo.

Ad esempio, le limitazioni di sicurezza generalmente applicate a un controller di dominio possono ridurre significativamente le prestazioni di Administration Server e rendere impossibile l'utilizzo di alcune funzionalità di Administration Server. Se un intruso ottiene l'accesso privilegiato al controller di dominio, il database di AD DS (Active Directory Domain Services) può essere modificato, danneggiato o distrutto. Inoltre, tutti i sistemi e gli account gestiti da Active Directory possono essere compromessi.

Account per l'installazione e l'esecuzione di Administration Server

Si consiglia di eseguire l'installazione di Administration Server con un account amministratore locale per evitare di utilizzare account di dominio per accedere al database di Administration Server. Un set di account richiesti e i loro diritti dipende dal tipo di DBMS selezionato, dalla posizione del DBMS e dal metodo di creazione del database di Administration Server.

Durante l'installazione di Kaspersky Security Center vengono creati automaticamente i gruppi KLAdmins e KLOperators. A questi gruppi vengono concesse le autorizzazioni per la connessione ad Administration Server e per l'elaborazione dei relativi oggetti.

A seconda del tipo di account utilizzato per l'installazione di Kaspersky Security Center, i gruppi KLAdmins e KLOperators vengono creati come segue:

- Se l'applicazione è installata tramite un account utente incluso in un dominio, i gruppi vengono creati sia nel dispositivo Administration Server che nel dominio che include l'Administration Server.
- Se l'applicazione è installata tramite un account di sistema, i gruppi vengono creati soltanto nel dispositivo Administration Server.

Per evitare di creare i gruppi KLAdmins e KLOperators nel dominio e, di conseguenza, **fornire i privilegi per gestire Administration Server a un account esterno al dispositivo Administration Server**, si consiglia di installare Kaspersky Security Center con un account locale.

Durante l'installazione di Administration Server, selezionare l'account che verrà utilizzato per avviare Administration Server come servizio. Per impostazione predefinita, l'applicazione crea un account locale denominato KL-AK-*, con il quale verrà eseguito il servizio Administration Server (il servizio klserver).

Se necessario, il servizio Administration Server può essere eseguito con l'account selezionato. A questo account devono essere concessi i diritti richiesti per accedere al DBMS. Per motivi di sicurezza, utilizzare un account senza privilegi per eseguire il servizio Administration Server.

Per evitare l'uso di impostazioni dell'account errate, si consiglia di generare l'account automaticamente.

Esclusione di Administration Server da un dominio

Se si utilizza Administration Server per proteggere gruppi di dispositivi di importanza critica, si sconsiglia di includere il dispositivo Administration Server nel dominio. In questo modo, è possibile differenziare i diritti di gestione di Kaspersky Security Center e impedire l'accesso ad Administration Server nel caso in cui l'account di dominio venga compromesso.

Tenere presente che se si installa Administration Server in un dispositivo incluso nel gruppo di lavoro, i seguenti scenari di utilizzo di Administration Server non saranno disponibili:

- Utilizzo di un cluster di failover Kaspersky Security Center
- Utilizzo di un cluster di failover di Windows Server
- Utilizzo di SQL Server per Windows in un dispositivo separato

  È possibile utilizzare SQL Server per Windows in un dispositivo separato solo se Administration Server e SQL Server si trovano nello stesso dominio o in domini attendibili. Se Administration Server, SQL Server e una condivisione UNC per i backup si trovano in un gruppo di lavoro, non è possibile configurare in modo sicuro i diritti di accesso e di lettura-scrittura tra SQL Server e la condivisione.
- Installazione remota con gli strumenti di Administration Server tramite i criteri di gruppo di Active Directory

Se è necessario disconnettere Administration Server dal dominio Active Directory, attenersi alla procedura descritta nell'argomento: Come modificare il nome di Kaspersky Security Center.

Se è necessario installare Administration Server in un dispositivo incluso nel gruppo di lavoro, è possibile utilizzare anche Kaspersky Security Center Linux anziché Kaspersky Security Center Windows.

Sicurezza della connessione

Utilizzo di TLS

Si consiglia di vietare le connessioni non sicure ad Administration Server. Ad esempio, è possibile vietare le connessioni che utilizzano HTTP nelle impostazioni di Administration Server.

Si noti che, per impostazione predefinita, diverse porte HTTP di Administration Server sono chiuse. La porta rimanente viene utilizzata per il server Web di Administration Server (8060). Questa porta può essere limitata dalle impostazioni del firewall del dispositivo Administration Server.

Impostazioni TLS rigorose

Si consiglia di utilizzare il protocollo TLS versione 1.2 e successive e di limitare o vietare gli algoritmi di criptaggio non sicuri.

È possibile configurare i protocolli di criptaggio (TLS) utilizzati da Administration Server. Si noti che al momento del rilascio di una versione di Administration Server, le impostazioni del protocollo di criptaggio sono configurate per impostazione predefinita per garantire un trasferimento sicuro dei dati.

Divieto di autenticazione remota tramite account Windows

È possibile utilizzare il contrassegno LP_RestrictRemoteOsAuth per vietare le connessioni SSPI da indirizzi remoti. Questo contrassegno consente di vietare l'autenticazione remota in Administration Server utilizzando account Windows locali o di dominio.

Per commutare il contrassegno LP_RestrictRemoteOsAuth nella modalità di divieto delle connessioni dagli indirizzi remoti:

1. Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

2. Eseguire il comando riportato di seguito nella riga di comando per specificare il valore del contrassegno LP_RestrictRemoteOsAuth:

   ```
   klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
   ```

3. Riavviare il servizio Administration Server.

Il contrassegno LP_RestrictRemoteOsAuth non funziona se l'autenticazione remota viene eseguita tramite Kaspersky Security Center Web Console o Administration Console installato nel dispositivo Administration Server.

Limitazione dell'accesso al database di Administration Server

Si consiglia di limitare l'accesso al database di Administration Server. Ad esempio, concedere l'accesso solo dal dispositivo Administration Server. In questo modo, si riduce la probabilità che il database di Administration Server venga compromesso a causa di vulnerabilità note.

È possibile configurare i parametri in base alle istruzioni operative del database utilizzato, nonché fornire porte chiuse sui firewall.

Autenticazione di Microsoft SQL Server

Se Kaspersky Security Center utilizza Microsoft SQL Server come DBMS, è necessario proteggere i dati di Kaspersky Security Center trasferiti da o verso il database e i dati archiviati nel database da accessi non autorizzati. A tale scopo, è necessario fornire comunicazione sicura tra Kaspersky Security Center e SQL Server. Il modo più affidabile per garantire comunicazioni sicure è installare Kaspersky Security Center e SQL Server nello stesso dispositivo e utilizzare il meccanismo di memoria condivisa per entrambe le applicazioni. In tutti gli altri casi, è consigliabile utilizzare un certificato SSL/TLS per autenticare l'istanza di SQL Server.

In genere, Administration Server può indirizzare SQL Server tramite i seguenti provider:

- SQLOLEDB tramite TCP/IP o Named Pipe

  Questo provider è installato nel sistema operativo Windows e utilizzato per impostazione predefinita.

- MSOLEDBSQL tramite TCP/IP, Named Pipe o Memoria condivisa

  Se si desidera utilizzare questo provider, è necessario installarlo nel dispositivo con Administration Server, quindi impostare il valore `1` sulla variabile di ambiente globale `KLDBADO_UseMSOLEDBSQL`.

- MSOLEDBSQL19 utilizzando TCP/IP, Named Pipe o Memoria condivisa

  Se si desidera utilizzare questo provider, è necessario installarlo nel dispositivo con Administration Server, quindi impostare il valore `1` sulla variabile di ambiente globale `KLDBADO_UseMSOLEDBSQL` e il valore `MSOLEDBSQL19` nella variabile di ambiente globale `KLDBADO_ProviderName`.

Inoltre, prima di utilizzare TCP/IP, Named Pipe o Memoria condivisa, verificare che il protocollo richiesto sia abilitato.

Interazione di sicurezza con un DBMS esterno

Se il DBMS è installato in un dispositivo separato durante l'installazione di Administration Server (DBMS esterno), si consiglia di configurare i parametri per l'interazione sicura e l'autenticazione con questo DBMS. Per ulteriori informazioni sulla configurazione dell'autenticazione SSL, fare riferimento a Autenticazione di PostgreSQL Server e Scenario: Autenticazione di MySQL Server.

Configurazione di una lista di indirizzi IP consentiti per la connessione ad Administration Server

Per impostazione predefinita, gli utenti di Kaspersky Security Center possono accedere a Kaspersky Security Center da qualsiasi dispositivo in cui sono installate le applicazioni Kaspersky Security Center Administration Console basato su MMC, Kaspersky Security Center Web Console oppure OpenAPI. È possibile configurare Administration Server in modo che gli utenti possano connettersi ad esso solo da dispositivi con indirizzi IP consentiti. Ad esempio, se un intruso tenta di connettersi a Kaspersky Security Center tramite Kaspersky Security Center Web Console Server installato su un dispositivo non incluso nella lista consentiti, non sarà in grado di accedere a Kaspersky Security Center.

Configurazione di una lista di indirizzi IP consentiti per connettersi a Kaspersky Security Center Web Console

Per impostazione predefinita, gli utenti di Kaspersky Security Center possono connettersi a Kaspersky Security Center Web Console da qualsiasi dispositivo. Su un dispositivo in cui è installato Kaspersky Security Center Web Console, è necessario configurare il firewall (integrato nel sistema operativo o di terze parti) in modo che gli utenti possano connettersi a Kaspersky Security Center Web Console solo da indirizzi IP consentiti.

Sicurezza della connessione al controller di dominio durante il polling

Administration Server o un punto di distribuzione Linux si connettono al controller di dominio tramite LDAPS per eseguire il polling del dominio. Per impostazione predefinita, la verifica del certificato non è richiesta durante la connessione. Per imporre la verifica del certificato, impostare il contrassegno `KLNAG_LDAP_TLS_REQCERT` su 1. È inoltre possibile specificare un percorso personalizzato all'autorità di certificazione (CA) per accedere alla catena di certificati utilizzando il contrassegno `KLNAG_LDAP_SSL_CACERT`.

Account e autenticazione

Prima di eseguire i seguenti passaggi, creare una copia di backup di Kaspersky Security Center Administration Server utilizzando Backup dei dati di Administration Server o l'utilità klbackup e salvarla in una posizione sicura.

Utilizzo della verifica in due passaggi con Administration Server

Kaspersky Security Center fornisce la verifica in due passaggi per gli utenti di Kaspersky Security Center Web Console e Administration Console, basata sullo standard RFC 6238 (algoritmo TOTP, Time-based One-time Password).

Quando la verifica in due passaggi è abilitata per il proprio account, ogni volta che si accede a Kaspersky Security Center Web Console o Administration Console è necessario immettere il nome utente, la password e un codice di sicurezza monouso aggiuntivo. Se si utilizza l'autenticazione del dominio per il proprio account, è sufficiente immettere un codice di sicurezza monouso aggiuntivo. Per ricevere un codice di sicurezza monouso è necessario installare un'app di autenticazione nel computer o nel dispositivo mobile.

Esistono autenticatori software e hardware (token) che supportano lo standard RFC 6238. Ad esempio, gli autenticatori software includono Google Authenticator, Microsoft Authenticator, FreeOTP.

Si sconsiglia vivamente di installare l'app di autenticazione nello stesso dispositivo da cui viene stabilita la connessione ad Administration Server. È possibile installare un'app di autenticazione nel dispositivo mobile.

Limitare i nuovi utenti a impostare la verifica in due passaggi per se stessi.

Per migliorare ulteriormente la protezione dell'accesso a Kaspersky Security Center Web Console, è possibile impedire ai nuovi utenti di impostare autonomamente la verifica in due passaggi.

Quando questa opzione è abilitata, un utente con la verifica in due passaggi disabilitata, ad esempio un nuovo amministratore di dominio, non può configurare autonomamente la verifica in due passaggi. Pertanto, tale utente non può essere autenticato in Administration Server e non può accedere a Kaspersky Security Center Web Console senza l'approvazione di un altro amministratore di Kaspersky Security Center che ha già abilitato la verifica in due passaggi.

Utilizzo dell'autenticazione a due fattori per un sistema operativo

Si consiglia di utilizzare l'autenticazione a più fattori (MFA) per l'autenticazione nel dispositivo Administration Server utilizzando un token, una smart card o un altro metodo (se possibile).

Limitare il salvataggio della password amministratore

Se si utilizza Administration Console, si sconsiglia di salvare la password dell'amministratore nella finestra di dialogo di connessione di Administration Server.

Se si utilizza Kaspersky Security Center Web Console, si sconsiglia di salvare la password amministratore nel browser installato nel dispositivo dell'utente.

Autenticazione di un account utente interno

Per impostazione predefinita, la password di un account utente interno di Administration Server deve rispettare le seguenti regole:

- La password deve avere una lunghezza compresa tra 8 e 256 caratteri.
- La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
  - Lettere maiuscole (A-Z)
  - Lettere minuscole (a-z)
  - Numeri (0-9)
  - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- La password non deve contenere spazi, caratteri Unicode o la combinazione di "." e "@", quando "." si trova prima di "@".

Per impostazione predefinita, il numero massimo di tentativi di immissione della password consentiti è 10. È possibile modificare il numero di tentativi di immissione della password consentiti.

L'utente di Kaspersky Security Center può immettere una password non valida un numero limitato di volte. Una volta raggiunto il limite, l'account utente viene bloccato per un'ora.

Configurazione delle opzioni per la modifica della password di un account utente interno

Si consiglia di configurare le seguenti opzioni per modificare la password di un account utente interno:

- Periodo di rotazione della password
- Ora dell'avviso preliminare sulla necessità di modificare la password
- Valore dell'opzione **L'utente deve modificare la password al primo accesso**

Protezione dell'account dalle modifiche non autorizzate

Si consiglia di abilitare un'opzione aggiuntiva per proteggere un account utente interno di Administration Server da modifiche non autorizzate. Questa protezione deve essere configurata separatamente per ogni utente interno.

Gruppo di amministrazione dedicato per Administration Server

Si consiglia di creare un gruppo di amministrazione dedicato per Administration Server. Concedere a questo gruppo diritti di accesso speciali e creare un criterio di sicurezza speciale per lo stesso.

Per evitare di abbassare intenzionalmente il livello di sicurezza di Administration Server, si consiglia di limitare l'elenco degli account che possono gestire il gruppo di amministrazione dedicato.

I gruppi KLAdmins e KLOperators

Durante l'installazione di Kaspersky Security Center vengono creati automaticamente i gruppi KLAdmins e KLOperators. Al gruppo KLAdmins vengono concessi tutti i diritti di accesso. Al gruppo KLOperators sono concessi solo i diritti di lettura ed esecuzione. I diritti concessi al gruppo KLAdmins sono **bloccati**.

È possibile visualizzare i gruppi KLAdmins e KLOperators e apportare modifiche a questi utilizzando gli strumenti di amministrazione standard del sistema operativo.

Quando si sviluppano i regolamenti per l'utilizzo di Administration Server, è necessario determinare se lo specialista della sicurezza delle informazioni richiede l'accesso completo (e l'inclusione nel gruppo KLAdmins) per eseguire le attività standard.

La maggior parte delle attività amministrative di base può essere distribuita tra reparti aziendali (o diversi dipendenti dello stesso reparto) e di conseguenza tra diversi account. In Kaspersky Security Center, è inoltre possibile impostare la differenziazione dell'accesso ai gruppi di amministrazione. Di conseguenza, è possibile implementare uno scenario in cui l'autorizzazione per gli account del gruppo KLAdmins sarà anomala e potrebbe essere considerata un incidente.

Se Kaspersky Security Center è stato installato con un account di sistema, i gruppi vengono creati solo nel dispositivo Administration Server. In questo caso, si consiglia di verificare che nel gruppo siano incluse solo le voci create durante l'installazione di Kaspersky Security Center. Si sconsiglia di aggiungere gli eventuali gruppi al gruppo KLAdmins (locale e/o di dominio) creato automaticamente durante l'installazione di Kaspersky Security Center. È inoltre necessario limitare i diritti per modificare questo gruppo. Il gruppo KLAdmins deve includere solo singoli account senza privilegi.

Se l'installazione è stata eseguita con un account utente di dominio, i gruppi KLAdmins e KLOperators vengono creati sia in Administration Server che nel dominio che include Administration Server. Si consiglia un approccio simile come l'installazione di un account locale.

Limitazione dell'appartenenza al ruolo di amministratore principale

Si consiglia di limitare l'appartenenza al ruolo di amministratore principale.

Per impostazione predefinita, dopo l'installazione di Administration Server, il ruolo di amministratore principale viene assegnato al gruppo di amministratori locali e al gruppo KLAdmins creato. È utile per la gestione, ma è fondamentale dal punto di vista della sicurezza, poiché il ruolo di amministratore principale ha una vasta gamma di privilegi. L'assegnazione di questo ruolo agli utenti dovrebbe essere strettamente regolamentata.

Gli amministratori locali possono essere esclusi dall'elenco di utenti con privilegi di amministratore di Kaspersky Security Center. Il ruolo di amministratore principale non può essere rimosso dal gruppo KLAdmins. È possibile includere nel gruppo KLAdmins gli account che verranno utilizzati per gestire Administration Server.

Se si utilizza l'autenticazione del dominio, si consiglia di limitare i privilegi degli account amministratore di dominio in Kaspersky Security Center. Per impostazione predefinita, questi account hanno il ruolo di amministratore principale. Inoltre, un amministratore di dominio può includere il proprio account nel gruppo KLAdmins per ottenere il ruolo di amministratore principale. Per evitare questo, nelle impostazioni di sicurezza di Kaspersky Security Center è possibile aggiungere il gruppo Domain Users e quindi definire le relative regole di divieto. Queste regole devono avere la precedenza su quelle di autorizzazione.

È inoltre possibile utilizzare i ruoli utente predefiniti con un set di diritti già configurato.

Configurazione dei diritti di accesso alle funzionalità dell'applicazione

Si consiglia di utilizzare una configurazione flessibile dei diritti di accesso alle funzionalità di Kaspersky Security Center per ciascun utente o gruppo di utenti.

Il controllo degli accessi in base al ruolo consente la creazione di ruoli utente standard con un set di diritti predefinito e l'assegnazione di tali ruoli agli utenti sulla base dell'ambito delle relative mansioni lavorative.

Principali vantaggi del modello di controllo degli accessi in base al ruolo:

- Amministrazione semplificata
- Gerarchia dei ruoli
- Approccio con privilegio minimo
- Separazione dei compiti

È possibile assegnare ruoli predefiniti a determinati dipendenti in base alle loro posizioni o creare ruoli completamente nuovi.

Durante la configurazione dei ruoli, prestare attenzione ai privilegi associati alla modifica dello stato della protezione del dispositivo Administration Server e all'installazione remota di software di terzi:

- Gestione dei gruppi di amministrazione.
- Operazioni con Administration Server.
- Installazione remota.
- Modifica dei parametri per l'archiviazione di eventi e l'invio delle notifiche.

  Questo privilegio consente di impostare notifiche che eseguono uno script o un modulo eseguibile nel dispositivo Administration Server quando si verifica un evento.

Account separato per l'installazione remota delle applicazioni

Oltre alla differenziazione di base dei diritti di accesso, si consiglia di limitare l'installazione remota delle applicazioni per tutti gli account (ad eccezione dell'amministratore principale o di un altro account specializzato).

Si consiglia di utilizzare un account separato per l'installazione remota delle applicazioni. È possibile assegnare un ruolo o autorizzazioni all'account separato.

Protezione degli accessi privilegiati di Windows

Si consiglia di consultare i suggerimenti di Microsoft per garantire la sicurezza degli accessi privilegiati. Per visualizzare questi suggerimenti, consultare l'articolo Protezione degli accessi privilegiati.

Uno dei punti chiave dei suggerimenti è l'implementazione di workstation ad accesso privilegiato (PAW, Privileged Access Workstation).

Utilizzo di un account MSA (Managed Service Account) o di account gMSA (group Managed Service Account) per eseguire il servizio Administration Server

Active Directory dispone di un tipo speciale di account per l'esecuzione sicura dei servizi, denominati MSA/gMSA. Kaspersky Security Center supporta gli account MSA e gli account gMSA. Se nel dominio vengono utilizzati questi tipi di account, è possibile selezionarne uno come account del servizio Administration Server.

Controllo periodico di tutti gli utenti e delle azioni degli utenti

Si consiglia di eseguire un controllo periodico di tutti gli utenti sul dispositivo Administration Server. In questo modo, è possibile rispondere a determinati tipi di minacce alla sicurezza associate alla possibile compromissione del dispositivo.

È inoltre possibile monitorare le azioni degli utenti, ad esempio la connessione e la disconnessione da Administration Server, la connessione ad Administration Server con un errore e la modifica degli oggetti (per gli oggetti che supportano la gestione delle revisioni).

Gestione della protezione di Administration Server

Selezione di un software di protezione di Administration Server

A seconda del tipo di distribuzione di Administration Server e della strategia di protezione generale, selezionare l'applicazione per proteggere il dispositivo Administration Server.

Se si distribuisce Administration Server in un dispositivo dedicato, si consiglia di selezionare l'applicazione Kaspersky Endpoint Security per proteggere il dispositivo Administration Server. In questo modo, è possibile applicare tutte le tecnologie disponibili per proteggere il dispositivo Administration Server, inclusi i moduli di analisi del comportamento.

Se Administration Server è installato in un dispositivo esistente nell'infrastruttura ed è stato utilizzato in precedenza per altre attività, si consiglia di prendere in considerazione il seguente software di protezione:

- Kaspersky Industrial CyberSecurity for Nodes. Si consiglia di installare questa applicazione nei dispositivi inclusi in una rete industriale. Kaspersky Industrial CyberSecurity for Nodes è un'applicazione che dispone di certificati di compatibilità con vari produttori di software industriale.

- Prodotti di sicurezza suggeriti. Se Administration Server è installato in un dispositivo con altro software, si consiglia di consultare i suggerimenti del fornitore del software sulla compatibilità delle soluzioni di sicurezza (potrebbero già essere disponibili suggerimenti per la selezione di una soluzione di sicurezza e potrebbe essere necessario configurare l'area attendibile).

Creazione di un criterio di sicurezza separato per l'applicazione di protezione

Si consiglia di creare un criterio di sicurezza separato per l'applicazione che protegge il dispositivo Administration Server. Questo criterio deve essere diverso dal criterio di sicurezza per i dispositivi client. In questo modo, è possibile specificare le impostazioni di sicurezza più appropriate per Administration Server, senza influire sul livello di protezione di altri dispositivi.

Si consiglia di dividere i dispositivi in gruppi e quindi di inserire il dispositivo Administration Server in un gruppo separato per il quale è possibile creare criteri di sicurezza speciali.

Moduli di protezione

In assenza di suggerimenti speciali da parte del fornitore del software di terzi installato nello stesso dispositivo di Administration Server, si consiglia di attivare e configurare tutti i moduli di protezione disponibili (dopo aver verificato il funzionamento di tali moduli di protezione per un certo periodo di tempo).

Configurazione del firewall del dispositivo Administration Server

Nel dispositivo Administration Server, si consiglia di configurare il firewall in modo da limitare il numero di dispositivi da cui gli amministratori possono connettersi ad Administration Server tramite Administration Console o Kaspersky Security Center Web Console.

Per impostazione predefinita, Administration Server utilizza la porta 13291 per ricevere connessioni da Administration Console e la porta 13299 per ricevere connessioni da Kaspersky Security Center Web Console. Si consiglia di limitare il numero di dispositivi da cui è possibile gestire Administration Server utilizzando queste porte.

Gestione della protezione dei dispositivi client

Limitazione dell'aggiunta di chiavi di licenza ai pacchetti di installazione

I pacchetti di installazione sono archiviati nella cartella condivisa di Administration Server, nella sottocartella Pacchetti. Se si aggiunge una chiave di licenza a un pacchetto di installazione, la chiave di licenza potrebbe essere compromessa poiché i diritti di accesso in lettura condivisi sono abilitati per l'archivio dei pacchetti di installazione.

Per evitare di compromettere la chiave di licenza, si sconsiglia di aggiungere chiavi di licenza ai pacchetti di installazione.

Si consiglia di utilizzare la distribuzione automatica delle chiavi di licenza ai dispositivi gestiti, la distribuzione tramite l'attività Aggiungi chiave di licenza per un'applicazione gestita e aggiungere manualmente un codice di attivazione o un file chiave ai dispositivi.

Regole automatiche per lo spostamento dei dispositivi tra i gruppi di amministrazione

Si consiglia di limitare l'uso delle regole automatiche per lo spostamento dei dispositivi tra i gruppi di amministrazione.

Se si utilizzano regole automatiche per lo spostamento dei dispositivi, ciò potrebbe comportare la propagazione di criteri che forniscono più privilegi al dispositivo spostato rispetto a quelli di cui disponeva prima del riposizionamento.

Inoltre, lo spostamento di un dispositivo client in un altro gruppo di amministrazione può comportare la propagazione delle impostazioni dei criteri. Queste impostazioni dei criteri potrebbero non essere appropriate per la distribuzione a dispositivi guest e non attendibili.

Questo suggerimento non si applica all'allocazione iniziale una tantum dei dispositivi ai gruppi di amministrazione.

Requisiti di sicurezza per i punti di distribuzione e i gateway di connessione

I dispositivi con Network Agent installato possono fungere da punto di distribuzione ed eseguire le seguenti funzioni:

- Distribuire gli aggiornamenti e i pacchetti di installazione ricevuti da Administration Server ai dispositivi client all'interno del gruppo.
- Eseguire l'installazione remota di software di terzi e applicazioni Kaspersky nei dispositivi client.
- Eseguire il polling della rete per rilevare nuovi dispositivi e aggiornare le informazioni sui dispositivi esistenti. Il punto di distribuzione può utilizzare gli stessi metodi di rilevamento dei dispositivi di Administration Server.

Posizionamento dei punti di distribuzione sulla rete dell'organizzazione utilizzati per:

- Riduzione del carico su Administration Server
- Ottimizzazione del traffico
- Concessione all'Administration Server dell'accesso ai dispositivi in parti difficili da raggiungere della rete

Tenendo conto delle capacità disponibili, si consiglia di proteggere i dispositivi che fungono da punti di distribuzione da qualsiasi tipo di accesso non autorizzato (anche fisico).

Limitazione dell'assegnazione automatica dei punti di distribuzione

Per semplificare l'amministrazione e assicurare l'operatività della rete, si consiglia di utilizzare l'assegnazione automatica dei punti di distribuzione. Tuttavia, per le reti industriali e le reti di piccole dimensioni, si consiglia di evitare l'assegnazione automatica dei punti di distribuzione, poiché, ad esempio, le informazioni private degli account utilizzati per il push delle attività di installazione remota possono essere trasferite ai punti di distribuzione tramite il sistema operativo.

Per le reti industriali e le reti di piccole dimensioni, è possibile assegnare manualmente i dispositivi in modo che fungano da punti di distribuzione.

È inoltre possibile visualizzare il Rapporto sull'attività dei punti di distribuzione.

Requisiti di sicurezza per i dispositivi degli utenti di Kaspersky Security Center

Per i dispositivi degli utenti di Kaspersky Security Center devono essere applicati requisiti di sicurezza speciali. Si consiglia di proteggere questi dispositivi da qualsiasi tipo di accesso non autorizzato (anche fisico):

I dispositivi utente di Kaspersky Security Center includono quanto segue:

- Dispositivi dai quali gli utenti si connettono a Kaspersky Security Center Web Console tramite un browser.
- Dispositivi dai quali gli utenti si connettono a Kaspersky Security Center tramite Administration Console basata su MMC.
- Dispositivi dai quali le applicazioni che interagiscono con Administration Server tramite OpenAPI sono connesse a Kaspersky Security Center.

Requisiti di sicurezza per i dispositivi con il programma di installazione di Kaspersky Security Center Web Console installato

Per gestire Kaspersky Security Center vengono utilizzati dispositivi in cui è installato il programma di installazione di Kaspersky Security Center Web Console, pertanto per la sicurezza di questi dispositivi è necessario applicare requisiti speciali. Si consiglia di proteggere questi dispositivi da qualsiasi tipo di accesso non autorizzato (anche fisico).

Configurazione della protezione per le applicazioni gestite

Criteri delle applicazioni gestite

Si consiglia di creare un criterio per ogni tipo di applicazione utilizzata e componente di Kaspersky Security Center (Network Agent, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Agent e altri). Questo criterio deve essere applicato a tutti i dispositivi gestiti (il gruppo di amministrazione principale) o a un gruppo separato in cui i nuovi dispositivi gestiti vengono automaticamente spostati in base alle regole di spostamento configurate.

Indicazione della password per disabilitare la protezione e disinstallare l'applicazione

Per impedire agli intrusi di disabilitare le applicazioni di protezione Kaspersky, si consiglia vivamente di abilitare la protezione tramite password per disabilitare la protezione e disinstallare le applicazioni di protezione Kaspersky. È possibile impostare la password, ad esempio, per Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Server, Network Agent e altre applicazioni Kaspersky. Dopo aver abilitato la protezione tramite password, si consiglia di bloccare queste impostazioni chiudendo il "lucchetto".

Specificazione della password per la connessione manuale di un dispositivo client ad Administration Server (utilità klmover)

L'utilità klmover consente di connettere manualmente un dispositivo client ad Administration Server. Quando si installa Network Agent su un dispositivo client, l'utilità viene automaticamente copiata nella cartella di installazione di Network Agent.

Per impedire agli intrusi di spostare i dispositivi fuori dal controllo di Administration Server, si consiglia di abilitare la protezione tramite password per l'esecuzione dell'utilità klmover. Per abilitare la protezione con password, selezionare l'opzione **Usa password di disinstallazione** nelle impostazioni dei criteri di Network Agent.

L'utilità klmover richiede i diritti di amministratore locale. La protezione tramite password per l'esecuzione dell'utilità klmover può essere omessa per i dispositivi utilizzati senza diritti di amministratore locale.

L'abilitazione dell'opzione **Usa password di disinstallazione** abilita anche la protezione con password per lo strumento Cleaner (cleaner.exe).

Utilizzo di Kaspersky Security Network

In tutti i criteri delle applicazioni gestite e nelle proprietà di Administration Server, si consiglia di abilitare l'uso di Kaspersky Security Network (KSN) e di accettare l'Informativa KSN. Quando si aggiorna o si effettua l'upgrade di Administration Server, è possibile accettare l'Informativa KSN aggiornata. In alcuni casi, quando l'uso dei servizi cloud è vietato dalla legge o da altri regolamenti, è possibile disabilitare KSN.

Scansione regolare dei dispositivi gestiti

Per tutti i gruppi di dispositivi, si consiglia di creare un'attività che esegua periodicamente una scansione completa dei dispositivi.

Individuazione di nuovi dispositivi

Si consiglia di configurare correttamente le impostazioni di rilevamento dei dispositivi: impostare l'integrazione con Active Directory e specificare gli intervalli di indirizzi IP per il rilevamento di nuovi dispositivi.

Per motivi di sicurezza, è possibile utilizzare il gruppo di amministrazione predefinito che include tutti i nuovi dispositivi e i criteri predefiniti che interessano questo gruppo.

Selezione di una cartella condivisa

Se si distribuisce Administration Server nel dispositivo in cui viene eseguito Windows con la selezione di una cartella condivisa esistente (utilizzata, ad esempio, per l'inserimento dei pacchetti di installazione e l'archiviazione dei database aggiornati), si consiglia di verificare che i diritti di lettura siano concessi al gruppo Everyone, e i diritti di scrittura sono concessi al gruppo KLAdmins.

Manutenzione di Administration Server

Copia di backup dei dati di Administration Server

Backup dei dati consente di ripristinare i dati di Administration Server senza perdita di dati.

Per impostazione predefinita, un'attività di backup dei dati viene creata automaticamente dopo l'installazione di Administration Server e viene eseguita periodicamente, salvando i backup nella directory appropriata.
Le impostazioni dell'attività di backup dei dati possono essere modificate come segue:

- La frequenza di backup aumenta
- Viene specificata una directory speciale per il salvataggio delle copie
- Le password per le copie di backup sono state modificate

Se si archiviano copie di backup in una directory speciale, diversa dalla directory predefinita, si consiglia di limitare l'elenco di controllo di accesso (ACL, Access Control List) per questa directory. Gli account di Administration Server e gli account del database di Administration Server devono disporre dell'accesso in scrittura per questa directory.

Manutenzione di Administration Server

La manutenzione di Administration Server consente di ridurre il volume del database e migliorare le prestazioni e l'affidabilità delle operazioni dell'applicazione. È consigliabile eseguire la manutenzione di Administration Server almeno ogni settimana.

La manutenzione di Administration Server viene eseguita tramite un'attività specializzata. Durante la manutenzione di Administration Server, l'applicazione esegue le azioni seguenti:

- Verifica se sono presenti errori nel database
- Riorganizza gli indici del database
- Aggiorna le statistiche del database
- Riduce le dimensioni del database (se necessario)

Installazione degli aggiornamenti del sistema operativo e degli aggiornamenti software di terzi

Si consiglia vivamente di installare periodicamente gli aggiornamenti software per il sistema operativo e il software di terzi nel dispositivo Administration Server.

I dispositivi client non richiedono una connessione continua ad Administration Server, quindi è possibile riavviare il dispositivo Administration Server in modo sicuro dopo aver installato gli aggiornamenti. Tutti gli eventi registrati nei dispositivi client durante il periodo di inattività di Administration Server vengono inviati ad esso dopo il ripristino della connessione.

Trasferimento di eventi a sistemi di terzi

Monitoraggio e generazione dei rapporti

Per una risposta tempestiva ai problemi di sicurezza, si consiglia di configurare le funzionalità di monitoraggio e generazione dei rapporti.

Esportazione di eventi nei sistemi SIEM

Per il rilevamento rapido dei problemi di sicurezza prima che si verifichino danni significativi, si consiglia di utilizzare l'esportazione degli eventi in un sistema SIEM.

Notifiche e-mail degli eventi di controllo

Kaspersky Security Center consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Per una risposta tempestiva alle emergenze, si consiglia di configurare Administration Server in modo che invii notifiche sugli eventi di controllo, gli eventi critici, gli eventi di errore e gli avvisi pubblicati.

Poiché questi eventi sono eventi interni al sistema, è prevedibile che se ne verifichino pochi; si tratta di una situazione abbastanza normale per la posta.

Statistiche della funzione Administration Server

Per una risposta tempestiva in caso di problemi di sicurezza, è consigliabile configurare l'invio delle statistiche della funzione Administration Server alle applicazioni di terzi, utilizzando il protocollo SNMP (Simple Network Management Protocol).

Suggerimenti sulla sicurezza per i sistemi informativi di terze parti

Raccomandazioni sulla sicurezza da CIS Benchmarks

Quando si utilizzano versioni di sistemi operativi, piattaforme di virtualizzazione o server di database supportati da Administration Server e Network Agent, è consigliabile applicare le best practice di sicurezza informatica del Center for Internet Security (CIS), se presenti, per ottimizzare questi sistemi informatici.

Il Center for Internet Security (CIS) è un'organizzazione senza scopo di lucro dedicata al miglioramento della sicurezza nel campo della tecnologia informatica. In particolare, il CIS sviluppa e distribuisce standard di sicurezza come CIS Controls e CIS Benchmarks. Questi standard sono un insieme di raccomandazioni e pratiche per garantire la sicurezza dei sistemi informatici.

Il portale CIS contiene raccomandazioni per le versioni dei seguenti sistemi informatici supportati da Administration Server e Network Agent:

- Sistemi operativi delle seguenti famiglie:
  - Windows per desktop
  - Windows per server
  - Debian
  - Ubuntu
  - CentOS
  - Oracle Linux
  - Red Hat Enterprise Linux
  - SUSE Linux Enterprise Server
  - macOS
- Piattaforme di virtualizzazione VMware
- Server del database:
  - Microsoft SQL Server
  - MySQL
  - MariaDB
  - PostgreSQL

Raccomandazioni di sicurezza per il sistema operativo Astra Linux

Quando si utilizza il sistema operativo Astra Linux, è necessario seguire i suggerimenti di sicurezza descritti nel Red Book per la versione corrispondente di Astra Linux.

Raccomandazioni di sicurezza per il sistema operativo RED OS

Quando si utilizza il sistema operativo RED OS, è necessario utilizzare i suggerimenti sulla protezione nella guida dell'amministratore descritti nella documentazione ufficiale di RED OS.

Suggerimenti per l'utilizzo delle applicazioni di protezione Kaspersky

Utilizzo della password KLAdmin in Kaspersky Endpoint Security for Windows

Più utenti con diversi livelli di alfabetizzazione informatica possono condividere un dispositivo in cui Kaspersky Endpoint Security for Windows è installato. Se gli utenti hanno accesso illimitato a Kaspersky Endpoint Security for Windows e alle relative impostazioni, il livello generale di protezione del dispositivo potrebbe essere ridotto. La protezione tramite password consente di limitare l'accesso degli utenti a Kaspersky Endpoint Security for Windows, in base alle autorizzazioni concesse loro (ad esempio, l'autorizzazione di chiudere l'applicazione).

Uno dei modi per limitare l'accesso a Kaspersky Endpoint Security for Windows e ai relativi parametri consiste nell'utilizzare un account KLAdmin. L'account KLAdmin è un account amministratore con accesso illimitato a Kaspersky Endpoint Security for Windows. L'account KLAdmin ha il diritto di eseguire qualsiasi azione protetta tramite password in Kaspersky Endpoint Security for Windows. Non è possibile revocare le autorizzazioni per l'account KLAdmin. È possibile impostare la password per l'account KLAdmin nelle proprietà del criterio di Kaspersky Endpoint Security for Windows. L'amministratore di Kaspersky Endpoint Security for Windows è pienamente responsabile dell'utilizzo sicuro della password per l'account KLAdmin. Se l'organizzazione dispone di un proprio criterio password, seguire le istruzioni di tale criterio.

I nostri suggerimenti per proteggere l'organizzazione dal furto della password KLAdmin sono i seguenti:

- **Requisiti generali**

  Non utilizzare il nome account o parte del nome come password.

- **Requisiti di lunghezza minima della password**

  Creare una password che contenga almeno 10 caratteri.

- **Requisiti per l'utilizzo di più tipi di carattere**

  Impostare una password complessa che contenga caratteri di diverse categorie: lettere minuscole e maiuscole, numeri e caratteri speciali.

- **Requisiti di scadenza della password**

  Impostare una data di scadenza minima della password di 90 giorni. Una nuova password non deve corrispondere a nessuna delle ultime 24 password.

Preparazione per la distribuzione

Questa sezione descrive le operazioni che è necessario eseguire prima della distribuzione di Kaspersky Security Center.

Pianificazione della distribuzione di Kaspersky Security Center

Questa sezione contiene informazioni sulle opzioni più convenienti per la distribuzione dei componenti di Kaspersky Security Center nella rete di un'organizzazione a seconda dei seguenti criteri:

- Numero totale di dispositivi
- Unità (sedi locali, filiali) separate a livello organizzativo o geografico
- Reti distinte connesse tramite canali con larghezza di banda ridotta
- Necessità dell'accesso via Internet all'Administration Server

Schemi tipici di distribuzione di un sistema di protezione

In questa sezione vengono descritti gli schemi standard per la distribuzione di un sistema di protezione anti-virus in una rete aziendale tramite Kaspersky Security Center.

Il sistema deve essere protetto contro qualsiasi tipo di accesso non autorizzato. È consigliabile installare tutti gli aggiornamenti della protezione disponibili per il sistema operativo prima di installare l'applicazione nel dispositivo e proteggere fisicamente Administration Server e punti di distribuzione.

È possibile utilizzare Kaspersky Security Center per distribuire un sistema di protezione in una rete aziendale tramite i seguenti schemi di distribuzione:

- Distribuzione di un sistema di protezione tramite Kaspersky Security Center, mediante uno dei seguenti modi:
  - Tramite Administration Console
  - Tramite Kaspersky Security Center Web Console

  Le applicazioni Kaspersky vengono installate automaticamente nei dispositivi client che, a loro volta, vengono connessi automaticamente ad Administration Server utilizzando Kaspersky Security Center.

  Lo schema di distribuzione di base prevede la distribuzione di un sistema di protezione tramite Administration Console. L'utilizzo di Kaspersky Security Center Web Console consente di avviare l'installazione delle applicazioni Kaspersky da un browser.

- Distribuzione manuale di un sistema di protezione utilizzando pacchetti di installazione indipendenti generati da Kaspersky Security Center.

  L'installazione delle applicazioni Kaspersky nei dispositivi client e nella workstation dell'amministratore viene eseguita manualmente; le impostazioni per la connessione dei dispositivi client ad Administration Server vengono specificate durante l'installazione di Network Agent.

  Questo metodo di distribuzione è consigliato nei casi in cui l'installazione remota non è possibile.

Kaspersky Security Center consente inoltre di distribuire il sistema di protezione utilizzando i criteri di gruppo di Microsoft Active Directory®.

Informazioni sulla pianificazione della distribuzione di Kaspersky Security Center nella rete di un'organizzazione

Un solo Administration Server può supportare un massimo di 100.000 dispositivi. Se il numero totale di dispositivi nella rete di un'organizzazione è superiore a 100.000, è necessario distribuire più Administration Server nella rete e combinarli in una gerarchia per gestirli comodamente in modo centralizzato.

Se un'organizzazione include sedi locali remote su larga scala (filiali) con amministratori distinti, è consigliabile distribuire gli Administration Server in tali sedi. In caso contrario, tali filiali devono essere considerate reti distinte connesse tramite canali a basso throughput; vedere la sezione "Configurazione standard: poche sedi su larga scala gestite da amministratori distinti".

Quando si utilizzano reti distinte connesse tramite canali con larghezza di banda ridotta, è possibile ridurre il traffico assegnando a uno o più Network Agent il ruolo di punto di distribuzione (vedere la tabella per il calcolo del numero di punti di distribuzione). In questo caso, tutti i dispositivi in una rete distinta recupereranno gli aggiornamenti da tali centri di aggiornamento locali. I punti di distribuzione effettivi possono scaricare gli aggiornamenti sia da Administration Server (scenario predefinito) sia dai server Kaspersky in Internet (vedere la sezione "Configurazione standard: più sedi remote di piccole dimensioni").

La sezione "Configurazioni standard di Kaspersky Security Center" fornisce descrizioni dettagliate delle configurazioni standard di Kaspersky Security Center. Durante la pianificazione della distribuzione, scegliere la configurazione standard più adatta, in base alla struttura dell'organizzazione.

In fase di pianificazione della distribuzione, deve essere valutata l'assegnazione di uno speciale certificato X.509 all'Administration Server. L'assegnazione del certificato X.509 all'Administration Server può essere utile nei seguenti casi (elenco parziale):

- Ispezione del traffico SSL (Secure Sockets Layer) per mezzo di un proxy con terminazione SSL o per l'utilizzo di un proxy inverso
- Integrazione con l'infrastruttura PKI (Public Key Infrastructure) di un'organizzazione
- Specificazione dei valori richiesti nei campi del certificato
- Specificazione del livello di criptaggio richiesto di un certificato

Selezione di una struttura per la protezione di un'azienda

La selezione di una struttura per la protezione di un'organizzazione viene definita dai seguenti fattori:

- Topologia della rete dell'organizzazione.
- Struttura dell'organizzazione.
- Numero di dipendenti responsabili della protezione della rete e allocazione delle relative responsabilità.
- Risorse hardware che possono essere allocate nei componenti di gestione della protezione.
- Throughput dei canali di comunicazione che è possibile allocare per la manutenzione dei componenti della protezione nella rete dell'organizzazione.
- Limiti di tempo per l'esecuzione di operazioni amministrative critiche nella rete dell'organizzazione. Le operazioni amministrative critiche includono, ad esempio, la distribuzione dei database anti-virus e la modifica dei criteri per i dispositivi client.

Quando si seleziona una struttura di protezione, è innanzitutto consigliabile effettuare una stima delle risorse hardware e di rete disponibili che è possibile utilizzare per l'esecuzione di un sistema di protezione centralizzato.

Per analizzare l'infrastruttura di rete e hardware, è consigliabile attenersi alla seguente procedura:

1. Definire le seguenti impostazioni della rete per cui verrà distribuita la protezione:
   - Numero di segmenti di rete.
   - Velocità dei canali di comunicazione tra i singoli segmenti di rete.
   - Numero di dispositivi gestiti in ciascun segmento di rete.
   - Throughput di ciascun canale di comunicazione che è possibile allocare per garantire il funzionamento della protezione.
2. Determinare il tempo massimo consentito per l'esecuzione delle operazioni di amministrazione chiave per tutti i dispositivi gestiti.
3. Analizzare le informazioni dei passaggi 1 e 2, oltre ai dati dai test di carico del sistema di amministrazione. In base all'analisi, rispondere alle seguenti domande:
   - È possibile servire tutti i client con un solo Administration Server o è necessaria una gerarchia di Administration Server?
   - Quale configurazione hardware di Administration Server è necessaria per gestire tutti i client nel rispetto dei limiti di tempo specificati al passaggio 2?
   - È necessario utilizzare i punti di distribuzione per ridurre il carico sui canali di comunicazione?

Dopo aver ottenuto le risposte alle domande indicate nel passaggio 3, è possibile compilare un set di strutture consentite per la protezione dell'organizzazione.

Nella rete dell'organizzazione è possibile utilizzare una delle seguenti strutture di protezione standard:

- Un solo Administration Server. Tutti i dispositivi client sono connessi a un solo Administration Server. Administration Server opera come punto di distribuzione.
- Un solo Administration Server con punti di distribuzione. Tutti i dispositivi client sono connessi a un solo Administration Server. Alcuni dispositivi client della rete operano come punti di distribuzione.
- Gerarchia di Administration server. Per ciascun segmento di rete viene allocato un singolo Administration Server, che entra a far parte di una gerarchia generale di Administration Server. L'Administration Server primario opera come punto di distribuzione.
- Gerarchia di Administration Server con punti di distribuzione. Per ciascun segmento di rete viene allocato un singolo Administration Server, che entra a far parte di una gerarchia generale di Administration Server. Alcuni dispositivi client della rete operano come punti di distribuzione.

Configurazioni standard di Kaspersky Security Center

Questa sezione descrive le seguenti configurazioni standard utilizzate per la distribuzione dei componenti di Kaspersky Security Center nella rete di un'organizzazione:

- Singola sede
- Poche sedi su larga scala, separate a livello geografico e gestite da amministratori distinti
- Più sedi di piccole dimensioni, separate a livello geografico

Configurazione standard: singola sede

È possibile distribuire uno o più Administration Server nella rete dell'organizzazione. Il numero di Administration Server che è possibile selezionare può essere basato sull'hardware disponibile o sul numero totale di dispositivi gestiti.

Un solo Administration Server può supportare fino a 100.000 dispositivi. È necessario tenere conto della possibilità di aumentare il numero di dispositivi gestiti in futuro: può essere utile connettere un numero più limitato di dispositivi a un singolo Administration Server.

Gli Administration Server possono essere distribuiti nella rete interna o nella rete perimetrale, a seconda del fatto che sia necessario o meno l'accesso via Internet agli Administration Server.

Se vengono utilizzati più server, è consigliabile combinarli in una gerarchia. L'utilizzo di una gerarchia di Administration Server consente di evitare la duplicazione di criteri e attività e di amministrare l'intero set di dispositivi gestiti come se fossero gestiti da un singolo Administration Server (ricerca di dispositivi, creazione di selezioni di dispositivi e generazione di rapporti).

Configurazione standard: poche sedi su larga scala gestite da amministratori distinti

Se un'organizzazione ha diverse sedi su larga scala e geograficamente distanti, è necessario prendere in considerazione l'opzione di distribuire Administration Server in ciascuna sede. Per ogni sede possono essere distribuiti uno o più server di amministrazione, a seconda del numero di dispositivi client e dell'hardware disponibile. In questo caso, ciascuna sede avrà le caratteristiche descritte nello scenario "Configurazione standard: singola sede". Per semplificare l'amministrazione è consigliabile combinare tutti gli Administration Server in una gerarchia (possibilmente multi-livello).

Se alcuni dipendenti si spostano da un ufficio all'altro con i propri dispositivi (laptop), creare profili di connessione di Network Agent nel criterio di Network Agent. I profili di connessione di Network Agent sono supportati solo per i dispositivi Windows e macOS.

Configurazione standard: più sedi remote di piccole dimensioni

Questa configurazione standard prevede una sede centrale e diverse sedi remote di piccole dimensioni che possono comunicare con la sede centrale tramite Internet. Ogni sede remota può essere posizionata dietro un NAT (Network Address Translation), quindi non è possibile stabilire alcuna connessione tra due sedi remote poiché sono isolate.

È necessario distribuire un Administration Server nella sede centrale e assegnare uno o più punti di distribuzione a tutte le altre sedi. Se le sedi sono collegate via Internet, può essere utile creare un'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per i punti di distribuzione, in modo gli aggiornamenti vengano scaricati direttamente dai server di Kaspersky, dalla cartella locale o di rete, invece che da Administration Server.

Se alcuni dispositivi in una sede remota non hanno accesso diretto all'Administration Server (ad esempio, l'accesso all'Administration Server viene fornito via Internet ma alcuni dispositivi non hanno accesso a Internet), i punti di distribuzione devono essere impostati in modalità gateway di connessione. In questo caso, i Network Agent nei dispositivi della sede remota saranno connessi per l'ulteriore sincronizzazione all'Administration Server, ma attraverso il gateway, non direttamente.

Poiché in genere l'Administration Server non è in grado di eseguire il polling della rete della sede remota, può essere utile assegnare questa funzione a un punto di distribuzione.

L'Administration Server non potrà inviare notifiche tramite la porta UDP 15000 ai dispositivi gestiti posizionati dietro il NAT nella sede remota. Per risolvere questo problema, è possibile abilitare la modalità di connessione continua ad Administration Server nelle proprietà dei dispositivi che operano come punti di distribuzione (casella di controllo **Non eseguire la disconnessione da Administration Server**). Questa modalità è disponibile se il numero totale di punti di distribuzione non è superiore a 300. Utilizzare i server push per assicurarsi che vi sia una connettività costante tra un dispositivo gestito e l'Administration Server. Per ulteriori dettagli, fare riferimento al seguente argomento: Utilizzo di un punto di distribuzione come server push.

Selezione di un DBMS per Administration Server

Durante la selezione del sistema di gestione database (DBMS) che deve essere utilizzato da un Administration Server, è necessario tenere conto del numero di dispositivi coperti dall'Administration Server.

Nella seguente tabella, sono elencate le opzioni DBMS valide, nonché i suggerimenti e le limitazioni per il relativo utilizzo.

Suggerimenti e limitazioni su DBMS

DBMS	Suggerimenti e limitazioni
SQL Server Express Edition 2016 o versione successiva	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 10.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. È possibile limitare il numero massimo di eventi nell'archivio eventi per evitare l'overflow del database. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database. L'utilizzo simultaneo del DBMS SQL Server Express Edition da parte di Administration Server e di un'altra applicazione non è consentito. Il database Microsoft SQL Express non è supportato per l'attività **Esegui sincronizzazione di Windows Update**.
Edizione di SQL Server in locale diversa da Express, 2016 o versione successiva	Nessuna limitazione.
Edizione di SQL Server in remoto diversa da Express, 2016 o successiva	Valida solo se entrambi i dispositivi si trovano nello stesso dominio Windows®. Se i domini sono differenti, è necessario stabilire una relazione di trust bidirezionale tra di essi.
MySQL 5.5, 5.6 o 5.7 in locale o in remoto (le versioni 5.5.1, 5.5.2, 5.5.3, 5.5.4 e 5.5.5 di MySQL non sono più supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 10.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database.
MySQL 8.0.20 locale o remoto o versioni successive	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 50.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database.

DBMS	Suggerimenti e limitazioni
MariaDB locale o remoto (vedere le versioni supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 20.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database.
PostgreSQL, Postgres Pro (vedere le versioni supportate)	Utilizzare uno di questi DBMS se si intende eseguire un singolo server di amministrazione per meno di 50.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database.

Se si utilizza SQL Server 2019 come DBMS e non si dispone della patch cumulativa CU12 o versione successiva, è necessario eseguire le seguenti operazioni dopo l'installazione di Kaspersky Security Center:

1. Stabilire la connessione a SQL Server utilizzando SQL Management Studio.
2. Eseguire il seguente comando (se è stato selezionato un nome diverso per il database, utilizza quel nome invece di KAV):

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. Riavviare il servizio SQL Server 2019.

In alternativa, l'utilizzo di SQL Server 2019 può generare errori, ad esempio "Memoria di sistema insufficiente nel pool di risorse 'interno' per l'esecuzione di questa query".

Configurazione del server MariaDB x64 per l'utilizzo con Kaspersky Security Center 15.1

Per configurare correttamente il server MariaDB x64 per l'utilizzo di Kaspersky Security Center, è necessario utilizzare i parametri del server predefiniti ad eccezione dei parametri del server specificati in questo articolo.

Kaspersky Security Center 15.1 supporta il DBMS MariaDB. Per ulteriori informazioni sulle versioni supportate di MariaDB, vedere la sezione Requisiti hardware e software.

Se si utilizza il DBMS MariaDB per Kaspersky Security Center, abilitare il supporto per InnoDB e l'archiviazione MEMORY, nonché per le codifiche UTF-8 e UCS-2.

Impostazioni consigliate per il file my.ini

Per configurare il file my.ini:

1. Aprire il file my.ini in un editor di testo.

2. Aggiungere le seguenti righe nella sezione `[mysqld]` del file my.ini:

```
sort_buffer_size=10M
join_buffer_size=100M
join_buffer_space_limit=300M
join_cache_level=8
tmp_table_size=512M
max_heap_table_size=512M
key_buffer_size=200M
innodb_buffer_pool_size=<il valore reale non deve essere inferiore all'80% delle
dimensioni previste del database KAV>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
sql_mode="STRICT_TRANS_TABLES,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION"
```

Il valore di `innodb_buffer_pool_size` non deve essere inferiore all'80% della dimensione del database KAV prevista. Si noti che la memoria specificata viene allocata all'avvio del server. Se la dimensione del database è inferiore alla dimensione del buffer specificata, viene allocata solo la memoria richiesta. Se si utilizza MariaDB 10.4.3 o versione precedente, la dimensione effettiva della memoria allocata è di circa il 10% maggiore rispetto alla dimensione del buffer specificata.

È consigliabile utilizzare il valore del parametro `innodb_flush_log_at_trx_commit=0`, perché i valori "1" o "2" influiscono negativamente sulla velocità di esecuzione di MariaDB. Assicurarsi che il parametro `innodb_file_per_table` sia impostato su `1`.

Per MariaDB 10.1, immettere inoltre le seguenti righe nella sezione [mysqld]:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

Per MariaDB 10.6, immettere inoltre le seguenti righe nella sezione [mysqld]:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Per impostazione predefinita, i componenti aggiuntivi dell'ottimizzatore `join_cache_incremental`, `join_cache_hashed` e `join_cache_bka` sono abilitati. Se questi componenti aggiuntivi non sono abilitati, è necessario abilitarli.

Per verificare se i componenti aggiuntivi dell'ottimizzatore sono abilitati:

1. Nella console del client MariaDB eseguire il comando:

   ```
   SELECT @@optimizer_switch;
   ```

2. Verificare che l'output del comando contenga le seguenti righe:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Se queste righe sono presenti e hanno il valore `on`, i componenti aggiuntivi dell'ottimizzatore sono abilitati.

   Se queste righe non sono presenti o hanno il valore `off`, eseguire le seguenti operazioni:

   1. Aprire il file my.ini in un editor di testo.

   2. Aggiungere le seguenti righe nella sezione `[mysqld]` del file my.ini:

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

I componenti aggiuntivi `join_cache_incremental`, `join_cache_hash` e `join_cache_bka` vengono abilitati.

Configurazione del server MySQL x64 per l'utilizzo con Kaspersky Security Center 15.1

Per configurare correttamente il server MySQL x64 per l'utilizzo di Kaspersky Security Center, è necessario utilizzare i parametri del server predefiniti ad eccezione dei parametri del server specificati in questo articolo.

Se si utilizza il DBMS MySQL per Kaspersky Security Center, abilitare il supporto per InnoDB e l'archiviazione MEMORY, nonché per le codifiche UTF-8 e UCS-2.

Impostazioni consigliate per il file my.ini

Per configurare il file my.ini:

1. Aprire il file my.ini in un editor di testo.

2. Aggiungere le seguenti righe nella sezione `[mysqld]` del file my.ini:

```
sort_buffer_size=10M
join_buffer_size=20M
tmp_table_size=600M
max_heap_table_size=600M
key_buffer_size=200M
innodb_buffer_pool_size=<il valore reale non deve essere inferiore all'80% delle dimensioni previste del database KAV>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (nella maggior parte dei casi il server utilizza piccole transazioni)
innodb_lock_wait_timeout=300
max_allowed_packet=32M
max_connections=151
max_prepared_stmt_count=12800
table_open_cache=60000
table_open_cache_instances=4
table_definition_cache=60000
```

   Si noti che la memoria specificata nel valore `innodb_buffer_pool_size` viene allocato all'avvio del server. Se la dimensione del database è inferiore alla dimensione del buffer specificata, viene allocata solo la memoria richiesta. La dimensione effettiva della memoria allocata è di circa il 10% maggiore rispetto alla dimensione del buffer specificata. Per ulteriori dettagli, consultare la documentazione di MySQL.

   È consigliabile utilizzare il valore del parametro `innodb_flush_log_at_trx_commit = 0`, perché i valori "1" o "2" influiscono negativamente sulla velocità di esecuzione di MySQL. Assicurarsi che il parametro `innodb_file_per_table` sia impostato su `1`.

Configurazione del server PostgreSQL o Postgres per l'utilizzo con Kaspersky Security Center 15.1

Per configurare correttamente il server PostgreSQL o Postgres Pro per l'utilizzo con Kaspersky Security Center, è necessario utilizzare i parametri del server predefiniti ad eccezione dei parametri del server specificati in questo articolo.

Kaspersky Security Center 15.1 supporta i DBMS PostgreSQL e Postgres Pro. Se si utilizza uno di questi DBMS, prendere in considerazione la configurazione dei parametri del server DBMS per ottimizzare il funzionamento del DBMS con Kaspersky Security Center.

Il percorso predefinito del file di configurazione è: `C:\Program Files\PostgreSQL\<VERSIONE>\data\postgresql.conf`

Parametri consigliati per PostgreSQL e Postgres Pro:

- `shared_buffers` = 25% del valore della RAM del dispositivo in cui è installato il DBMS

  Se la RAM è inferiore a 1 GB, lasciare il valore predefinito.

- `max_stack_depth = 2MB`

- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `max_connections = 151`
- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128MB`

Assicurarsi che il parametro `standard_conforming_strings` sia impostato sul valore predefinito `on`. Ricaricare la configurazione o riavviare il server dopo aver aggiornato il file postgresql.conf. Per ulteriori dettagli, consultare la documentazione di PostgreSQL.

Se si utilizza Postgres Pro 15.7 o Postgres Pro 15.7.1, disabilitare il parametro `enable_compound_index_stats`:

```
enable_compound_index_stats = off
```

Per informazioni dettagliate sui parametri dei server PostgreSQL e Postgres Pro e su come specificarli, fare riferimento alla documentazione del DBMS corrispondente.

Per ulteriori dettagli sulla creazione e la configurazione degli account per PostgreSQL e Postgres Pro, consultare il seguente argomento: Configurazione degli account per l'utilizzo di PostgreSQL e Postgres Pro.

Gestione dei dispositivi mobili con Kaspersky Endpoint Security for Android

I dispositivi mobili in cui è installato Kaspersky Endpoint Security for Android™ (di seguito denominati dispositivi KES) sono gestiti tramite l'Administration Server. Kaspersky Security Center supporta le seguenti funzionalità per la gestione dei dispositivi KES:

- Gestione dei dispositivi mobili come dispositivi client:
  - Appartenenza ai gruppi di amministrazione
  - Monitoraggio, ad esempio la visualizzazione di stati, eventi e rapporti
  - Modifica delle impostazioni locali e assegnazione di criteri per Kaspersky Endpoint Security for Android
- Invio di comandi in modalità centralizzata
- Installazione remota di pacchetti app mobili

Administration Server gestisce i dispositivi KES tramite TLS, porta TCP 13292.

Concessione dell'accesso via Internet all'Administration Server

L'accesso via Internet all'Administration Server è necessario nei seguenti casi:

- Aggiornamento periodico dei database, dei moduli software e delle applicazioni Kaspersky
- Aggiornamento di software di terze parti

  Per impostazione predefinita, non è richiesta la connessione Internet per l'installazione degli aggiornamenti software Microsoft nei dispositivi gestiti da parte di Administration Server. I dispositivi gestiti possono ad esempio scaricare gli aggiornamenti software Microsoft direttamente dai server Microsoft Update o da Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione. Administration Server deve essere connesso a Internet nei seguenti casi:

  - Quando si usa Administration Server come server WSUS
  - Per installare gli aggiornamenti di software di terze parti diverso dal software Microsoft
- Correzione delle vulnerabilità del software di terze parti

  È necessaria una connessione Internet affinché Administration Server esegua le seguenti attività:

  - Per creare un elenco di correzioni consigliate per le vulnerabilità del software Microsoft. L'elenco viene creato e aggiornato regolarmente dagli specialisti Kaspersky.
  - Per correggere le vulnerabilità in software di terze parti diverso dal software Microsoft.
- Gestione dei dispositivi (portatili) degli utenti fuori sede
- Gestione dei dispositivi nelle sedi remote
- Interazione con gli Administration Server primari o secondari situati nelle sedi remote
- Gestione dei dispositivi mobili

Questa sezione descrive i modi tipici per fornire l'accesso via Internet all'Administration Server. Ciascuno dei casi che prevedono l'accesso via Internet ad Administration Server può richiedere un certificato dedicato per Administration Server.

Accesso a Internet: Administration Server in una rete locale

Se l'Administration Server è posizionato nella rete interna di un'organizzazione, è consigliabile rendere la porta TCP 13000 dell'Administration Server accessibile dall'esterno per mezzo del port forwarding. Se è necessaria la gestione dei dispositivi mobili, è consigliabile rendere accessibile la porta TCP 13292.

Accesso a Internet: Administration Server in una rete perimetrale

Se l'Administration Server è posizionato nella rete perimetrale dell'organizzazione, non ha accesso alla rete interna dell'organizzazione. Si applicano pertanto le seguenti limitazioni:

- L'Administration Server non può rilevare nuovi dispositivi.
- Administration Server non può eseguire la distribuzione iniziale di Network Agent tramite l'installazione forzata sui dispositivi nella rete interna dell'organizzazione.

Questo vale solo per l'installazione iniziale di Network Agent. Qualsiasi ulteriore upgrade di Network Agent o l'installazione dell'applicazione di protezione potranno comunque essere eseguiti dall'Administration Server. Allo stesso tempo, la distribuzione iniziale dei Network Agent può essere eseguita con altri sistemi, ad esempio tramite i criteri di gruppo di Microsoft® Active Directory®.

- L'Administration Server non può inviare notifiche ai dispositivi gestiti tramite la porta UDP 15000, che non è critica per il funzionamento di Kaspersky Security Center.

- L'Administration Server non può eseguire il polling di Active Directory. Tuttavia, i risultati del polling di Active Directory non sono richiesti nella maggior parte degli scenari.

Se le limitazioni precedenti sono considerate di importanza critica, possono essere rimosse utilizzando punti di distribuzione posizionati nella rete dell'organizzazione:

- Per eseguire la distribuzione iniziale nei dispositivi senza Network Agent, installare Network Agent in uno dei dispositivi e quindi assegnargli lo stato di punto di distribuzione. L'installazione iniziale di Network Agent negli altri dispositivi sarà eseguita da Administration Server tramite questo punto di distribuzione.

- Per rilevare i nuovi dispositivi nella rete interna dell'organizzazione ed eseguire il polling di Active Directory, è necessario abilitare i metodi di device discovery appropriati in uno dei punti di distribuzione.

Per assicurare il corretto invio delle notifiche alla porta UDP 15000 sui dispositivi gestiti nella rete interna dell'organizzazione, è necessario coprire l'intera rete con punti di distribuzione. Nelle proprietà dei punti di distribuzione assegnati selezionare la casella di controllo **Non eseguire la disconnessione da Administration Server**. Administration Server stabilirà una connessione continua ai punti di distribuzione e questi potranno inviare notifiche alla porta UDP 15000 nei dispositivi che si trovano nella rete interna dell'organizzazione (può trattarsi di una rete IPv4 o IPv6).

Accesso a Internet: Network Agent come gateway di connessione nella rete perimetrale

Administration Server può essere posizionato nella rete interna dell'organizzazione: in una rete perimetrale (DMZ) di tale rete può essere presente un dispositivo con Network Agent eseguito come gateway di connessione con connettività inversa (Administration Server stabilisce una connessione a Network Agent). In questo caso, devono essere soddisfatte le seguenti condizioni per garantire l'accesso a Internet:

- Nel dispositivo posizionato nella rete perimetrale deve essere installato Network Agent. Quando si installa Network Agent, nella finestra **Gateway di connessione** dell'Installazione guidata selezionare **Utilizzare Network Agent come gateway di connessione nella rete perimetrale**.

- Il dispositivo con il gateway di connessione installato deve essere aggiunto come punto di distribuzione. Quando si aggiunge il gateway di connessione, nella finestra **Aggiungi punto di distribuzione** selezionare l'opzione **Seleziona → Aggiungi gateway di connessione nella rete perimetrale in base all'indirizzo**.

- Per utilizzare una connessione Internet per connettere dispositivi desktop esterni ad Administration Server, è necessario correggere il pacchetto di installazione per Network Agent. Nelle proprietà del pacchetto di installazione creato selezionare l'opzione **Avanzate →Esegui la connessione ad Administration Server utilizzando un gateway di connessione**, quindi specificare il nuovo gateway di connessione creato.

Per il gateway di connessione nella rete perimetrale, Administration Server crea un certificato firmato con il certificato di Administration Server. Se l'amministratore decide di assegnare un certificato personalizzato ad Administration Server, questa operazione deve essere eseguita prima di creare un gateway di connessione nella rete perimetrale.

Se alcuni dipendenti utilizzano computer portatili che possono connettersi ad Administration Server sia dalla rete locale che via Internet, può essere utile creare una regola per il passaggio di Network Agent nel criterio di Network Agent.

Informazioni sui punti di distribuzione

Un dispositivo in cui è installato Network Agent può essere utilizzato come punto di distribuzione. In questa modalità, Network Agent può eseguire le seguenti funzioni:

- Distribuire gli aggiornamenti (recuperati dall'Administration Server o dai server di Kaspersky). Nel secondo caso, è necessario creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per il dispositivo che opera come punto di distribuzione:
    - Installare il software (inclusa la distribuzione iniziale dei Network Agent) in altri dispositivi.
    - Eseguire il polling della rete per rilevare nuovi dispositivi e aggiornare le informazioni sui dispositivi esistenti. Un punto di distribuzione può applicare gli stessi metodi di device discovery di Administration Server.

La distribuzione dei punti di distribuzione nella rete di un'organizzazione ha i seguenti obiettivi:

- Riduzione del carico sull'Administration Server.
- Ottimizzazione del traffico.
- Concessione all'Administration Server dell'accesso ai dispositivi in posizioni difficili da raggiungere della rete dell'organizzazione. La disponibilità di un punto di distribuzione nella rete dietro un NAT (in relazione all'Administration Server) consente all'Administration Server di eseguire le seguenti azioni:
    - Inviare notifiche ai dispositivi tramite UDP nella rete IPv4 o IPv6
    - Eseguire il polling della rete IPv4 o IPv6
    - Eseguire la distribuzione iniziale
    - Fungere da server push

Un punto di distribuzione viene assegnato a un gruppo di amministrazione. In questo caso, l'ambito del punto di distribuzione include tutti i dispositivi all'interno del gruppo di amministrazione e di tutti i relativi sottogruppi. Tuttavia, il dispositivo che opera come punto di distribuzione può non essere incluso nel gruppo di amministrazione a cui è stato assegnato.

È possibile far funzionare un punto di distribuzione come gateway di connessione. In questo caso, i dispositivi nell'ambito del punto di distribuzione saranno connessi all'Administration Server tramite il gateway, non direttamente. Questa modalità può essere utile negli scenari che non consentono di stabilire una connessione diretta tra Administration Server e dispositivi gestiti.

Se si utilizza un dispositivo basato su Linux come punto di distribuzione, si consiglia vivamente di aumentare il limite dei descrittori di file per il servizio klnagent, poiché se l'ambito del punto di distribuzione include molti dispositivi, il numero massimo predefinito di file che è possibile aprire potrebbe non essere sufficiente.

Aumento del limite dei descrittori di file per il servizio klnagent

Se l'ambito di un punto di distribuzione basato su Linux include molti dispositivi, il limite predefinito di file che è possibile aprire (descrittori di file) potrebbe non essere sufficiente. Per evitare questo, è possibile aumentare il limite dei descrittori di file per il servizio klnagent.

Per aumentare il limite dei descrittori di file per il servizio klnagent:

1. Nel dispositivo basato su Linux che funge da punto di distribuzione, aprire il file `/lib/systemd/system/klnagent64.service`, quindi specificare i limiti hard e soft dei descrittori di file nel parametro `LimitNOFILE` della sezione `[Service]`:

   `LimitNOFILE=<limite risorse trasferibili>:<limite risorse hardware>`

   Ad esempio, `LimitNOFILE=32768:131072`. Si noti che il limite soft dei descrittori di file deve essere inferiore o uguale al limite hard.

2. Eseguire il seguente comando per assicurarsi che i parametri siano specificati correttamente:

   `systemd-analyze verify klnagent64.service`

   Se i parametri sono specificati in modo errato, questo comando può generare uno dei seguenti errori:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Se si verifica questo errore, i simboli nella riga `LimitNOFILE` sono stati specificati in modo errato. È necessario controllare e correggere la riga immessa.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Se si verifica questo errore, il limite soft dei descrittori di file immessi è maggiore del limite hard. È necessario controllare la riga immessa e assicurarsi che il limite soft dei descrittori di file sia uguale o inferiore al limite hard.

3. Eseguire il seguente comando per ricaricare il processo systemd:

   `systemctl daemon-reload`

4. Eseguire il seguente comando per riavviare il servizio Network Agent:

   `systemctl restart klnagent`

5. Eseguire il seguente comando per assicurarsi che i parametri specificati vengano applicati correttamente:

   `less /proc/<id processo nagent>/limits`

   dove il parametro `<id processo nagent>` è l'identificatore del processo di Network Agent. È possibile eseguire il seguente comando per ottenere l'identificatore:

   `ps -ax | grep klnagent`

Per il punto di distribuzione basato su Linux, il limite di file che è possibile aprire è stato aumentato.

Calcolo del numero e configurazione dei punti di distribuzione

Più dispositivi client contiene una rete, maggiore è il numero dei punti di distribuzione richiesti. È consigliabile non disabilitare l'assegnazione automatica dei punti di distribuzione. Quando è abilitata l'assegnazione automatica dei punti di distribuzione, Administration Server assegna i punti di distribuzione se il numero dei dispositivi client è ampio e definisce la configurazione.

Utilizzo di punti di distribuzione assegnati in modo esclusivo

Se si prevede di utilizzare alcuni dispositivi specifici come punti di distribuzione (ovvero, server assegnati in modo esclusivo), è possibile scegliere di non utilizzare l'assegnazione automatica dei punti di distribuzione. In questo caso, verificare che i dispositivi a cui assegnare il ruolo di punti di distribuzione dispongano di un volume sufficiente di spazio libero su disco, che non vengano arrestati regolarmente e che la modalità di sospensione sia disabilitata.

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–100	1
Più di 100	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Utilizzo di dispositivi client standard (workstation) come punti di distribuzione

Se si prevede di utilizzare dispositivi client standard (ovvero, workstation) come punti di distribuzione, è consigliabile assegnare i punti di distribuzione come indicato nelle tabelle seguenti per evitare un carico eccessivo sui canali di comunicazione e su Administration Server:

Numero di workstation che operano come punti di distribuzione in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Numero di workstation che operano come punti di distribuzione in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–30	1
31–300	2
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Se un punto di distribuzione viene arrestato (o non è disponibile per altri motivi), i dispositivi gestiti nel relativo ambito possono accedere ad Administration Server per gli aggiornamenti.

Gerarchia di Administration Server

Un MSP può eseguire diversi Administration Server. Poiché può essere scomodo amministrare più Administration Server distinti, è possibile applicare una gerarchia. Una configurazione "primario/secondario" per due Administration Server fornisce le seguenti opzioni:

- Un Administration Server secondario eredita i criteri e le attività dall'Administration Server primario, evitando così la duplicazione delle impostazioni.
- Le selezioni di dispositivi nell'Administration Server primario possono includere i dispositivi degli Administration Server secondari.
- I rapporti nell'Administration Server primario possono contenere dati (incluse informazioni dettagliate) ottenuti dagli Administration Server secondari.

L'Administration Server primario riceve i dati solo dagli Administration Server secondari non virtuali nell'ambito delle opzioni elencate sopra. Questa limitazione non si applica agli Administration Server virtuali, che condividono il database con l'Administration Server primario.

Administration Server virtuali

Sulla base di un Administration Server fisico, è possibile creare più Administration Server virtuali, simili agli Administration Server secondari. Rispetto al modello di accesso discrezionale, che è basato su elenchi di controllo di accesso (ACL), il modello degli Administration Server virtuali è più funzionale e fornisce un maggior livello di isolamento. Oltre a una struttura dedicata di gruppi di amministrazione per i dispositivi assegnati con criteri e attività, ogni Administration Server virtuale dispone di un proprio gruppo di dispositivi non assegnati, di insiemi di rapporti, dispositivi ed eventi selezionati, pacchetti di installazione, regole di spostamento e così via. L'ambito funzionale degli Administration Server virtuali può essere utilizzato sia dai provider di servizi (xSP) per massimizzare l'isolamento dei clienti, sia da organizzazioni su vasta scala con flussi di lavoro sofisticati e numerosi amministratori.

Gli Administration Server virtuali sono molto simili agli Administration Server secondari, ma con le seguenti distinzioni:

- Un Administration Server virtuale non dispone della maggior parte delle impostazioni globali e di specifiche porte TCP.
- Un Administration Server virtuale non dispone di Administration Server secondari.
- Un Administration Server virtuale non include altri Administration Server virtuali.
- Un Administration Server fisico visualizza i dispositivi, i gruppi, gli eventi e gli oggetti nei dispositivi gestiti (elementi in Quarantena, registro delle applicazioni e così via) di tutti i relativi Administration Server virtuali.
- Un Administration Server virtuale può eseguire solo la scansione della rete a cui sono connessi punti di distribuzione.

Informazioni sulle limitazioni di Kaspersky Security Center

Nella seguente tabella sono riportate le limitazioni della versione corrente di Kaspersky Security Center.

Limitazioni di Kaspersky Security Center

Tipo di limitazione	Valore
Numero massimo di dispositivi gestiti per ogni Administration Server	100.000
Numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata	300
Numero massimo di gruppi di amministrazione	10.000
Numero massimo di eventi che è possibile memorizzare	45.000.000
Numero massimo di criteri	2000
Numero massimo di attività	2000
Numero massimo di oggetti Active Directory (unità organizzative, account utente, dispositivi e gruppi di protezione)	1.000.000
Numero massimo di profili in un criterio	100
Numero massimo di Administration Server secondari in un singolo Administration Server primario	500
Numero massimo di Administration Server virtuali	500
Numero massimo di dispositivi a cui può essere applicato un singolo punto di distribuzione (i punti di distribuzione sono applicabili solo ai dispositivi non mobili)	10.000
Numero massimo di dispositivi che possono utilizzare un singolo gateway di connessione	10.000, inclusi i dispositivi mobili
Numero massimo di dispositivi mobili per ogni Administration Server	100000 meno il numero di dispositivi gestiti fissi

Carico di rete

Questa sezione contiene informazioni sul volume del traffico di rete scambiato tra i dispositivi client e Administration Server durante gli scenari di amministrazione chiave.

Il carico principale sulla rete è causato dai seguenti scenari di amministrazione:

- Distribuzione iniziale della protezione anti-virus
- Aggiornamento iniziale dei database anti-virus
- Sincronizzazione di un dispositivo client con Administration Server
- Aggiornamenti periodici dei database anti-virus
- Elaborazione di eventi nei dispositivi client da parte di Administration Server

Distribuzione iniziale della protezione anti-virus

In questa sezione, vengono fornite informazioni sui valori del volume del traffico registrati dopo l'installazione di Network Agent e Kaspersky Endpoint Security for Windows nel dispositivo client (vedere la tabella seguente).

Network Agent viene installato utilizzando l'installazione forzata, in cui i file necessari per l'installazione vengono copiati da Administration Server in una cartella condivisa nel dispositivo client. Al termine dell'installazione, Network Agent recupera il pacchetto di distribuzione di Kaspersky Endpoint Security for Windows utilizzando la connessione ad Administration Server.

Traffico

Scenario	Installazione di Network Agent per un singolo dispositivo client	Installazione di Kaspersky Endpoint Security for Windows in un dispositivo client (con database aggiornati)	Installazione simultanea di Network Agent e Kaspersky Endpoint Security for Windows
Traffico da un dispositivo client ad Administration Server, KB	1638,4	7843,84	9707,52
Traffico da Administration Server a un dispositivo client, KB	69.990,4	259.317,76	329.318,4
Traffico totale (per un singolo dispositivo client), KB	71.628,8	267.161,6	339.025,92

Dopo l'installazione di Network Agent nei dispositivi client, a uno dei dispositivi nel gruppo di amministrazione può essere assegnato il ruolo di punto di distribuzione. Questo viene utilizzato per la distribuzione dei pacchetti di installazione. In questo caso, il volume di traffico trasferito durante la distribuzione iniziale della protezione anti-virus varia in modo significativo a seconda del fatto che si utilizzi o meno la modalità IP multicast.

Se viene utilizzata la modalità IP multicast, i pacchetti di installazione vengono inviati una sola volta a tutti i dispositivi in esecuzione nel gruppo di amministrazione. Il traffico totale si riduce quindi di N volte, dove N è il numero totale di dispositivi in esecuzione nel gruppo di amministrazione. Se non si utilizza la modalità IP multicast, il traffico totale è identico al traffico calcolato quando i pacchetti di distribuzione vengono scaricati da Administration Server. Tuttavia, l'origine dei pacchetti è il punto di distribuzione anziché Administration Server.

Aggiornamento iniziale dei database anti-virus

I valori del traffico durante l'aggiornamento iniziale dei database anti-virus (al primo avvio dell'attività di aggiornamento del database in un dispositivo client) sono i seguenti:

- Traffico da un dispositivo client ad Administration Server: 1,8 MB.
- Traffico da Administration Server a un dispositivo client: 113 MB.
- Traffico totale (per un singolo dispositivo client): 114 MB.

I dati possono variare leggermente a seconda della versione corrente del database anti-virus.

Sincronizzazione di un client con Administration Server

Questo scenario descrive lo stato del sistema di amministrazione nei casi in cui si verifica una sincronizzazione intensiva dei dati tra un dispositivo client e Administration Server. I dispositivi client si connettono ad Administration Server in base all'intervallo definito dall'amministratore. Administration Server confronta lo stato dei dati in un dispositivo client con quello sul server, registra le informazioni nel database sull'ultima connessione del dispositivo client e sincronizza i dati.

Questa sezione contiene informazioni sui valori del traffico per scenari di amministrazione di base durante la connessione di un client ad Administration Server (vedere la tabella seguente). I dati nella tabella possono variare leggermente a seconda della versione corrente del database anti-virus.

Traffico

Scenario	Traffico dai dispositivi client ad Administration Server, KB	Traffico da Administration Server ai dispositivi client, KB	Traffico totale (per un singolo dispositivo client), KB
Sincronizzazione iniziale prima dell'aggiornamento dei database in un dispositivo client	699,44	568,42	1267,86
Sincronizzazione iniziale dopo l'aggiornamento dei database in un dispositivo client	735,8	4474,88	5210,68
Sincronizzazione senza modifiche in un dispositivo client e Administration Server	11,99	6,73	18,72

Sincronizzazione dopo la modifica del valore di un'impostazione in un criterio di gruppo	9,79	11,39	21,18
Sincronizzazione dopo la modifica del valore di un'impostazione in un'attività di gruppo	11,27	11,72	22,99
Sincronizzazione forzata senza modifiche in un dispositivo client	77,59	99,45	177,04

Il volume del traffico complessivo varia considerevolmente a seconda dell'utilizzo della modalità IP multicast nei gruppi di amministrazione. Se si utilizza la modalità IP multicast, il volume di traffico totale diminuisce approssimativamente di N volte per il gruppo, dove N sta per il numero totale di dispositivi inclusi nel gruppo di amministrazione.

Il volume di traffico al momento della sincronizzazione iniziale prima e dopo un aggiornamento dei database è specificato per i seguenti casi:

- Installazione di Network Agent e di un'applicazione di protezione in un dispositivo client
- Trasferimento di un dispositivo client in un gruppo di amministrazione
- Applicazione in un dispositivo client di un criterio e delle attività che sono state create per il gruppo per impostazione predefinita

Questa tabella specifica i valori del traffico in caso di modifiche di una delle impostazioni di protezione incluse nelle impostazioni del criterio di Kaspersky Endpoint Security. I dati per le altre impostazioni dei criteri possono risultare diversi da quelli riportati nella tabella.

Aggiornamento aggiuntivo dei database anti-virus

I valori del traffico in caso di aggiornamento incrementale dei database anti-virus 20 ore dopo l'aggiornamento precedente sono i seguenti:

- Traffico da un dispositivo client ad Administration Server: 169 KB.
- Traffico da Administration Server a un dispositivo client: 16 MB.
- Traffico totale (per un singolo dispositivo client): 16,3 MB.

I dati nella tabella possono variare leggermente a seconda della versione corrente del database anti-virus.

Il volume del traffico varia considerevolmente a seconda dell'utilizzo della modalità IP multicast nei gruppi di amministrazione. Se si utilizza la modalità IP multicast, il volume di traffico totale diminuisce approssimativamente di N volte per il gruppo, dove N sta per il numero totale di dispositivi inclusi nel gruppo di amministrazione.

Elaborazione di eventi nei client da parte di Administration Server

In questa sezione vengono fornite informazioni sui valori del traffico quando in un dispositivo client si verifica un evento di rilevamento di virus, che viene quindi inviato ad Administration Server e registrato nel database (vedere la tabella seguente).

Traffico

Scenario	Trasferimento di dati ad Administration Server quando si verifica un evento "Individuato virus"	Trasferimento di dati ad Administration Server quando si verificano nove eventi "Individuato virus"
Traffico da un dispositivo client ad Administration Server, KB	49,66	64,05
Traffico da Administration Server a un dispositivo client, KB	28,64	31,97
Traffico totale (per un singolo dispositivo client), KB	78,3	96,02

I dati nella tabella possono variare leggermente a seconda della versione corrente dell'applicazione anti-virus e degli eventi definiti nel relativo criterio per la registrazione nel database di Administration Server.

Traffico nell'arco di 24 ore

Questa sezione contiene informazioni sui valori del traffico per 24 ore di attività del sistema di amministrazione in condizione di "inattività", quando non vengono apportate modifiche ai dati né dai dispositivi client né da Administration Server (vedere la tabella seguente).

I dati presentati nella tabella descrivono la condizione della rete dopo l'installazione standard di Kaspersky Security Center e il completamento dell'Avvio rapido guidato. La frequenza di sincronizzazione del dispositivo client con Administration Server era di 20 minuti; gli aggiornamenti venivano scaricati nell'archivio di Administration Server ogni ora.

Valori del traffico per 24 ore nello stato inattivo

Flusso di traffico	Valore
Traffico da un dispositivo client ad Administration Server, KB	3235,84
Traffico da Administration Server a un dispositivo client, KB	64.378,88
Traffico totale (per un singolo dispositivo client), KB	67.614,72

Preparazione per Mobile Device Management

Questa scheda fornisce le seguenti informazioni:

- Informazioni sul server MDM iOS utilizzato per la gestione dei dispositivi iOS installando profili MDM iOS dedicati in tali dispositivi
- Informazioni sulla gestione dei dispositivi mobili in cui è installato Kaspersky Endpoint Security for Android

Server per dispositivi mobili MDM iOS

Il server MDM iOS consente di gestire i dispositivi iOS installando profili MDM iOS dedicati in tali dispositivi. Sono supportate le seguenti funzionalità:

- Blocco del dispositivo
- Reimpostazione della password
- Cancellazione dei dati
- Installazione o rimozione di app
- Utilizzo di un profilo MDM iOS con impostazioni avanzate (ad esempio per VPN, e-mail, Wi-Fi, fotocamera, certificati e così via)

Il server MDM iOS è un servizio Web che riceve le connessioni in entrata dai dispositivi mobili tramite la porta TLS (per impostazione predefinita, la porta 443), che è gestita da Kaspersky Security Center mediante Network Agent. Network Agent è installato in locale in un dispositivo in cui è distribuito un server MDM iOS.

Durante la distribuzione di un server MDM iOS, l'amministratore deve eseguire le seguenti operazioni:

- Fornire a Network Agent l'accesso all'Administration Server
- Fornire ai dispositivi mobili l'accesso alla porta TCP del server MDM iOS

In questa sezione sono descritte due configurazioni standard di un server MDM iOS.

Configurazione standard: gestione di Kaspersky Device Management for iOS nella rete perimetrale

Un server MDM iOS è posizionato nella rete perimetrale della rete locale di un'organizzazione con accesso a Internet. Una caratteristica speciale di questo approccio è l'assenza di qualsiasi problema quando i dispositivi accedono al servizio Web MDM iOS via Internet.

Poiché la gestione di un server MDM iOS richiede l'installazione di Network Agent in locale, è necessario garantire l'interazione di Network Agent con l'Administration Server. A tale scopo, è possibile utilizzare uno dei seguenti metodi:

- Spostamento di Administration Server nella rete perimetrale.
- Utilizzo di un gateway di connessione:
  a. Nel dispositivo in cui è distribuito il server MDM iOS connettere Network Agent all'Administration Server tramite un gateway di connessione.
  b. Nel dispositivo in cui è distribuito il server MDM iOS assegnare a Network Agent il ruolo di gateway di connessione.

Configurazione standard: server per dispositivi mobili MDM iOS nella rete locale di un'organizzazione

Un server per dispositivi mobili MDM iOS è posizionato nella rete interna di un'organizzazione. La porta 443 (porta predefinita) deve essere abilitata per l'accesso esterno, ad esempio pubblicando il servizio Web MDM iOS nel proxy inverso che supporta la delega vincolata Kerberos.

Qualsiasi configurazione standard richiede l'accesso ai servizi Web di Apple per il server MDM iOS (intervallo 17.0.0.0/8) tramite la porta TCP 2197. La porta viene utilizzata per informare i dispositivi dei nuovi comandi tramite un servizio dedicato denominato APNs.

Gestione dei dispositivi mobili con Kaspersky Endpoint Security for Android

I dispositivi mobili in cui è installato Kaspersky Endpoint Security for Android™ (di seguito denominati dispositivi KES) sono gestiti tramite l'Administration Server. Kaspersky Security Center supporta le seguenti funzionalità per la gestione dei dispositivi KES:

- Gestione dei dispositivi mobili come dispositivi client:
  - Appartenenza ai gruppi di amministrazione
  - Monitoraggio, ad esempio la visualizzazione di stati, eventi e rapporti
  - Modifica delle impostazioni locali e assegnazione di criteri per Kaspersky Endpoint Security for Android
- Invio di comandi in modalità centralizzata
- Installazione remota di pacchetti app mobili

Administration Server gestisce i dispositivi KES tramite TLS, porta TCP 13292.

Informazioni sulle prestazioni di Administration Server

Questa sezione presenta i risultati dei test sulle prestazioni di Administration Server per differenti configurazioni hardware e le limitazioni per la connessione dei dispositivi gestiti all'Administration Server.

Limitazioni relative alla connessione a un Administration Server

Un Administration Server supporta la gestione di un massimo di 100000 dispositivi senza compromettere le prestazioni.

Limitazioni per le connessioni a un Administration Server senza compromettere le prestazioni:

- Un solo Administration Server può supportare fino a 500 Administration Server virtuali.
- L'Administration Server primario supporta non più di 1000 sessioni contemporaneamente.
- Gli Administration Server virtuali supportano non più di 1000 sessioni contemporaneamente.

Risultati dei test sulle prestazioni di Administration Server

I risultati dei test sulle prestazioni di Administration Server hanno consentito di determinare il numero massimo di dispositivi client con cui Administration Server può essere sincronizzato per gli intervalli di tempo specificati. È possibile utilizzare queste informazioni per selezionare lo schema ottimale per la distribuzione della protezione anti-virus nelle reti di computer.

I dispositivi con le seguenti configurazioni hardware (vedere le seguenti tabelle) sono stati utilizzati per i test:

Configurazione hardware di Administration Server

Parametro	Valore
CPU	Intel Xeon CPU E5630, velocità di clock di 2,53 GHz, 2 socket, 8 core, 16 processori logici
RAM	26 GB
Disco rigido	Dispositivo disco IBM ServeRAID M5014, 487 GB
Sistema operativo	Microsoft Windows Server 2019 Standard, versione 10.0.17763, build 17763
Rete	QLogic BCM5709C Gigabit Ethernet (client NDIS VBD)

Configurazione hardware del dispositivo SQL Server

Parametro	Valore
CPU	Intel Xeon CPU X5570, velocità di clock di 2,93 GHz, 2 socket, 8 core, 16 processori logici
RAM	32 GB
Disco rigido	Adaptec Array SCSI Disk Device, 2047 GB
Sistema operativo	Microsoft Windows Server 2019 Standard, versione 10.0.17763, build 17763
Rete	Intel 82576 Gigabit

Administration Server supportava la creazione di 500 Administration Server virtuali.

L'intervallo di sincronizzazione era di 15 minuti per ogni 10.000 dispositivi gestiti (vedere la tabella di seguito).

Riepilogo dei risultati dei test di carico di Administration Server

Intervallo di sincronizzazione (min.)	Numero di dispositivi gestiti
15	10.000
30	20.000
45	30.000
60	40.000
75	50.000
90	60.000
105	70.000
120	80.000
135	90.000
150	100.000

Se si connette Administration Server a un server database MySQL o SQL Express, è consigliabile evitare di utilizzare l'applicazione per gestire più di 10000 dispositivi. Per il sistema di gestione database MariaDB, il numero massimo di dispositivi gestiti consigliato è 20.000.

Risultati dei test sulle prestazioni del server proxy KSN

Se la rete aziendale include una grande quantità di dispositivi client che utilizzano Administration Server come server proxy KSN, l'hardware di Administration Server deve soddisfare requisiti specifici per essere in grado di elaborare le richieste provenienti dai dispositivi client. È possibile utilizzare i risultati dei test di seguito per valutare il carico di Administration Server nella rete e pianificare le risorse hardware per garantire il corretto funzionamento del servizio proxy KSN.

Le seguenti tabelle mostrano la configurazione hardware di Administration Server e SQL Server. Questa configurazione è stata utilizzata per i test.

Configurazione hardware di Administration Server

Parametro	Valore
CPU	Intel Xeon CPU E5450, velocità di clock di 3 GHz, 2 socket, 8 core, 16 processori logici
RAM	32 GB
Sistema operativo	Microsoft Windows Server 2016 Standard

Configurazione hardware di SQL Server

Parametro	Valore
CPU	Intel Xeon CPU E5450, velocità di clock di 3 GHz, 2 socket, 8 core, 16 processori logici
RAM	32 GB
Sistema operativo	Microsoft Windows Server 2019 Standard

La tabella seguente consente di visualizzare i risultati del test.

Riepilogo dei risultati dei test sulle prestazioni del server proxy KSN

Parametro	Valore
Numero massimo di richieste elaborate al secondo	4914
Utilizzo massimo della CPU	36%

Impostazioni di rete per l'interazione con servizi esterni

Kaspersky Security Center utilizza le seguenti impostazioni di rete per l'interazione con i servizi esterni.

Impostazioni di rete	Indirizzo	Descrizione
Porta: 443 Protocollo: HTTPS	activation-v2.kaspersky.com	Attivazione dell'applicazione.
Porta: 443 Protocollo: HTTPS	https://s00.upd.kaspersky.com https://s01.upd.kaspersky.com https://s02.upd.kaspersky.com https://s03.upd.kaspersky.com https://s04.upd.kaspersky.com https://s05.upd.kaspersky.com https://s06.upd.kaspersky.com https://s07.upd.kaspersky.com https://s08.upd.kaspersky.com https://s09.upd.kaspersky.com https://s10.upd.kaspersky.com https://s11.upd.kaspersky.com https://s12.upd.kaspersky.com https://s13.upd.kaspersky.com https://s14.upd.kaspersky.com https://s15.upd.kaspersky.com https://s16.upd.kaspersky.com https://s17.upd.kaspersky.com https://s18.upd.kaspersky.com https://s19.upd.kaspersky.com https://cm.k.kaspersky-labs.com	Aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky.
Porta: 443 Protocollo: HTTPS	https://downloads.upd.kaspersky.com	• Aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky. • Verifica dell'accessibilità dei server Kaspersky. Prima di scaricare i database e i moduli software di Kaspersky, Kaspersky Security Center verifica se i server Kaspersky sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici.

Impostazioni di rete	Indirizzo	Descrizione
Porta: 80 Protocollo: HTTP	http://p00.upd.kaspersky.com http://p01.upd.kaspersky.com http://p02.upd.kaspersky.com http://p03.upd.kaspersky.com http://p04.upd.kaspersky.com http://p05.upd.kaspersky.com http://p06.upd.kaspersky.com http://p07.upd.kaspersky.com http://p08.upd.kaspersky.com http://p09.upd.kaspersky.com http://p10.upd.kaspersky.com http://p11.upd.kaspersky.com http://p12.upd.kaspersky.com http://p13.upd.kaspersky.com http://p14.upd.kaspersky.com http://p15.upd.kaspersky.com http://p16.upd.kaspersky.com http://p17.upd.kaspersky.com http://p18.upd.kaspersky.com http://p19.upd.kaspersky.com http://downloads0.kaspersky-labs.com http://downloads1.kaspersky-labs.com http://downloads2.kaspersky-labs.com http://downloads3.kaspersky-labs.com http://downloads4.kaspersky-labs.com http://downloads5.kaspersky-labs.com http://downloads6.kaspersky-labs.com http://downloads7.kaspersky-labs.com http://downloads8.kaspersky-labs.com http://downloads9.kaspersky-labs.com http://downloads.kaspersky-labs.com http://cm.k.kaspersky-labs.com	Aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky.
Porta: 443 Protocollo: HTTPS	ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com	Utilizzo di Kaspersky Security Network.
Porto: 443, 1443 Protocollo: HTTPS	ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com	Utilizzo di Kaspersky Security Network.
Porta: 443 Protocollo: HTTPS	click.kaspersky.com redirect.kaspersky.com	Visita dei collegamenti sull'interfaccia.

Impostazioni di rete	Indirizzo	Descrizione
Porta: 80 Protocollo: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Questi server fanno parte della Public Key Infrastructure (PKI) e sono necessari per verificare lo stato di validità dei certificati di firma digitale Kaspersky. Il CRL è un elenco di certificati revocati. L'OCSP consente di richiedere lo stato di uno specifico certificato in tempo reale. Questi server aiutano a garantire la sicurezza dell'interazione con i certificati digitali e a proteggersi da possibili attacchi.
Porta: 443 Protocollo: HTTPS	https://ipm-klca.kaspersky.com	Annunci di marketing.

Per una corretta interazione di Kaspersky Security Center con i servizi esterni, tenere conto dei seguenti suggerimenti:
- Il traffico di rete non criptato deve essere consentito sulle porte 443 e 1443 dell'apparecchiatura di rete e del server proxy dell'organizzazione.
- Quando Administration Server interagisce con i server di aggiornamento Kaspersky e con i server di Kaspersky Security Network, è necessario evitare di dirottare il traffico di rete con la sostituzione del certificato (attacchi MITM).

Per scaricare gli aggiornamenti tramite il protocollo HTTP o HTTPS utilizzando l'utilità klscflag:

1. Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

2. Se si desidera scaricare gli aggiornamenti tramite il protocollo HTTP, eseguire uno dei seguenti comandi:

   - Nel dispositivo in cui è installato Administration Server:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Su un punto di distribuzione;

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Se si desidera scaricare gli aggiornamenti tramite il protocollo HTTPS, eseguire uno dei seguenti comandi:

   - Nel dispositivo in cui è installato Administration Server:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - Su un punto di distribuzione;

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Distribuzione di Network Agent e dell'applicazione di protezione

Per gestire i dispositivi in un'organizzazione, è necessario installare Network Agent su ciascuno di essi. La distribuzione di Kaspersky Security Center nei dispositivi di un'organizzazione in genere ha inizio con l'installazione di Network Agent nei dispositivi.

In Microsoft Windows XP Network Agent potrebbe non eseguire correttamente le seguenti operazioni: download degli aggiornamenti direttamente dai server di Kaspersky (come punto di distribuzione); funzionamento come un server proxy KSN (come punto di distribuzione); e rilevamento di vulnerabilità di terze parti (se è in uso Vulnerability e patch management).

Distribuzione iniziale

Per gestire i dispositivi in un'organizzazione, è necessario installare Network Agent su ciascun dispositivo.

L'installazione di Network Agent nel dispositivo gestito che esegue Windows può essere effettuata nei seguenti modi:

- Con strumenti di terze parti per l'installazione remota delle applicazioni.
- Clonando un'immagine del disco rigido dell'amministratore con il sistema operativo e Network Agent, utilizzando gli strumenti forniti da Kaspersky Security Center per la gestione delle immagini disco o con strumenti di terze parti.
- Con i criteri di gruppo di Windows, utilizzando gli strumenti di gestione standard di Windows per i criteri di gruppo o in modalità automatica, attraverso l'apposita opzione corrispondente nell'attività di installazione remota di Kaspersky Security Center.
- In modalità forzata, utilizzando le risorse del sistema operativo tramite l'attività di installazione remota di Kaspersky Security Center.
- Inviando agli utenti dei dispositivi collegamenti ai pacchetti indipendenti generati da Kaspersky Security Center. I pacchetti indipendenti sono moduli eseguibili che contengono i pacchetti di distribuzione delle applicazioni selezionate con le relative impostazioni definite.
- Manualmente, eseguendo i programmi di installazione delle applicazioni nei dispositivi.

L'installazione iniziale di Network Agent nel dispositivo gestito Linux può essere effettuata nei seguenti modi:

- Collegandosi al dispositivo gestito tramite SSH ed eseguendo l'attività di installazione remota.
- Eseguendo l'installazione del pacchetto nel dispositivo gestito.

L'installazione iniziale di Network Agent nel dispositivo gestito macOS può essere effettuata nei seguenti modi:

- Eseguendo l'attività di installazione remota nel punto di distribuzione macOS.
- Inviando agli utenti dei dispositivi collegamenti ai pacchetti indipendenti generati da Kaspersky Security Center. I pacchetti indipendenti sono moduli eseguibili che contengono i pacchetti di distribuzione delle applicazioni selezionate, con le impostazioni predefinite.

Dopo aver installato Network Agent su un dispositivo, è possibile eseguire l'installazione remota delle applicazioni Kaspersky su tale dispositivo tramite Network Agent. Il pacchetto di distribuzione di un'applicazione da installare viene trasferito mediante i canali di comunicazione tra i Network Agent e Administration Server, insieme alle impostazioni di installazione definite dall'amministratore. Per trasferire il pacchetto di distribuzione, è possibile utilizzare nodi di distribuzione per il trasferimento, cioè punti di distribuzione, recapito multicast e così via.

Al momento della scelta di un metodo e di una strategia per la distribuzione delle applicazioni in una rete gestita, è necessario considerare diversi fattori (elenco parziale):

- Configurazione della rete dell'organizzazione.
- Numero totale di dispositivi.
- Presenza nella rete dell'organizzazione di dispositivi che non appartengono ad alcun dominio Active Directory e presenza di account uniformi con diritti di amministratore su tali dispositivi.
- Capacità del canale tra l'Administration Server e i dispositivi.
- Tipo di comunicazione tra Administration Server e le subnet remote e capacità dei canali di rete in tali subnet.
- Impostazioni di sicurezza applicate sui dispositivi remoti all'inizio della distribuzione. Questi parametri consentono di stabilire la connessione remota al dispositivo gestito e di avviare il programma di installazione.

Configurazione dei programmi di installazione

Prima di avviare la distribuzione delle applicazioni Kaspersky in una rete, è necessario specificare le impostazioni di installazione, ovvero quelle definite durante l'installazione dell'applicazione. Durante l'installazione di Network Agent, è necessario specificare almeno un indirizzo per la connessione ad Administration Server, tuttavia possono essere richieste anche alcune impostazioni avanzate. A seconda del metodo di installazione selezionato, è possibile definire le impostazioni in diversi modi. Nel caso più semplice (installazione interattiva manuale in un dispositivo selezionato), tutte le impostazioni appropriate possono essere definite attraverso l'interfaccia utente del programma di installazione.

Questo metodo per definire le impostazioni non è appropriato per l'installazione automatica delle applicazioni in gruppi di dispositivi. In generale, l'amministratore deve specificare i valori per le impostazioni in modalità centralizzata. Tali valori possono successivamente essere utilizzati per l'installazione automatica nei dispositivi della rete selezionati.

Pacchetti di installazione

Il metodo principale per definire le impostazioni di installazione delle applicazioni è adatto per tutti i metodi di installazione, sia con gli strumenti di Kaspersky Security Center che con la maggior parte strumenti di terze parti. Questo metodo consiste nella creazione di pacchetti di installazione delle applicazioni in Kaspersky Security Center.

I pacchetti di installazione sono generati utilizzando i seguenti metodi:

- Automaticamente, dai pacchetti di distribuzione specificati, in base ai *descrittori* inclusi (file con estensione kud che contengono regole per l'installazione e l'analisi dei risultati e altre informazioni)
- Dai file eseguibili dei programmi di installazione o dai programmi di installazione in formato nativo (.msi, .deb, .rpm) per le applicazioni standard o supportate

I pacchetti di installazione generati sono organizzati gerarchicamente come cartelle con sottocartelle e file. Oltre al pacchetto di distribuzione originale, un pacchetto di installazione contiene impostazioni modificabili (incluse le impostazioni del programma di installazione e le regole per elaborare casi come la necessità di riavviare il sistema operativo per completare l'installazione), nonché moduli ausiliari minori.

I valori delle impostazioni di installazione specifici per una singola applicazione supportata possono essere definiti nell'interfaccia utente di Administration Console al momento della creazione del pacchetto di installazione. Durante l'esecuzione dell'installazione remota delle applicazioni tramite gli strumenti di Kaspersky Security Center, i pacchetti di installazione vengono inviati ai dispositivi. L'esecuzione del programma di installazione di un'applicazione rende disponibili tutte le impostazioni definite dall'amministratore per tale applicazione. Quando si utilizzano strumenti di terze parti per l'installazione delle applicazioni Kaspersky, è sufficiente garantire la disponibilità dell'intero pacchetto di installazione nel dispositivo, ovvero la disponibilità del pacchetto di distribuzione e delle relative impostazioni. I pacchetti di installazione vengono creati e archiviati da Kaspersky Security Center in un'apposita sottocartella della cartella condivisa.

Non specificare dettagli degli account privilegiati nei parametri dei pacchetti di installazione.

Per istruzioni sull'utilizzo di questo metodo di configurazione per le applicazioni Kaspersky prima della distribuzione mediante strumenti di terze parti, vedere la sezione "Distribuzione tramite i criteri di gruppo di Microsoft Windows".

Subito dopo l'installazione di Kaspersky Security Center, alcuni pacchetti di installazione vengono generati automaticamente: sono pronti per l'installazione e includono i pacchetti di Network Agent e i pacchetti delle applicazioni di protezione per Microsoft Windows.

Anche se è possibile impostare la chiave di licenza per un'applicazione nelle proprietà di un pacchetto di installazione, è consigliabile evitare questo metodo di distribuzione della licenza, perché è semplice ottenere l'accesso in lettura ai pacchetti di installazione. È necessario utilizzare chiavi di licenza distribuite automaticamente o le attività di installazione per le chiavi di licenza.

Proprietà e file di trasformazione MSI

Un altro modo per configurare l'installazione nella piattaforma Windows è definire le proprietà e i file di trasformazione MSI. Questo metodo può essere applicato nei seguenti casi:

- Durante l'installazione tramite i criteri di gruppo di Windows, utilizzando gli strumenti standard di Microsoft o altri strumenti di terze parti per la gestione dei criteri di gruppo di Windows.
- Durante l'installazione delle applicazioni tramite strumenti di terze parti per la gestione dei programmi di installazione in formato Microsoft Installer.

Distribuzione con strumenti di terze parti per l'installazione remota delle applicazioni

Se nell'organizzazione sono disponibili strumenti per l'installazione remota delle applicazioni (ad esempio, Microsoft System Center), è possibile eseguire la distribuzione iniziale utilizzando tali strumenti.

È necessario eseguire le seguenti operazioni:

- Selezionare il metodo per la configurazione dell'installazione più adatto per lo strumento di distribuzione da utilizzare.
- Definire il meccanismo per la sincronizzazione tra la modifica delle impostazioni dei pacchetti di installazione (attraverso l'interfaccia di Administration Console) e l'esecuzione degli strumenti di terze parti selezionati utilizzati per la distribuzione delle applicazioni dai dati dei pacchetti di installazione.
- Durante l'esecuzione dell'installazione da una cartella condivisa, è necessario assicurarsi che tale risorsa file abbia una capacità sufficiente.

Informazioni sulle attività di installazione remota in Kaspersky Security Center

Kaspersky Security Center fornisce diversi meccanismi per l'installazione remota delle applicazioni, che sono implementati come attività di installazione remota (installazione forzata, installazione tramite copia di un'immagine del disco rigido, installazione tramite i criteri di gruppo di Microsoft Windows). È possibile creare un'attività di installazione remota sia per un gruppo di amministrazione specificato che per dispositivi specifici o per una selezione di dispositivi (tali attività sono visualizzate in Administration Console, nella cartella **Attività**). Durante la creazione di un'attività, è possibile selezionare i pacchetti di installazione (quelli di Network Agent e/o di un'altra applicazione) per l'installazione con questa attività, nonché specificare determinate impostazioni che definiscono il metodo di installazione remota. È inoltre possibile utilizzare l'Installazione remota guidata, che è basata sulla creazione di un'attività di installazione remota e sul monitoraggio dei risultati.

Le attività per i gruppi di amministrazione influiscono sia sui dispositivi inclusi in un gruppo specificato che su tutti i dispositivi in tutti i sottogruppi compresi in tale gruppo di amministrazione. Un'attività copre i dispositivi degli Administration Server secondari inclusi in un gruppo o in qualsiasi dei relativi sottogruppi se l'impostazione corrispondente è abilitata nell'attività.

Le attività per dispositivi specifici aggiornano l'elenco dei dispositivi client a ogni esecuzione, in conformità con i contenuti della selezione al momento dell'avvio dell'attività. Se una selezione include dispositivi che sono stati connessi ad Administration Server secondari, l'attività verrà eseguita anche in tali dispositivi. Per informazioni dettagliate sulle impostazioni e i metodi di installazione, vedere più avanti in questa sezione.

Per garantire la corretta esecuzione di un'attività di installazione remota nei dispositivi connessi agli Administration Server secondari, è necessario utilizzare l'attività di trasmissione per trasferire anticipatamente i pacchetti di installazione utilizzati dall'attività agli Administration Server secondari corrispondenti.

Distribuzione tramite l'acquisizione e la copia dell'immagine di un dispositivo

Se Network Agent deve essere installato in dispositivi in cui è necessario installare (o reinstallare) anche un sistema operativo e altro software, è possibile utilizzare il meccanismo di acquisizione e copia dell'immagine del dispositivo.

Per eseguire la distribuzione acquisendo e copiando un disco rigido:

1. Creare un dispositivo "di riferimento" con un sistema operativo e il software appropriato installato, incluso Network Agent e un'applicazione di protezione.

2. Acquisire l'immagine di riferimento nel dispositivo e distribuire tale immagine nei nuovi dispositivi tramite l'attività dedicata di Kaspersky Security Center.

   Per acquisire e installare le immagini disco, è possibile utilizzare gli strumenti di terze parti disponibili nell'organizzazione o la funzionalità fornita (con la licenza Vulnerability e patch management) da Kaspersky Security Center.

Se si utilizza uno strumento di terze parti per elaborare le immagini disco, è necessario eliminare le informazioni utilizzate da Kaspersky Security Center per identificare il dispositivo gestito, al momento della distribuzione in un dispositivo da un'immagine di riferimento. In caso contrario, Administration Server non sarà in grado di distinguere correttamente i dispositivi che sono stati creati copiando la stessa immagine.

In caso di acquisizione di un'immagine disco con gli strumenti di Kaspersky Security Center, questo problema viene risolto automaticamente.

Copia di un'immagine disco con strumenti di terze parti

Quando si applicano strumenti di terze parti per l'acquisizione dell'immagine di un dispositivo con Network Agent installato, utilizzare uno dei seguenti metodi:

- Metodo consigliato. Durante l'installazione di Network Agent in un dispositivo di riferimento acquisire l'immagine del dispositivo prima della prima esecuzione del servizio Network Agent (perché le informazioni univoche che identificano il dispositivo vengono create alla prima connessione di Network Agent ad Administration Server). È quindi consigliabile evitare di eseguire il servizio Network Agent fino al completamento dell'operazione di acquisizione dell'immagine.

- Sul dispositivo di riferimento, interrompere il servizio Network Agent ed eseguire l'utilità klmover con l'opzione -dupfix. L'utilità klmover è inclusa nel pacchetto di installazione di Network Agent. Evitare qualsiasi successiva esecuzione del servizio Network Agent finché l'operazione di acquisizione dell'immagine non viene completata.

- Verificare che l'utilità klmover venga eseguita con l'opzione -dupfix prima (requisito obbligatorio) della prima esecuzione del servizio Network Agent nei dispositivi di destinazione, al primo avvio del sistema operativo dopo la distribuzione dell'immagine. L'utilità klmover è inclusa nel pacchetto di installazione di Network Agent.

- Utilizzare la modalità di clonazione del disco di Network Agent.

Se l'immagine del disco rigido è stata copiata in modo errato, è possibile risolvere il problema.

È inoltre possibile acquisire l'immagine di un dispositivo senza Network Agent installato. A tale scopo, eseguire la distribuzione dell'immagine nei dispositivi di destinazione, quindi distribuire Network Agent. Se si utilizza questo metodo, fornire l'accesso alla cartella di rete con i pacchetti di installazione indipendenti da un dispositivo.

Errori di copia di un'immagine del disco rigido

Se è stata copiata un'immagine del disco rigido in cui è installato Network Agent senza seguire le regole di distribuzione, alcuni dispositivi possono essere visualizzati insieme in Administration Console con un'unica icona e con un nome che subisce continue variazioni.

È possibile risolvere il problema utilizzando uno dei seguenti metodi:

- Rimozione di Network Agent

  Questo metodo è il più affidabile. È necessario rimuovere Network Agent dai dispositivi che sono stati copiati in modo errato dall'immagine, utilizzando strumenti di terze parti, e quindi installarlo di nuovo. Network Agent non può essere rimosso tramite gli strumenti di Kaspersky Security Center, perché Administration Server non può distinguere fra i dispositivi in errore (tutti condividono la stessa icona in Administration Console).

- Esecuzione dell'utilità klmover con l'opzione "-dupfix"

  Utilizzare strumenti di terze parti per eseguire una volta l'utilità klmover, disponibile nella cartella di installazione di Network Agent, con l'opzione "-dupfix" (klmover-dupfix) nei dispositivi in errore (quelli copiati in modo errato dall'immagine). Non è possibile eseguire l'utilità tramite gli strumenti di Kaspersky Security Center, perché Administration Server non può distinguere fra i dispositivi in errore (tutti condividono la stessa icona in Administration Console).

  Eliminare quindi l'icona con cui erano visualizzati i dispositivi in errore prima dell'esecuzione dell'utilità.

- Modifica della regola per il rilevamento dei dispositivi copiati in modo errato.

  > Questo metodo è applicabile solo se sono installati Administration Server e Network Agent versione 10 Service Pack 1 o successiva.

  La regola per il rilevamento dei Network Agent copiati in modo errato deve essere modificata in modo che la modifica del nome NetBIOS di un dispositivo determini una "correzione" automatica di tali Network Agent (presupponendo che tutti i dispositivi copiati abbiano nomi NetBIOS univoci).

  Nel dispositivo con Administration Server è necessario importare nel Registro di sistema il file reg indicato di seguito e quindi riavviare il servizio Administration Server.

  - Se nel dispositivo con Administration Server è installato un sistema operativo a 32 bit:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

  - Se nel dispositivo con Administration Server è installato un sistema operativo a 64 bit:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

Distribuzione tramite i criteri di gruppo di Microsoft Windows

È consigliabile eseguire la distribuzione iniziale dei Network Agent tramite i criteri di gruppo di Microsoft Windows se sono soddisfatte le seguenti condizioni:

- Il dispositivo fa parte di un dominio Active Directory.
- Lo schema di distribuzione consente di attendere il successivo riavvio abituale dei dispositivi di destinazione prima di avviare la distribuzione nei Network Agent su di essi (oppure è possibile forzare l'applicazione di un criterio di gruppo di Windows in tali dispositivi).

Questo schema di distribuzione comprende quanto segue:

- Il pacchetto di distribuzione dell'applicazione in formato Microsoft Installer (pacchetto MSI) è disponibile in una cartella condivisa (una cartella per cui gli account LocalSystem dei dispositivi di destinazione dispongono di autorizzazioni di lettura).
- Nel criterio di gruppo di Active Directory, viene creato un oggetto di installazione per il pacchetto di distribuzione.
- L'ambito di installazione è impostato specificando l'unità organizzativa (UO) e / o il gruppo di protezione che include i dispositivi di destinazione.
- Al successivo accesso al dominio di un dispositivo di destinazione (prima che gli utenti del dispositivo accedano al sistema), tutte le applicazioni installate vengono esaminate per verificare che sia presente l'applicazione richiesta. Se l'applicazione non viene trovata, il pacchetto di distribuzione viene scaricato dalla risorsa specificata nel criterio e quindi viene installato.

Un vantaggio di questo schema di distribuzione è il fatto che le applicazioni assegnate sono installate nei dispositivi di destinazione durante il caricamento del sistema operativo, prima che l'utente acceda al sistema. Anche se un utente con diritti sufficienti rimuove l'applicazione, questa sarà reinstallata al successivo avvio del sistema operativo. Lo svantaggio di questo schema di distribuzione è che le modifiche apportate dall'amministratore al criterio di gruppo non hanno effetto finché i dispositivi non vengono riavviati (se non vengono utilizzati strumenti aggiuntivi).

È possibile utilizzare i criteri di gruppo per installare sia Network Agent che altre applicazioni se i relativi programmi di installazione sono in formato Windows Installer.

Quando si seleziona questo schema di distribuzione, è anche necessario valutare il carico sulla risorsa file da cui saranno copiati i file nei dispositivi dopo l'applicazione del criterio di gruppo di Windows.

Gestione dei criteri di Microsoft Windows tramite l'attività di installazione remota di Kaspersky Security Center

Il modo più semplice per installare le applicazioni tramite i criteri di gruppo di Microsoft Windows è selezionare l'opzione **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory** nelle proprietà dell'attività di installazione remota di Kaspersky Security Center. In questo caso, Administration Server esegue automaticamente le azioni seguenti durante l'esecuzione dell'attività:

- Crea gli oggetti richiesti nel criterio di gruppo di Microsoft Windows.
- Crea gruppi di protezione dedicati, include i dispositivi di destinazione in tali gruppi e assegna l'installazione delle applicazioni selezionate per i dispositivi. Il set di gruppi di protezione sarà aggiornato a ogni esecuzione

dell'attività, in base al pool di dispositivi al momento dell'esecuzione.

Per rendere disponibile questa funzionalità, nelle proprietà dell'attività specificare un account con autorizzazioni di scrittura nei criteri di gruppo di Active Directory.

Se si prevede di installare sia Network Agent che un'altra applicazione tramite la stessa attività, la selezione dell'opzione **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory** determina la creazione di un oggetto di installazione nel criterio di Active Directory solo per Network Agent. La seconda applicazione selezionata nell'attività sarà installata tramite gli strumenti di Network Agent non appena quest'ultimo viene installato nel dispositivo. Se si desidera installare un'applicazione diversa da Network Agent tramite i criteri di gruppo di Windows, è necessario creare un'attività di installazione solo per tale pacchetto di installazione (senza il pacchetto di Network Agent). Non tutte le applicazioni possono essere installate utilizzando i criteri di gruppo Microsoft Windows. Per ottenere informazioni su questa funzionalità, è possibile fare riferimento alle informazioni sui possibili metodi per installare l'applicazione.

Se gli oggetti richiesti sono creati nel criterio di gruppo utilizzando gli strumenti di Kaspersky Security Center, verrà utilizzata la cartella condivisa di Kaspersky Security Center come origine del pacchetto di installazione. Durante la pianificazione della distribuzione, è necessario correlare la velocità di lettura per questa cartella con il numero di dispositivi e le dimensioni del pacchetto di distribuzione da installare. Può essere utile posizionare la cartella condivisa di Kaspersky Security Center in un archivio di file dedicato a elevate prestazioni.

Oltre alla sua facilità di utilizzo, la creazione automatica dei criteri di gruppo di Windows tramite Kaspersky Security Center offre un particolare vantaggio: durante la pianificazione dell'installazione di Network Agent, è possibile specificare facilmente il gruppo di amministrazione di Kaspersky Security Center in cui i dispositivi saranno spostati automaticamente al termine dell'installazione. È possibile specificare questo gruppo nella Creazione guidata nuova attività o nella finestra delle impostazioni dell'attività di installazione remota.

Quando si gestiscono i criteri di gruppo di Windows tramite Kaspersky Security Center, è possibile specificare i dispositivi per un oggetto criteri di gruppo creando un gruppo di protezione. Kaspersky Security Center sincronizza i contenuti del gruppo di protezione con il set corrente di dispositivi nell'attività. Utilizzando altri strumenti per gestire i criteri di gruppo, è possibile associare direttamente gli oggetti criteri di gruppo alle unità organizzative di Active Directory selezionate.

Installazione non assistita delle applicazioni tramite i criteri di Microsoft Windows

L'amministratore può creare autonomamente gli oggetti richiesti per l'installazione in un criterio di gruppo di Windows. In questo caso, può fornire collegamenti ai pacchetti archiviati nella cartella condivisa di Kaspersky Security Center oppure caricare i pacchetti su un file server dedicato e fornire collegamenti a tali pacchetti.

Sono possibili i seguenti scenari di installazione:

- L'amministratore crea un pacchetto di installazione e ne imposta le proprietà in Administration Console. L'oggetto criteri di gruppo fornisce un collegamento al file MSI di questo pacchetto archiviato nella cartella condivisa di Kaspersky Security Center.

- L'amministratore crea un pacchetto di installazione e ne imposta le proprietà in Administration Console. L'amministratore copia quindi l'intera sottocartella EXEC di questo pacchetto dalla cartella condivisa di Kaspersky Security Center in una cartella su una risorsa file dedicata dell'organizzazione. L'oggetto criteri di gruppo fornisce un collegamento al file MSI di questo pacchetto archiviato in una sottocartella sulla risorsa file dedicata dell'organizzazione.

- L'amministratore scarica da Internet il pacchetto di distribuzione dell'applicazione (incluso quello di Network Agent) e lo carica nella risorsa file dedicata dell'organizzazione. L'oggetto criteri di gruppo fornisce un collegamento al file MSI di questo pacchetto archiviato in una sottocartella sulla risorsa file dedicata dell'organizzazione. Le impostazioni di installazione sono definite configurando le proprietà MSI o configurando i file di trasformazione MST.

Distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center

Per eseguire la distribuzione iniziale di Network Agent o di altre applicazioni, è possibile forzare l'installazione dei pacchetti di installazione selezionati utilizzando l'attività di installazione remota di Kaspersky Security Center, a condizione che ogni dispositivo disponga di uno o più account utente con diritti di amministratore locali.

L'installazione forzata può anche essere applicata se i dispositivi non sono direttamente accessibili da Administration Server, ad esempio se i dispositivi sono in rete isolata o se si trovano in una rete locale mentre Administration Server è in una rete perimetrale.

In caso di distribuzione iniziale, Network Agent non è installato. Pertanto, nelle impostazioni dell'attività di installazione remota, non è possibile selezionare la distribuzione dei file richiesti per l'installazione dell'applicazione utilizzando Network Agent. È possibile scegliere di distribuire i file solo utilizzando le risorse del sistema operativo tramite Administration Server o i punti di distribuzione.

Il servizio Administration Server deve essere eseguito con un account con privilegi di amministratore nei dispositivi di destinazione. In alternativa, è possibile specificare un account che ha accesso alla condivisione admin$ nelle impostazioni dell'attività di installazione remota.

> Per impostazione predefinita, l'attività di installazione remota viene applicata ai dispositivi utilizzando le credenziali dell'account con cui è in esecuzione Administration Server. È importante chiarire che questo è l'account utilizzato per accedere alla condivisione admin$, anziché l'account con cui viene eseguita l'attività di installazione remota. L'installazione viene eseguita con l'account LocalSystem.

È possibile specificare i dispositivi di destinazione esplicitamente (con un elenco), selezionando il gruppo di amministrazione di Kaspersky Security Center a cui appartengono o creando una selezione di dispositivi in base a un criterio specifico. L'ora di inizio dell'installazione è definita dalla pianificazione dell'attività. Se l'impostazione **Esegui attività non effettuate** è abilitata nelle proprietà dell'attività, l'attività può essere eseguita subito dopo l'accensione dei dispositivi di destinazione o quando vengono spostati nel gruppo di amministrazione di destinazione.

L'installazione forzata consiste nella distribuzione dei pacchetti di installazione ai dispositivi di destinazione, nella successiva copia dei file nella risorsa admin$ in ciascuno dei dispositivi di destinazione e nella registrazione remota dei servizi di supporto in tali dispositivi. L'invio dei pacchetti di installazione ai dispositivi di destinazione viene eseguito tramite una funzionalità di Kaspersky Security Center che garantisce l'interazione di rete. In questo caso, devono essere soddisfatte le seguenti condizioni:

- I dispositivi di destinazione sono accessibili dal lato di Administration Server o dal lato del punto di distribuzione.
- La risoluzione dei nomi per i dispositivi di destinazione funziona correttamente nella rete.
- Le condivisioni amministrative (admin$) rimangono abilitate nei dispositivi di destinazione.
- I seguenti servizi di sistema sono in esecuzione nei dispositivi di destinazione:
  - Server (LanmanServer)

    Per impostazione predefinita, questo servizio è in esecuzione.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- La porta TCP 445 è aperta nei dispositivi di destinazione per abilitare l'accesso remoto tramite Windows Management Instrumentation.

  TCP 139, UDP 137 e UDP 138 vengono utilizzati dai protocolli precedenti e non sono più necessari per le applicazioni correnti.

  Le porte di accesso dinamiche in uscita devono essere consentite nel firewall per le connessioni da Administration Server e dai punti di distribuzione ai dispositivi di destinazione.
- Le impostazioni di protezione del criterio di dominio di Active Directory possono fornire il funzionamento del protocollo NTLM durante la distribuzione di Network Agent.
- Nei dispositivi di destinazione che eseguono Microsoft Windows XP, la modalità Simple File Sharing è disabilitata.
- Nei dispositivi di destinazione, il modello di protezione e condivisione dell'accesso è impostato su *Classico: gli utenti locali eseguono l'autenticazione come se stessi*. Non può in alcun modo essere *Solo Guest: gli utenti locali si autenticano come Guest*.
- I dispositivi di destinazione sono utenti del dominio o vengono creati anticipatamente account uniformi con diritti di amministratore nei dispositivi di destinazione.

Per distribuire correttamente Network Agent o altre applicazioni in un dispositivo che non fa parte di un dominio Active Directory di Windows Server 2003 o versione successiva, è necessario disabilitare Controllo dell'account utente remoto in tale dispositivo. Controllo dell'account utente remoto è uno dei motivi che impedisce agli account amministrativi locali di accedere ad admin$, necessario per la distribuzione forzata di Network Agent o di altre applicazioni. La disabilitazione di Controllo dell'account utente remoto non influisce su Controllo dell'account utente locale.

Durante l'installazione in nuovi dispositivi che non sono stati ancora assegnati ad alcun gruppo di amministrazione di Kaspersky Security Center, è possibile aprire le proprietà dell'attività di installazione remota e specificare il gruppo di amministrazione in cui spostare i dispositivi dopo l'installazione di Network Agent.

Al momento della creazione di un'attività di gruppo, tenere presente che ogni attività di gruppo influisce su tutti i dispositivi in tutti i gruppi nidificati all'interno un gruppo selezionato. È pertanto necessario evitare di duplicare le attività di installazione nei sottogruppi.

Un modo semplificato per creare attività per l'installazione forzata delle applicazioni è l'installazione automatica. A tale scopo, è necessario aprire le proprietà del gruppo di amministrazione, aprire l'elenco dei pacchetti di installazione e selezionare quelli da installare nei dispositivi di questo gruppo. I pacchetti di installazione selezionati saranno installati automaticamente in tutti i dispositivi di questo gruppo e di tutti i relativi sottogruppi. L'intervallo di tempo richiesto per l'installazione dei pacchetti dipende dalla velocità effettiva della rete e dal numero totale di dispositivi in rete.

Per ridurre il carico su Administration Server durante la distribuzione dei pacchetti di installazione ai dispositivi di destinazione, è possibile selezionare l'installazione tramite i punti di distribuzione nell'attività di installazione. Tenere presente che questo metodo di installazione comporta un carico significativo per i dispositivi che operano come punti di distribuzione. Pertanto, si consiglia di selezionare i dispositivi che soddisfano i requisiti per i punti di distribuzione. Se si utilizzano punti di distribuzione, è necessario assicurarsi che siano presenti in ciascuna delle subnet isolate che ospitano i dispositivi di destinazione.

L'utilizzo dei punti di distribuzione come centri di installazione locali può anche essere utile durante l'installazione nei dispositivi in subnet che comunicano con Administration Server tramite un canale con una capacità limitata, mentre è disponibile un canale con una maggiore capacità tra i dispositivi nella stessa subnet.

Lo spazio libero su disco nella partizione con la cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit deve superare, di diverse volte, le dimensioni totali dei pacchetti di distribuzione delle applicazioni installate.

Esecuzione di pacchetti indipendenti creati tramite Kaspersky Security Center

I metodi descritti in precedenza per la distribuzione iniziale di Network Agent e delle altre applicazioni non possono essere sempre implementati perché non è possibile soddisfare tutte le condizioni applicabili. In tali casi, è possibile creare un comune file eseguibile denominato *pacchetto di installazione indipendente* tramite Kaspersky Security Center, utilizzando i pacchetti di installazione con le impostazioni di installazione appropriate che sono stati preparati dall'amministratore. Il pacchetto di installazione indipendente è archiviato nella cartella condivisa di Kaspersky Security Center.

È possibile utilizzare Kaspersky Security Center per inviare agli utenti selezionati un messaggio e-mail che contiene un collegamento a questo file nella cartella condivisa, richiedendo loro di eseguire il file (in modalità interattiva o con l'opzione "-s" per l'installazione automatica). È possibile allegare il pacchetto di installazione indipendente a un messaggio e-mail e quindi inviarlo agli utenti dei dispositivi che non hanno accesso alla cartella condivisa di Kaspersky Security Center. L'amministratore può anche copiare il pacchetto indipendente in un'unità rimovibile, trasferirlo in un dispositivo appropriato e quindi eseguirlo in un secondo momento.

È possibile creare un pacchetto indipendente da un pacchetto di Network Agent, un pacchetto di un'altra applicazione (ad esempio, l'applicazione di protezione) o entrambi. Se il pacchetto indipendente è stato creato da Network Agent e un'altra applicazione, l'installazione inizia da Network Agent.

Durante la creazione di un pacchetto indipendente con Network Agent, è possibile specificare il gruppo di amministrazione nel quale verranno automaticamente spostati i nuovi dispositivi (quelli che non sono stati allocati ad alcun gruppo di amministrazione) al termine dell'installazione di Network Agent.

I pacchetti indipendenti possono essere eseguiti in modalità interattiva (per impostazione predefinita), visualizzando il risultato dell'installazione delle applicazioni che contengono, o possono essere eseguiti in modalità automatica (con l'opzione "-s"). La modalità automatica può essere utilizzata per l'installazione tramite script, ad esempio script configurati per l'esecuzione dopo la distribuzione dell'immagine di un sistema operativo. Il risultato dell'installazione in modalità automatica è determinato dal codice restituito del processo.

Il Network Agent autonomo per Linux ha una dipendenza facoltativa dall'utilità nmap. Se l'utilità nmap è mancante o è precedente alla versione 6.0, la funzionalità Broadcast DHCP Discover non è supportata.

Opzioni per l'installazione manuale delle applicazioni

Gli amministratori o gli utenti esperti possono installare manualmente le applicazioni in modalità interattiva. Possono utilizzare i pacchetti di distribuzione originali o pacchetti di installazione generati da questi ultimi e archiviati nella cartella condivisa di Kaspersky Security Center. Per impostazione predefinita, i programmi di installazione vengono eseguiti in modalità interattiva e richiedono agli utenti tutti i valori richiesti. Tuttavia, eseguendo il processo setup.exe dalla radice di un pacchetto di installazione con l'opzione "-s", il programma di installazione verrà eseguito in modalità automatica e con le impostazioni che sono state definite durante la configurazione del pacchetto di installazione.

Quando si esegue setup.exe dalla radice di un pacchetto di installazione archiviato nella cartella condivisa di Kaspersky Security Center, il pacchetto sarà prima copiato in una cartella locale temporanea e quindi sarà eseguito il programma di installazione dell'applicazione dalla cartella locale.

Creazione di un file MST

Per trasformare il contenuto di un pacchetto MSI e applicare le impostazioni personalizzate a un file MSI esistente, è necessario creare un file di trasformazione in formato MST. A tale scopo, utilizzare l'editor Orca.exe, incluso in Windows SDK.

Per creare un file MST:

1. Eseguire l'editor Orca.exe.
2. Passare alla scheda **File** e nel menu fare clic su **Apri**.
3. Selezionare il file Kaspersky Network Agent.msi.
4. Passare alla scheda **Trasformazione** e nel menu selezionare **Nuova trasformazione**.
5. Nella colonna **Tabelle** selezionare **Proprietà** e scrivere i seguenti valori:
   - *EULA=1*
   - *SERVERADDRESS=<Indirizzo di Administration Server>*

   Fare clic sul pulsante **Salva**.
6. Passare alla scheda **Trasforma** e nel menu selezionare **Genera trasformazione**.
7. Nella finestra visualizzata, specificare un nome per il file di trasformazione creato, quindi fare clic sul pulsante **Salva**.

Il file MST viene salvato.

Installazione remota delle applicazioni nei dispositivi in cui è installato Network Agent

Se un Network Agent connesso all'Administration Server primario (o a uno dei relativi Server secondari) è installato in un dispositivo, è possibile eseguire l'upgrade di Network Agent in tale dispositivo, nonché installare, aggiornare o rimuovere qualsiasi applicazione supportata tramite Network Agent.

È possibile abilitare l'opzione **Utilizzando Network Agent** nelle proprietà dell'attività di installazione remota.

Se questa opzione è selezionata, i pacchetti di installazione con le impostazioni di installazione definite dall'amministratore saranno trasferiti ai dispositivi di destinazione tramite i canali di comunicazione tra Network Agent e Administration Server.

Per ottimizzare il carico su Administration Server e ridurre al minimo il traffico tra Administration Server e i dispositivi, è consigliabile assegnare punti di distribuzione in ogni rete remota o in ogni dominio di trasmissione (vedere le sezioni "Informazioni sui punti di distribuzione" e "Creazione di una struttura di gruppi di amministrazione e assegnazione dei punti di distribuzione"). In questo caso, i pacchetti di installazione e le impostazioni del programma di installazione sono distribuiti dall'Administration Server ai dispositivi di destinazione tramite i punti di distribuzione.

È inoltre possibile utilizzare i punti di distribuzione per l'invio (multicast) dei pacchetti di installazione, che consente di ridurre considerevolmente il traffico di rete durante la distribuzione delle applicazioni.

Durante il trasferimento dei pacchetti di installazione ai dispositivi di destinazione tramite i canali di comunicazione tra i Network Agent e l'Administration Server, tutti i pacchetti di installazione che sono stati preparati per il trasferimento saranno anche memorizzati nella cache nella cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Quando si utilizzano diversi pacchetti di installazione di grandi dimensioni, di vari tipi e che coinvolgono numerosi punti di distribuzione, le dimensioni di questa cartella possono aumentare notevolmente.

I file non possono essere eliminati manualmente della cartella FTServer. Quando i pacchetti di installazione originali vengono eliminati, i dati corrispondenti sono eliminati automaticamente della cartella FTServer.

I dati ricevuti dai punti di distribuzione vengono salvati nella cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

I file non possono essere eliminati manualmente della cartella $FTCITmp. Al termine delle attività che utilizzano i dati in questa cartella, i contenuti della cartella saranno eliminati automaticamente.

Poiché i pacchetti di installazione sono distribuiti tramite i canali di comunicazione tra Administration Server e i Network Agent da un archivio intermedio in un formato ottimizzato per i trasferimenti in rete, non sono consentite modifiche ai pacchetti di installazione archiviati nella cartella originale di ogni pacchetto di installazione. Tali modifiche non saranno registrate automaticamente da Administration Server. Se è necessario modificare manualmente i file dei pacchetti di installazione (sebbene sia consigliabile evitare questo scenario), è necessario modificare qualsiasi impostazione di un pacchetto di installazione in Administration Console. La modifica delle impostazioni di un pacchetto di installazione in Administration Console fa sì che Administration Server aggiorni l'immagine del pacchetto nella cache che è stato preparato per il trasferimento nei dispositivi di destinazione.

Gestione dei riavvii dei dispositivi nell'attività di installazione remota

I dispositivi spesso richiedono un riavvio per completare l'installazione remota delle applicazioni (in particolare in Windows).

Se si utilizza l'attività Installazione remota di Kaspersky Security Center, nella Creazione guidata nuova attività o nella finestra delle proprietà dell'attività che è stata creata (sezione **Riavvio del sistema operativo**), è possibile selezionare l'azione da eseguire quando il dispositivo Windows richiede un riavvio:

- **Non riavviare il dispositivo**. In questo caso, non sarà eseguito alcun riavvio automatico. Per completare l'installazione, è necessario riavviare il dispositivo (ad esempio, manualmente o tramite l'attività di gestione del dispositivo). Le informazioni sul riavvio richiesto saranno salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività di installazione nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**. In questo caso, il dispositivo viene sempre riavviato automaticamente quando è richiesto un riavvio per il completamento dell'installazione. Questa opzione è utile per le attività di installazione nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**. In questo caso, sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). L'opzione **Richiedi l'intervento dell'utente** è la più adatta per le workstation, in cui gli utenti devono avere la possibilità di selezionare l'orario che preferiscono per un riavvio del sistema.

Aggiornamento dei database in un pacchetto di installazione di un'applicazione di protezione

Prima di avviare la distribuzione della protezione, è necessario tenere presente che è possibile aggiornare i database anti-virus (inclusi i moduli delle patch automatiche) forniti con il pacchetto di distribuzione dell'applicazione di protezione. È consigliabile aggiornare i database nel pacchetto di installazione dell'applicazione prima di avviare la distribuzione (ad esempio, utilizzando il comando corrispondente nel menu di scelta rapida di un pacchetto di installazione selezionato). In tal modo, è possibile ridurre il numero di riavvii richiesti per il completamento della distribuzione della protezione nei dispositivi di destinazione.

Utilizzo di strumenti per l'installazione remota di applicazioni in Kaspersky Security Center per l'esecuzione di file eseguibili nei dispositivi gestiti

Utilizzando la Creazione guidata nuovo pacchetto, è possibile selezionare qualsiasi file eseguibile e definire le impostazioni della riga di comando per tale file. È possibile aggiungere al pacchetto di installazione il file selezionato o l'intera cartella che lo contiene. È quindi necessario creare l'attività di installazione remota e selezionare il pacchetto di installazione che è stato creato.

Durante l'esecuzione dell'attività, il file eseguibile specificato con le impostazioni definite del prompt dei comandi verrà eseguito nei dispositivi di destinazione.

Se si utilizzano programmi di installazione in formato Microsoft Windows Installer (MSI), Kaspersky Security Center analizza i risultati dell'installazione per mezzo di strumenti standard.

Se è disponibile una licenza per Vulnerability e patch management, Kaspersky Security Center (durante la creazione di un pacchetto di installazione per qualsiasi applicazione supportata nell'ambiente aziendale) utilizza anche regole per l'installazione e l'analisi dei risultati dell'installazione presenti nel proprio database aggiornabile.

In caso contrario, l'attività predefinita per i file eseguibili attende il completamento del processo in esecuzione e di tutti i relativi processi secondari. Dopo completamento di tutti i processi in esecuzione, l'attività verrà completata correttamente, indipendentemente dal codice restituito del processo iniziale. Per modificare il comportamento di questa attività, prima di creare l'attività, è necessario modificare manualmente i file .kpd che sono stati generati da Kaspersky Security Center nella cartella del pacchetto di installazione appena creato e nelle relative sottocartelle.

I file .kpd utilizzano la codifica ASCII. I file .kud utilizzano la codifica Unicode.

Per fare in modo che l'attività non attenda il completamento del processo in esecuzione, impostare il valore dell'impostazione Wait su 0 nella sezione [SetupProcessResult]:

```
[SetupProcessResult]
Wait=0
```

Per fare in modo che l'attività attenda solo il completamento del processo in esecuzione in Windows, e non quello di tutti i processi secondari, impostare il valore dell'impostazione WaitJob su 0 nella sezione [SetupProcessResult], ad esempio:

```
[SetupProcessResult]
WaitJob=0
```

Affinché l'attività venga completata correttamente o restituisca un errore a seconda del codice di ritorno del processo in esecuzione, creare un file .bat eseguibile che salvi il codice di errore in un file, ad esempio:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Quindi modificare i file .kud generati da Kaspersky Security Center nella cartella del pacchetto di installazione appena creato:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

In questo caso, qualsiasi codice diverso da quelli elencati determinerà la restituzione di un errore.

Per visualizzare nei risultati dell'attività una stringa con un commento relativo al completamento dell'attività o un errore, immettere brevi descrizioni degli errori che corrispondono ai codici restituiti del processo nelle sezioni [SetupProcessResult_SuccessCodes] e [SetupProcessResult_ErrorCodes], ad esempio:

```
[SetupProcessResult_SuccessCodes]
0=Installazione completata
3010=È necessario un riavvio per completare l'installazione
[SetupProcessResult_ErrorCodes]
```

```
1602=Installazione annullata dall'utente
1603=Errore irreversibile durante l'installazione
```

Per utilizzare gli strumenti di Kaspersky Security Center per gestire il riavvio del dispositivo (se è necessario un riavvio per completare un'operazione), elencare i codici restituiti del processo che indicano che deve essere eseguito un riavvio nella sezione [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
3010=
```

Monitoraggio della distribuzione

Per monitorare la distribuzione di Kaspersky Security Center e verificare che un'applicazione di protezione e Network Agent siano installati nei dispositivi gestiti, è necessario controllare l'indicatore a semaforo nella sezione **Distribuzione**. Questo indicatore a semaforo è disponibile nell'area di lavoro del nodo Administration Server nella finestra principale di Administration Console. L'indicatore a semaforo riflette lo stato corrente della distribuzione. Il numero di dispositivi con Network Agent e applicazioni di protezione installate è visualizzato accanto all'indicatore. Quando qualsiasi attività di installazione è in esecuzione, qui è possibile monitorarne lo stato di avanzamento. Se si verificano errori, il numero di errori viene visualizzato qui. È possibile visualizzare i dettagli di qualsiasi errore facendo clic sul collegamento.

È anche possibile utilizzare lo schema della distribuzione nell'area di lavoro della cartella **Dispositivi gestiti** nella scheda **Gruppi**. Il grafico riflette il processo di distribuzione, visualizzando il numero di dispositivi senza Network Agent, con Network Agent o con Network Agent e un'applicazione di protezione.

Per ulteriori informazioni sullo stato di avanzamento della distribuzione (o sull'esecuzione di una specifica attività di installazione), aprire la finestra dei risultati dell'attività di installazione remota appropriata: fare clic con il pulsante destro del mouse sull'attività, quindi selezionare **Risultati** nel menu di scelta rapida. La finestra visualizza due elenchi: quello superiore contiene gli stati dell'attività nei dispositivi, mentre quello inferiore contiene gli eventi dell'attività sul dispositivo attualmente selezionato nell'elenco superiore.

Le informazioni sugli errori di distribuzione vengono aggiunte al registro eventi Kaspersky su Administration Server. Le informazioni sugli errori sono anche disponibili tramite la selezione eventi corrispondente nel nodo Administration Server della scheda **Eventi**.

Configurazione dei programmi di installazione

Questa sezione fornisce informazioni sui file dei programmi di installazione di Kaspersky Security Center e sulle impostazioni di installazione, oltre a raccomandazioni su come installare Administration Server e Network Agent in modalità automatica.

Informazioni generali

I programmi di installazione di Kaspersky Security Center 15.1 (Administration Server, Network Agent e Administration Console) sono basati sulla tecnologia Windows Installer. L'elemento fondamentale di un programma di installazione è un pacchetto MSI. Questo formato dei pacchetti consente di sfruttare tutti i vantaggi offerti da Windows Installer: la scalabilità, la disponibilità di un sistema di applicazione delle patch, il sistema di trasformazione, l'installazione centralizzata tramite soluzioni di terze parti e la registrazione trasparente con il sistema operativo.

Installazione in modalità automatica (con un file di risposta)

I programmi di installazione di Administration Server e Network Agent supportano l'utilizzo di un file di risposta (ss_install.xml), in cui sono integrate le parametri per l'installazione in modalità automatica senza la partecipazione dell'utente. Il file ss_install.xml è disponibile nella stessa cartella del pacchetto MSI e viene utilizzato automaticamente durante l'installazione in modalità automatica. È possibile abilitare la modalità di installazione automatica con il tasto della riga di comando "/s".

Un esempio di esecuzione del comando è il seguente:

```
setup.exe /s
```

Prima di avviare il programma di installazione in modalità automatica, leggere il Contratto di licenza con l'utente finale (EULA). Se il kit di distribuzione di Kaspersky Security Center non include un file TXT con il testo dell'EULA, è possibile scaricare il file dal sito Web di Kaspersky.

Il file ss_install.xml è un'istanza del formato interno dei parametri del programma di installazione di Kaspersky Security Center. I pacchetti di distribuzione contengono il file ss_install.xml con i parametri predefiniti.

Non modificare il file ss_install.xml manualmente. Questo file può essere modificato mediante gli strumenti di Kaspersky Security Center durante la modifica dei parametri dei pacchetti di installazione in Administration Console.

Per modificare il file di risposta per l'installazione di Administration Server:

1. Aprire il pacchetto di distribuzione di Kaspersky Security Center. Se si utilizza un file EXE del pacchetto completo, decomprimerlo.
2. Nella cartella Server, aprire la riga di comando e quindi eseguire il seguente comando:
   ```
   setup.exe /r ss_install.xml
   ```
   Viene avviato il programma di installazione di Kaspersky Security Center.
3. Seguire i passaggi della procedura guidata per configurare l'installazione di Kaspersky Security Center.

   Una volta completata la procedura guidata, il file di risposta viene modificato automaticamente in base alle nuove impostazioni specificate.

Installazione di Network Agent in modalità automatica (senza un file di risposta)

È possibile installare Network Agent con un singolo pacchetto .msi, specificando i valori delle proprietà MSI nella modalità standard. Questo scenario consente l'installazione di Network Agent tramite i criteri di gruppo.

Non rinominare il pacchetto di installazione Kaspersky Network Agent.msi. La ridenominazione del pacchetto potrebbe causare errori di installazione durante gli aggiornamenti futuri di Network Agent.

Per evitare conflitti tra i parametri definiti attraverso le proprietà MSI e i parametri definiti nel file di risposta, è possibile disabilitare il file di risposta impostando la proprietà `DONT_USE_ANSWER_FILE=1`. Il file MSI è disponibile nel pacchetto di distribuzione di Kaspersky Security Center, nella cartella Packages\NetAgent\exec. Un esempio di esecuzione del programma di installazione di Network Agent con un pacchetto .msi è il seguente.

L'installazione di Network Agent in modalità automatica richiede l'accettazione delle condizioni del Contratto di licenza con l'utente finale. Utilizzare il parametro `EULA=1` solo se l'utente ha letto, compreso e accettato i termini del Contratto di licenza con l'utente finale.

Esempio:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

È anche possibile definire i parametri di installazione per un pacchetto msi preparando in anticipo il file di risposta (con estensione mst). Questo comando si presenta come segue:

Esempio:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

È possibile specificare diversi file di risposta in un singolo comando.

Se si desidera aggiornare Network Agent tramite il programma di installazione di Windows, eseguire il seguente comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Configurazione parziale dell'installazione tramite setup.exe

Durante l'esecuzione dell'installazione delle applicazioni tramite setup.exe, è possibile aggiungere i valori di qualsiasi proprietà MSI al pacchetto MSI.

Questo comando si presenta come segue:

Esempio:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parametri di installazione di Administration Server

Nella tabella seguente sono descritte le proprietà MSI che è possibile configurare durante l'installazione di Administration Server. Tutti i parametri sono facoltativi, ad eccezione di EULA e PRIVACYPOLICY.

Parametri dell'installazione di Administration Server in modalità automatica

Proprietà MSI	Descrizione	Valori disponibili
EULA	Accettazione dei termini del Contratto di licenza (obbligatorio)	• 1 - Ho letto, compreso e accettato i termini del Contratto di licenza con l'utente finale. • Altri valori o nessun valore- Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita).
PRIVACYPOLICY	Accettazione dei termini dell'Informativa sulla privacy (obbligatorio)	• 1 - Sono consapevole e accetto che i miei dati vengano gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy. Confermo di aver letto e compreso l'Informativa sulla privacy. • Altro valore o nessun valore- Non accetto i termini dell'Informativa sulla privacy (l'installazione non viene eseguita).

Proprietà MSI	Descrizione	Valori disponibili
INSTALLATIONMODETYPE	Tipo di installazione di Administration Server	• Standard. • Personalizzato.
INSTALLDIR	Cartella di installazione dell'applicazione	Valore stringa.
ADDLOCAL	Elenco dei componenti da installare (separati da virgole)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Elenco minimo di componenti sufficienti per la corretta installazione di Administration Server: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Dimensione della rete	• NRT_1_100 – Da 1 a 100 dispositivi. • NRT_100_1000 – Da 101 a 1000 dispositivi. • NRT_GREATER_1000 – Oltre 1000 dispositivi.
SRV_ACCOUNT_TYPE	Consente di specificare l'utente per l'esecuzione del servizio Administration Server	• SrvAccountDefault - L'account utente sarà creato automaticamente. • SrvAccountUser- L'account utente è definito manualmente.
SERVERACCOUNTNAME	Nome utente per il servizio	Valore stringa.
SERVERACCOUNTPWD	Password dell'utente per il servizio	Valore stringa.
DBTYPE	Tipo di database	• MySQL - Verrà utilizzato un database MySQL o MariaDB. • MSSQL - Verrà utilizzato il database Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	Nome completo del server MySQL o MariaDB	Valore stringa.
MYSQLSERVERPORT	Numero di porta per la connessione al server MySQL o MariaDB	Valore numerico.
MYSQLDBNAME	Nome del database del server MySQL o MariaDB	Valore stringa.
MYSQLACCOUNTNAME	Nome utente per la connessione al database del server MySQL o MariaDB	Valore stringa.
MYSQLACCOUNTPWD	Password utente per la connessione al database del server MySQL o MariaDB	Valore stringa.
MSSQLCONNECTIONTYPE	Tipo di utilizzo del database MSSQL	• InstallMSSEE - Installazione da un pacchetto. • ChooseExisting - Utilizzo del server installato.
MSSQLSERVERNAME	Nome completo dell'istanza di SQL Server	Valore stringa.
MSSQLDBNAME	Nome del database del server SQL	Valore stringa.
MSSQLAUTHTYPE	Metodo di autenticazione per la connessione a SQL Server	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nome utente per la connessione a SQL Server in modalità SQLServer	Valore stringa.
MSSQLACCOUNTPWD	Password dell'utente per la connessione a SQL Server in modalità SQLServer	Valore stringa.

Proprietà MSI	Descrizione	Valori disponibili

CREATE_SHARE_TYPE	Metodo per la specificazione della cartella condivisa	• Create - Creare una nuova cartella condivisa. In questo caso, è necessario definire le seguenti proprietà:
		  • SHARELOCALPATH - Percorso di una cartella locale.
		  • SHAREFOLDERNAME - Nome di rete di una cartella.
		• Null - Deve essere specificata la proprietà EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Percorso completo di una cartella condivisa esistente	Valore stringa.
SERVERPORT	Numero di porta per la connessione ad Administration Server	Valore numerico.
SERVERSSLPORT	Numero di porta per la creazione di una connessione ad Administration Server	Valore numerico.
SERVERADDRESS	Indirizzo di Administration Server	Valore stringa.
SERVERCERT2048BITS	Dimensione della chiave per il certificato di Administration Server (in bit)	• 1 - La dimensione della chiave per il certificato di Administration Server è di 2048 bit. • 0 - La dimensione della chiave per il certificato di Administration Server è di 1024 bit. • Se non viene specificato alcun valore, la dimensione della chiave per il certificato di Administration Server è di 2048 bit.
MOBILESERVERADDRESS	Indirizzo dell'Administration Server per la connessione dei dispositivi mobili; ignorato se il componente MobileSupport non è stato selezionato	Valore stringa.

Parametri di installazione di Network Agent

Nella tabella seguente sono descritte le proprietà MSI che è possibile configurare durante l'installazione di Network Agent. Tutti i parametri sono facoltativi, ad eccezione di EULA e SERVERADDRESS.

Parametri dell'installazione di Network Agent in modalità automatica

Proprietà MSI	Descrizione	Valori disponibili
EULA	Accettazione del Contratto di licenza	• 1 - Confermo di aver letto, compreso e accettato i termini e le condizioni del presente Contratto di licenza con l'utente finale. • 0—Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita). • Nessun valore—Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita).
DONT_USE_ANSWER_FILE	Leggere le impostazioni di installazione dal file di risposta	• 1—Non utilizzare. • Altri valori o nessun valore—Lettura.
INSTALLDIR	Percorso della cartella di installazione di Network Agent	Valore stringa.
SERVERADDRESS	Indirizzo di Administration Server (obbligatorio)	Valore stringa.
SERVERPORT	Numero di porta per la connessione ad Administration Server	Valore numerico.
SERVERSSLPORT	Numero di porta per la connessione criptata ad Administration Server tramite il protocollo SSL	Valore numerico.

Proprietà MSI	Descrizione	Valori disponibili
USESSL	Specifica se utilizzare connessione SSL	• 1 - Utilizzare. • Altri valori o nessun valore - Non utilizzare.
OPENUDPPORT	Specifica se aprire una porta UDP	• 1 - Aprire. • Altri valori o nessun valore - Non aprire.
UDPPORT	Numero di porta UDP	Valore numerico.
USEPROXY	Specifica se utilizzare un server proxy: Per motivi di compatibilità, non è consigliabile specificare le impostazioni di connessione proxy nelle impostazioni del pacchetto di installazione di Network Agent.	• 1 - Utilizzare. • Altri valori o nessun valore - Non utilizzare.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Indirizzo del proxy e numero di porta per la connessione al server proxy	Valore stringa.
PROXYLOGIN	Account per la connessione a un server proxy	Valore stringa.
PROXYPASSWORD	Password dell'account per la connessione al server proxy (non specificare i dettagli degli account con privilegi nei parametri dei pacchetti di installazione.)	Valore stringa.
GATEWAYMODE	Modalità di utilizzo del gateway di connessione	• 0 - Non utilizzare il gateway di connessione. • 1 - Utilizza questo Network Agent come gateway di connessione. • 2 - Connetti ad Administration Server utilizzando il gateway di connessione.
GATEWAYADDRESS	Indirizzo gateway connessione	Valore stringa.
CERTSELECTION	Metodo di ricezione di un certificato	• GetOnFirstConnection - Ricevere un certificato da Administration Server. • GetExistent - Selezionare un certificato esistente. Se questa opzione è selezionata, è necessario specificare la proprietà CERTFILE.
CERTFILE	Percorso del file di certificato	Valore stringa.
VMVDI	Abilitare la modalità dinamica per Virtual Desktop Infrastructure (VDI)	• 1 - Abilitare. • 0 - Non abilitare. • Nessun valore - Non abilitare.
VMOPTIMIZE	Se le impostazioni di Network Agent sono ottimali per l'hypervisor	• 1 - Abilitare. • 0 - Non abilitare. • Nessun valore - Non abilitare.
LAUNCHPROGRAM	Specifica se avviare il servizio Network Agent dopo l'installazione. Il parametro viene ignorato se VMVDI=1	• 1 - Avviare. • Altri valori o nessun valore - Non avviare.
NAGENTTAGS	Tag per Network Agent (ha la priorità sul tag assegnato nel file di risposta)	Valore stringa.

Infrastruttura virtuale

Kaspersky Security Center supporta l'utilizzo di macchine virtuali. È possibile installare Network Agent e l'applicazione di protezione in ogni macchina virtuale, nonché proteggere le macchine virtuali a livello di hypervisor. Nel primo caso è possibile utilizzare un'applicazione di protezione standard o Kaspersky Security for Virtualization Light Agent per proteggere le macchine virtuali. Nel secondo caso è possibile utilizzare Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center supporta i rollback delle macchine virtuali allo stato precedente.

Suggerimenti per la riduzione del carico sulle macchine virtuali

Durante l'installazione di Network Agent in una macchina virtuale, è consigliabile valutare se disabilitare alcune funzionalità di Kaspersky Security Center che risultano di scarsa utilità per le macchine virtuali.

Quando si installa Network Agent in una macchina virtuale o in un modello utilizzato per la generazione di macchine virtuali, è consigliabile eseguire le seguenti azioni:

- Se si esegue un'installazione remota, nella finestra delle proprietà del pacchetto di installazione di Network Agent, nella sezione **Avanzate** selezionare l'opzione **Ottimizza le impostazioni per VDI**.
- Se si esegue un'installazione interattiva tramite una procedura guidata, nella finestra della procedura guidata selezionare l'opzione **Ottimizza le impostazioni di Network Agent per l'infrastruttura virtuale**.

La selezione di queste opzioni modifica le impostazioni di Network Agent in modo da mantenere disabilitate le seguenti funzionalità per impostazione predefinita (prima dell'applicazione di un criterio):

- Recupero delle informazioni sul software installato
- Recupero delle informazioni sull'hardware
- Recupero delle informazioni sulle vulnerabilità rilevate
- Recupero delle informazioni sugli aggiornamenti richiesti

In genere, queste funzionalità non sono necessarie nelle macchine virtuali perché utilizzano software uniforme e hardware virtuale.

La disabilitazione delle funzionalità è reversibile. Se è richiesta una delle funzionalità disabilitate, è possibile abilitarla tramite il criterio di Network Agent o mediante le impostazioni locali di Network Agent. Le impostazioni locali di Network Agent sono disponibili tramite il menu di scelta rapida del dispositivo appropriato in Administration Console.

Supporto delle macchine virtuali dinamiche

Kaspersky Security Center supporta le macchine virtuali dinamiche. Se nella rete dell'organizzazione è stata distribuita un'infrastruttura virtuale, in alcuni casi è possibile utilizzare macchine virtuali (temporanee) dinamiche. Le macchine virtuali dinamiche vengono create con nomi univoci in base a un modello che è stato preparato dall'amministratore. L'utente lavora su una macchina virtuale per un certo periodo e, dopo lo spegnimento, questa macchina virtuale sarà rimossa dall'infrastruttura virtuale. Se Kaspersky Security Center è stato distribuito nella rete dell'organizzazione, una macchina virtuale con Network Agent installato verrà aggiunta al database di Administration Server. Dopo lo spegnimento di una macchina virtuale, anche la voce corrispondente deve essere rimossa dal database di Administration Server.

Per rendere disponibile la funzionalità di rimozione automatica delle voci nelle macchine virtuali, durante l'installazione di Network Agent in un modello per le macchine virtuali dinamiche, selezionare l'opzione **Abilita modalità dinamica per VDI**:

- Per l'installazione remota - Nella finestra delle proprietà del pacchetto di installazione di Network Agent (sezione **Avanzate**)
- Per l'installazione interattiva - Nell'Installazione guidata di Network Agent

> Evitare di selezionare l'opzione **Abilita modalità dinamica per VDI** durante l'installazione di Network Agent nei dispositivi fisici.

Se si desidera archiviare gli eventi generati dalle macchine virtuali dinamiche in Administration Server per un certo periodo dopo la rimozione delle macchine virtuali, nella finestra delle proprietà di Administration Server, nella sezione **Archivio eventi**, selezionare l'opzione **Archivia eventi dopo l'eliminazione dei dispositivi** e specificare il periodo di archiviazione massimo degli eventi (in giorni).

> Non è consigliabile abilitare il criptaggio delle unità nelle macchine virtuali dinamiche.

Supporto della copia delle macchine virtuali

La copia di una macchina virtuale con Network Agent installato o la creazione di una macchina virtuale da un modello con Network Agent installato sono identiche alla distribuzione dei Network Agent tramite l'acquisizione e la copia di un'immagine del disco rigido. In generale, durante la copia delle macchine virtuali è necessario eseguire le stesse azioni previste durante la distribuzione di Network Agent tramite la copia un'immagine del disco.

Tuttavia, nei due casi descritti di seguito viene illustrato Network Agent, che rileva automaticamente la copia. Per i motivi indicati in precedenza, non è necessario eseguire le operazioni sofisticate descritte in "Distribuzione tramite l'acquisizione e la copia dell'immagine del disco rigido di un dispositivo":

- L'opzione **Abilita modalità dinamica per VDI** era selezionata durante l'installazione di Network Agent: dopo ogni riavvio del sistema operativo, questa macchina virtuale sarà riconosciuta come un nuovo dispositivo, indipendentemente dal fatto che sia stata copiata.

- È in uso uno dei seguenti hypervisor: VMware™, HyperV® o Xen®: Network Agent rileva la copia della macchina virtuale in base agli ID modificati dell'hardware virtuale.

L'analisi delle modifiche nell'hardware virtuale non è assolutamente affidabile. Prima di applicare questo metodo su larga scala, è necessario testarlo su un piccolo gruppo di macchine virtuali per la versione dell'hypervisor attualmente in uso nell'organizzazione.

Supporto del rollback del file system per i dispositivi con Network Agent

Kaspersky Security Center è un'applicazione distribuita. Il rollback del file system uno stato precedente in un dispositivo con Network Agent installato determinerà la mancata sincronizzazione dei dati e impedirà il corretto funzionamento di Kaspersky Security Center.

È possibile eseguire il rollback del file system (o di una sua parte) nei seguenti casi:

- Durante la copia di un'immagine del disco rigido.

- Durante il ripristino di uno stato della macchina virtuale tramite l'infrastruttura virtuale.

- Durante il ripristino dei dati da una copia di backup o da un punto di ripristino.

Gli scenari in cui software di terze parti nei dispositivi con Network Agent installato influisce sulla cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ sono solo scenari critici per Kaspersky Security Center. Pertanto, è necessario escludere sempre questa cartella dalla procedura di ripristino, se possibile.

Dal momento che le regole per l'ambiente di lavoro di alcune organizzazioni consentono i rollback del file system nei dispositivi, il supporto per il rollback del file system nei dispositivi con Network Agent installato è stato aggiunto a Kaspersky Security Center a partire dalla versione 10 Maintenance Release 1 (Administration Server e i Network Agent devono essere della versione 10 Maintenance Release 1 o successiva). Quando sono rilevati, tali dispositivi vengono riconnessi automaticamente all'Administration Server con una cancellazione completa dei dati e una sincronizzazione completa.

Per impostazione predefinita, il supporto per il rilevamento del rollback del file system è abilitato in Kaspersky Security Center 15.1.

Per quanto possibile, evitare di eseguire il rollback della cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ nei dispositivi con Network Agent installato, perché la risincronizzazione completa dei dati richiede una notevole quantità di risorse.

Non è assolutamente consentito un rollback dello stato del sistema in un dispositivo con Administration Server installato, né un rollback del database utilizzato da Administration Server.

È possibile ripristinare uno stato di Administration Server da una copia di backup solo con l'utilità klbackup standard.

Installazione locale delle applicazioni

In questa sezione viene descritta una procedura di installazione per le applicazioni che possono essere installate solo nei dispositivi in locale.

Per eseguire l'installazione locale delle applicazioni in un dispositivo client specifico, è necessario disporre di diritti di amministratore per il dispositivo.

Per installare le applicazioni in locale in un dispositivo client specifico:

1. Installare Network Agent nel dispositivo client e configurare la connessione tra il dispositivo client e Administration Server.

2. Installare le applicazioni richieste nel dispositivo, come descritto nei manuali delle applicazioni.

3. Installare un plug-in di gestione per ognuna delle applicazioni installate nella workstation dell'amministratore.

Kaspersky Security Center supporta inoltre l'opzione per l'installazione locale delle applicazioni utilizzando un pacchetto di installazione indipendente. Kaspersky Security Center non supporta l'installazione di tutte le applicazioni Kaspersky.

Installazione locale di Network Agent

Per installare Network Agent in locale in un dispositivo:

1. Nel dispositivo eseguire il file setup.exe dal pacchetto di distribuzione scaricato da Internet. Per informazioni dettagliate, fare riferimento al seguente argomento: Acquisizione del pacchetto di installazione di Network Agent dal kit di distribuzione di Kaspersky Security Center.

   Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da installare.

2. Nella finestra di selezione dell'applicazione fare clic sul collegamento **Installa solo Kaspersky Security Center Network Agent** per avviare l'Installazione guidata di Network Agent. Seguire le istruzioni della procedura guidata.

   a. Administration Server

   Porta

   Specifica la porta non SSL utilizzata da Administration Server per ricevere le connessioni dai Network Agent.

   Per impostazione predefinita, questa opzione è impostata su 14000.

   Porta SSL

   Specifica la porta SSL utilizzata da Administration Server per ricevere le connessioni dai Network Agent.

   Per impostazione predefinita, questa opzione è impostata su 13000.

   Usa SSL per la connessione ad Administration Server

   Se questa opzione è abilitata, la connessione ad Administration Server viene stabilita attraverso una porta sicura tramite SSL.

   Per impostazione predefinita, questa opzione è abilitata.

   Consenti a Network Agent di aprire la porta UDP

   Se questa opzione è abilitata, il programma di installazione apre automaticamente la porta utilizzata da Administration Server per gestire il dispositivo client e ricevere informazioni al riguardo.

   Per impostazione predefinita, questa opzione è abilitata.

   Porta UDP

   Consente di configurare la porta utilizzata da Administration Server per gestire il dispositivo client e ricevere informazioni su di esso.

   Per impostazione predefinita, questa opzione è impostata su 15000.

   b. Configurazione del server proxy

Usa server proxy

Se questa opzione è abilitata, è possibile specificare le credenziali per l'autenticazione del server proxy.

È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

Per impostazione predefinita, questa opzione è disabilitata.

Indirizzo

Porta

Account

Nome utente dell'account con cui viene stabilita la connessione al server proxy.

È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

Password

Password dell'account con cui viene stabilita la connessione al server proxy.

È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

c. **Gateway di connessione**

Non utilizzare gateway di connessione

Utilizzare Network Agent come gateway di connessione nella rete perimetrale

Selezionare questa opzione per utilizzare Network Agent come gateway di connessione nella rete perimetrale per connettersi ad Administration Server, comunicare con esso e assicurare la protezione dei dati in Network Agent durante la trasmissione dei dati.

Esegui la connessione ad Administration Server utilizzando un gateway di connessione

Selezionare questa opzione e quindi specificare il dispositivo che fungerà da gateway di connessione.

d. **Certificato di Administration Server**

e. **Tag agente**

f. **Impostazioni avanzate**

Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito

Si consiglia di mantenere questa opzione abilitata. È possibile deselezionare questa opzione per disabilitare l'aggiornamento automatico e l'applicazione di patch per i componenti di Kaspersky Security Center. L'amministratore può riabilitare l'installazione automatica di aggiornamenti e patch in un secondo momento utilizzando un criterio.

Per impostazione predefinita, questa opzione è disabilitata.

Abilita la protezione del servizio Network Agent

Quando questa opzione è abilitata, dopo l'installazione di Network Agent in un dispositivo gestito, il componente non può essere rimosso o riconfigurato senza i privilegi richiesti. Il servizio Network Agent non può essere arrestato. Questa opzione non ha effetto sui controller di dominio.

Abilitare questa opzione per proteggere Network Agent sulle workstation gestite con diritti di amministratore locale.

Per impostazione predefinita, questa opzione è disabilitata.

Abilita modalità dinamica per VDI

Se questa opzione è abilitata, la modalità dinamica per Virtual Desktop Infrastructure (VDI) sarà abilitata per Network Agent installato in una macchina virtuale.

Per impostazione predefinita, questa opzione è disabilitata.

Ottimizzare le impostazioni di Kaspersky Security Center Network Agent per la VDI. Disabilitare la scansione delle vulnerabilità e l'inventario di applicazioni e hardware. È possibile modificare le impostazioni correnti tramite i criteri di Network Agent.

Se questa opzione è abilitata, le seguenti funzionalità sono disabilitate nelle impostazioni di Network Agent:

- Recupero delle informazioni sul software installato
- Recupero delle informazioni sull'hardware
- Recupero delle informazioni sulle vulnerabilità rilevate
- Recupero delle informazioni sugli aggiornamenti richiesti

Per impostazione predefinita, questa opzione è disabilitata.

g. **Avvia applicazione**

Al termine dell'Installazione guidata, Network Agent viene installato nel dispositivo.

È possibile visualizzare le proprietà del servizio Kaspersky Security Center Network Agent; è inoltre possibile avviare, arrestare e monitorare l'esecuzione di Network Agent utilizzando gli strumenti standard di Microsoft Windows: Gestione computer\Servizi.

Installazione di Network Agent in modalità automatica

Network Agent può essere installato in modalità automatica, ovvero senza l'input dei parametri di installazione. L'installazione automatica utilizza un pacchetto di installazione di Windows (MSI) per Network Agent. Il file MSI è disponibile nel pacchetto di distribuzione di Kaspersky Security Center, nella cartella Packages\NetAgent\exec.

Non rinominare il pacchetto di installazione Kaspersky Network Agent.msi. La ridenominazione del pacchetto potrebbe causare errori di installazione durante gli aggiornamenti futuri di Network Agent.

L'installazione di Network Agent dal pacchetto MSI è possibile solo in modalità automatica, l'installazione interattiva dal pacchetto MSI non è supportata.

Per installare Network Agent in un dispositivo locale in modalità automatica:

1. Leggere il Contratto di licenza con l'utente finale. Utilizzare il comando di seguito solo se sono stati compresi e accettati i termini del Contratto di licenza con l'utente finale.

2. Eseguire il comando

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <parametri_installazione>
   ```

   dove `parametri_installazione` è un elenco di parametri e dei valori corrispondenti separati da uno spazio (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   Nell'elenco dei parametri è necessario includere `EULA=1`. In caso contrario Network Agent non verrà installato.

Se si utilizzano le impostazioni di connessione standard per Kaspersky Security Center e Network Agent nei dispositivi remoti, eseguire il comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` è la chiave per la scrittura dei log. Il log viene creato durante l'installazione di Network Agent e salvato in C:\windows\temp\nag_inst.log.

Oltre a nag_inst.log, l'applicazione crea il file $klssinstlib.log, che contiene il log di installazione. Questo file è archiviato nella cartella %windir%\temp or %temp%. Per la risoluzione dei problemi, l'utente o un esperto del Servizio di assistenza tecnica Kaspersky potrebbe aver bisogno di entrambi i file di log: nag_inst.log e $klssinstlib.log.

Se è necessario specificare la porta per la connessione ad Administration Server, eseguire il comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

Il parametro `SERVERPORT` corrisponde al numero di porta per la connessione ad Administration Server.

I nomi e i possibili valori per i parametri che è possibile utilizzare durante l'installazione di Network Agent in modalità automatica sono elencati nella sezione Parametri di installazione di Network Agent.

Se si desidera aggiornare Network Agent tramite il programma di installazione di Windows, eseguire il seguente comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Installazione di Network Agent per Linux in modalità automatica (con un file di risposte)

È possibile installare Network Agent nei dispositivi Linux utilizzando un file di risposte, vale a dire un file di testo contenente un set personalizzato di parametri di installazione: variabili e rispettivi valori. L'uso di questo file di risposte consente di eseguire un'installazione in modalità automatica, ovvero senza la partecipazione dell'utente.

Per eseguire l'installazione di Network Agent per Linux in modalità automatica:

1. Preparare il dispositivo Linux attinente per l'installazione remota. Scaricare e creare il pacchetto di installazione remota, utilizzando un pacchetto .deb o .rpm di Network Agent, tramite qualsiasi sistema di gestione dei pacchetti idoneo.

2. Se si desidera installare Network Agent nei dispositivi con sistema operativo SUSE Linux Enterprise Server 15, installare il pacchetto insserv-compat prima di configurare Network Agent.

   Se si desidera installare Network Agent nei dispositivi con il sistema operativo RED OS 7.3.4 o versione successiva o MSVSPHERE 9.2 o versione successiva, installare il pacchetto libxcrypt-compat per il corretto funzionamento di Network Agent.

3. Leggere il Contratto di licenza con l'utente finale. Seguire i passaggi di seguito solo se sono stati compresi e accettati i termini del Contratto di licenza con l'utente finale.

4. Creare il file di risposte (in formato TXT). Aggiungere al file di risposte un elenco di variabili nel formato NOME_VARIABILE=valore_variabile, ognuna su una riga separata.

   Per il corretto utilizzo del file di risposte, è necessario includere un set minimo delle tre variabili richieste:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   È inoltre possibile aggiungere eventuali variabili opzionali per utilizzare parametri più specifici dell'installazione remota. La tabella seguente elenca tutte le variabili che possono essere incluse nel file di risposte:

   Variabili del file di risposte utilizzate come parametri dell'installazione di Network Agent per Linux in modalità automatica

Variabili del file di risposte utilizzate come parametri dell'installazione di Network Agent per Linux in modalità automatica

Nome della variabile	Richiesto	Descrizione	Valori possibili
KLNAGENT_SERVER	Sì	Contiene il nome di Administration Server sotto forma di nome di dominio completo (FQDN) o indirizzo IP.	Nome DNS o indirizzo IP.
KLNAGENT_AUTOINSTALL	Sì	Indica se la modalità di installazione automatica è abilitata.	1—La modalità automatica è abilitata; l'utente non deve eseguire alcuna operazione durante l'installazione. Altro—La modalità automatica è disabilitata; all'utente può essere richiesto di eseguire operazioni durante l'installazione.
EULA_ACCEPTED	Sì	Indica se l'utente accetta il Contratto di licenza con l'utente finale (EULA) di Network Agent; se non disponibile, può essere interpretato come la mancata accettazione dell'EULA.	1 - Confermo di aver letto, compreso e accettato i termini e le condizioni del presente Contratto di licenza con l'utente finale Altro o non specificato—Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita).
KLNAGENT_PROXY_USE	No	Indica se la connessione con Administration Server utilizzerà le impostazioni del proxy. Il valore predefinito è 0.	1—Le impostazioni del proxy vengono utilizzate. Altro—Le impostazioni del proxy non vengono utilizzate.
KLNAGENT_PROXY_ADDR	No	Indica l'indirizzo del server proxy utilizzato per la connessione con Administration Server.	Nome DNS o indirizzo IP.
KLNAGENT_PROXY_LOGIN	No	Indica il nome utente utilizzato per l'accesso al server proxy.	Qualsiasi nome utente esistente.
KLNAGENT_PROXY_PASSWORD	No	Indica la password utente utilizzata per l'accesso al server proxy.	Qualsiasi set di caratteri alfanumerici consentiti dal formato password nel sistema operativo.
KLNAGENT_VM_VDI	No	Indica se Network Agent è installato in un'immagine per la creazione di macchine virtuali dinamiche.	1—Network Agent è installato in un'immagine, che verrà successivamente utilizzata per la creazione di macchine virtuali dinamiche. Altro—Non viene utilizzata alcuna immagina durante l'installazione.
KLNAGENT_VM_OPTIMIZE	No	Indica se le impostazioni di Network Agent sono ottimali per l'hypervisor.	1—Le impostazioni locali predefinite di Network Agent vengono modificate per consentire l'utilizzo ottimizzato nell'hypervisor.
KLNAGENT_TAGS	No	Elenca i tag assegnati all'istanza di Network Agent.	Uno o più nomi di tag separati da un punto e virgola.
KLNAGENT_UDP_PORT	No	Indica la porta UDP utilizzata da Network Agent. Il valore predefinito è 15000.	Qualsiasi numero di porta esistente.
KLNAGENT_PORT	No	Definisce la porta non TLS utilizzata da Network Agent. Il valore predefinito è 14000.	Qualsiasi numero di porta esistente.

KLNAGENT_SSLPORT	No	Definisce la porta TLS utilizzata da Network Agent. Il valore predefinito è 13000.	Qualsiasi numero di porta esistente.
KLNAGENT_USESSL	No	Indica se per la connessione viene utilizzato Transport Layer Security (TLS).	1 (predefinito)—TLS viene utilizzato. Altro—TLS non viene utilizzato.
KLNAGENT_GW_MODE	No	Indica se viene utilizzato il gateway di connessione.	1 (predefinito)—Le impostazioni correnti non vengono modificate (alla prima chiamata non viene specificato alcun gateway di connessione). 2—Non viene utilizzato alcun gateway di connessione. 3—Il gateway di connessione viene utilizzato. KLNAGENT_GW_ADDRESS è obbligatorio. 4—L'istanza di Network Agent viene utilizzata come gateway di connessione nella rete perimetrale (DMZ). Il certificato del server è obbligatorio.
KLNAGENT_GW_ADDRESS	No	Indica l'indirizzo del gateway di connessione. Il valore è applicabile solo se KLNAGENT_GW_MODE=3.	Nome DNS o indirizzo IP.
KLNAGENT_DEVICEOWNER_REGISTRATION_START	No	Consente di eseguire la registrazione dell'utente come utilità del proprietario del dispositivo dopo l'installazione di Network Agent. Se disattivata, la registrazione come proprietario del dispositivo non è disponibile per un utente.	1: la registrazione dell'utente come utilità del proprietario del dispositivo verrà eseguita dopo l'installazione di Network Agent. Altro: disattivato.

5. Eseguire l'installazione di Network Agent. La variabile di ambiente KLAUTOANSWERS, che specifica il percorso del file di risposte, viene passata al comando di installazione. Eseguire uno dei seguenti comandi:

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 32 bit, eseguire il comando seguente:
     `sudo KLAUTOANSWERS=<percorso del file di risposte> yum install ./klnagent-<numero build>.i386.rpm`

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 64 bit, eseguire il comando seguente:
     `sudo KLAUTOANSWERS=<percorso del file di risposte> yum install ./klnagent64-<numero build>.x86_64.rpm`

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 64 bit per l'architettura Arm, eseguire il comando seguente:
     `sudo KLAUTOANSWERS=<percorso del file di risposte> yum install ./klnagent64-<numero build>.aarch64.rpm`

   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 32 bit, eseguire il comando seguente:
     `sudo KLAUTOANSWERS=<percorso del file di risposte> apt install ./klnagent_<numero build>_i386.deb`

- Per installare Network Agent da un pacchetto DEB in un sistema operativo a 64 bit, eseguire il comando seguente:
  `sudo KLAUTOANSWERS=<percorso del file di risposte> apt install ./klnagent64_<numero build>_amd64.deb`

- Per installare Network Agent da un pacchetto DEB in un sistema operativo a 64 bit per l'architettura Arm, eseguire il comando seguente:
  `sudo KLAUTOANSWERS=<percorso del file di risposte> apt install ./klnagent64_<numero build>_arm64.deb`

A seconda della configurazione del sistema operativo, è inoltre possibile utilizzare i gestori pacchetti rpm, dpkg o dnf per installare Network Agent.

L'installazione di Network Agent per Linux viene avviata in modalità automatica; all'utente non viene richiesto di eseguire alcuna operazione durante il processo.

Preparazione di un dispositivo in cui viene eseguito Astra Linux in modalità ambiente software chiuso per l'installazione di Network Agent

Prima di installare Network Agent in un dispositivo in cui viene eseguito Astrito Linux in modalità ambiente software chiuso, è necessario eseguire due procedure di preparazione: quella nelle istruzioni riportate di seguito e i passaggi generali di preparazione per qualsiasi dispositivo Linux.

Eseguire i comandi presenti in questa istruzione con un account con privilegi di root.

Per preparare un dispositivo in cui viene eseguito Astra Linux in modalità ambiente software chiuso per l'installazione di Network Agent:

1. Aprire il file `/etc/digsig/digsig_initramfs.conf`, quindi specificare la seguente impostazione:
   `DIGSIG_ELF_MODE=1`
2. Nella riga di comando, eseguire il seguente comando per installare il pacchetto di compatibilità:
   `apt install astra-digsig-oldkeys`
3. Creare una directory per la chiave dell'applicazione:
   `mkdir -p /etc/digsig/keys/legacy/kaspersky/`
4. Posizionare la chiave dell'applicazione /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg nella directory creata nel passaggio precedente:
   `cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/`

   Se il kit di distribuzione di Kaspersky Security Center non include la chiave dell'applicazione kaspersky_astra_pub_key.gpg, è possibile scaricarla facendo clic sul collegamento: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Aggiornare i dischi RAM:
   `update-initramfs -u -k all`
   Riavviare il sistema.

Il dispositivo Linux è pronto per l'installazione di Network Agent. È possibile installare Network Agent da remoto, in modalità interattiva o in modalità automatica.

Installazione di Network Agent per Linux in modalità interattiva

Questo articolo descrive come installare Network Agent nei dispositivi Linux in modalità interattiva, specificando passo dopo passo i parametri di installazione. In alternativa, è possibile utilizzare un file di risposte: un file di testo contenente un set personalizzato di parametri di installazione: variabili e rispettivi valori. L'uso di questo file di risposte consente di eseguire un'installazione in modalità automatica, ovvero senza la partecipazione dell'utente.

Se si desidera installare Network Agent nei dispositivi con il sistema operativo RED OS 7.3.4 o versione successiva o MSVSPHERE 9.2 o versione successiva, installare il pacchetto libxcrypt-compat per il corretto funzionamento di Network Agent.

Per installare Network Agent in modalità interattiva:

1. Eseguire l'installazione di Network Agent. A seconda della distribuzione Linux, eseguire uno dei seguenti comandi:

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 32 bit:

     `# yum -i klnagent-<numero build>.i386.rpm`

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 64 bit:

     `# yum -i klnagent64-<numero build>.x86_64.rpm`

   - Per installare Network Agent da un pacchetto RPM in un sistema operativo a 64 bit per l'architettura Arm:

     `# yum -i klnagent64-<numero build>.aarch64.rpm`

   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 32 bit:

     `# apt install ./klnagent_<numero build>_i386.deb`

   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 64 bit:

     `# apt install ./klnagent64_<numero build>_amd64.deb`

   - Per installare Network Agent da un pacchetto DEB in un sistema operativo a 64 bit per l'architettura Arm:

     `# apt install ./klnagent64_<numero build>_arm64.deb`

2. Eseguire la configurazione di Network Agent:

   `# /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl`

3. Leggere il Contratto di licenza con l'utente finale (EULA). Il testo viene visualizzato nella finestra della riga di comando. Premere la barra spaziatrice per visualizzare il segmento di testo successivo. Quando richiesto inserire uno dei seguenti valori:

   - Immettere `y` se i termini del Contratto di licenza con l'utente finale sono stati compresi e accettati.

   - Immettere `n` se non si accettano i termini del Contratto di licenza con l'utente finale. Per utilizzare Network Agent, è necessario accettare i termini del Contratto di licenza con l'utente finale.

   - Immettere `r` per mostrare nuovamente il Contratto di licenza con l'utente finale.

4. Immettere l'indirizzo IP o il nome DNS di Administration Server.

5. Immettere il numero di porta di Administration Server. Per impostazione predefinita, viene utilizzata la porta 14000.

6. Immettere il numero di porta SSL di Administration Server. Per impostazione predefinita, viene utilizzata la porta 13000.

7. Immettere `y` se si desidera utilizzare il criptaggio SSL per il traffico tra Network Agent e Administration Server. In caso contrario, immettere `n`.

8. Selezionare una delle seguenti opzioni per configurare Network Agent:

   - `[1]`: non configurare un gateway di connessione.

     Il dispositivo non fungerà da gateway di connessione e non si connetterà ad Administration Server tramite un gateway di connessione.

   - `[2]`: non utilizzare un gateway di connessione.

     Il dispositivo non si connetterà ad Administration Server tramite un gateway di connessione.

   - `[3]`: eseguire la connessione al server utilizzando un gateway di connessione.

     Il dispositivo si connetterà ad Administration Server tramite un gateway di connessione.

   - `[4]`: utilizzare come gateway di connessione.

     Il dispositivo fungerà da gateway di connessione.

Network Agent viene installato in un dispositivo Linux.

Installazione locale del plug-in di gestione dell'applicazione

Per installare il plug-in di gestione dell'applicazione:

In un dispositivo in cui è installato Administration Console, eseguire il file eseguibile klcfginst.exe, incluso nel pacchetto di distribuzione dell'applicazione.

Il file klcfginst.exe è incluso in tutte le applicazioni che possono essere gestite tramite Kaspersky Security Center. L'installazione è agevolata dalla procedura guidata e non richiede la configurazione manuale delle impostazioni.

Installazione di applicazioni in modalità automatica

Per installare un'applicazione in modalità automatica:

1. Aprire la finestra principale dell'applicazione di Kaspersky Security Center.

2. Nella cartella **Installazione remota** della struttura della console, nella sottocartella **Pacchetti di installazione**, selezionare il pacchetto di installazione dell'applicazione desiderata o creare un nuovo pacchetto di installazione per l'applicazione.

   Il pacchetto di installazione verrà memorizzato in Administration Server, nella sottocartella Packages della cartella condivisa. A ogni pacchetto di installazione corrisponde una sottocartella distinta.

3. Aprire la cartella che contiene il pacchetto di installazione richiesto in uno dei seguenti modi:

   - Copiando la cartella che corrisponde al pacchetto di installazione appropriato dall'Administration Server nel dispositivo client e aprendo la cartella copiata nel dispositivo client.

   - Aprendo dal dispositivo client la cartella condivisa che corrisponde al pacchetto di installazione desiderato in Administration Server.

   Se la cartella condivisa si trova in un dispositivo con sistema operativo Microsoft Windows Vista, selezionare il valore **Disabilitato** per l'impostazione **Controllo dell'account utente: esegui tutti gli amministratori in modalità Approvazione amministratore** (**Start** → **Pannello di controllo** → **Amministrazione** → **Criteri di protezione locali** → **Impostazioni di protezione**).

4. A seconda dell'applicazione selezionata, eseguire le seguenti operazioni:

   - Per Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers e Kaspersky Security Center, aprire la sottocartella exec, quindi eseguire il file eseguibile (con estensione .exe) con la chiave /s.

   - Per le altre applicazioni Kaspersky, eseguire il file eseguibile (con estensione .exe) con l'opzione /s dalla cartella aperta.

   L'esecuzione del file eseguibile con le chiavi `EULA=1` e `PRIVACYPOLICY=1` comporta la lettura, la comprensione e l'accettazione dei termini del Contratto di licenza con l'utente finale e dell'Informativa sulla privacy. L'utente è inoltre consapevole che i dati verranno gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy. Il testo del Contratto di licenza e dell'Informativa sulla privacy è incluso nel kit di distribuzione di Kaspersky Security Center. È necessario accettare le condizioni del Contratto di licenza e dell'Informativa sulla privacy per installare l'applicazione o per eseguire l'upgrade da una versione precedente dell'applicazione.

Installazione delle applicazioni tramite pacchetti indipendenti

Kaspersky Security Center consente di creare pacchetti di installazione indipendenti per le applicazioni. Un pacchetto di installazione indipendente è un file eseguibile che può essere posizionato su un server Web, inviato per e-mail o trasferito in altro modo a un dispositivo client. Il file ricevuto può essere eseguito in locale nel dispositivo client per installare un'applicazione senza utilizzare Kaspersky Security Center.

Il Network Agent autonomo per Linux ha una dipendenza facoltativa dall'utilità nmap. Se l'utilità nmap è mancante o è precedente alla versione 6.0, la funzionalità Broadcast DHCP Discover non è supportata.

Per installare un'applicazione utilizzando un pacchetto di installazione indipendente:

1. Eseguire la connessione all'Administration Server desiderato.

2. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Pacchetti di installazione**.

3. Nell'area di lavoro selezionare il pacchetto di installazione dell'applicazione desiderata.

4. Avviare il processo di creazione di un pacchetto di installazione indipendente in uno dei seguenti modi:

   - Selezionando **Crea pacchetto di installazione indipendente** nel menu di scelta rapida del pacchetto di installazione.
   - Fare clic sul collegamento **Crea pacchetto di installazione indipendente** nell'area di lavoro del pacchetto di installazione.

   Verrà avviata la Creazione guidata pacchetto di installazione indipendente. Seguire le istruzioni della procedura guidata.

   Nel passaggio finale della procedura guidata, selezionare un metodo per il trasferimento del pacchetto di installazione indipendente a un dispositivo client.

5. Trasferire il pacchetto di installazione indipendente nel dispositivo client.
6. Eseguire il pacchetto di installazione indipendente nel dispositivo client.

L'applicazione verrà installata nel dispositivo client con le impostazioni specificate nel pacchetto indipendente.

Quando si crea un pacchetto di installazione indipendente, questo viene automaticamente pubblicato nel server Web. Il collegamento per il download del pacchetto indipendente viene visualizzato nell'elenco dei pacchetti di installazione indipendenti creati. Se necessario, è possibile annullare la pubblicazione del pacchetto indipendente selezionato e ripubblicarlo sul server Web. Per impostazione predefinita, per il download dei pacchetti di installazione indipendenti viene utilizzata la porta 8060.

Impostazioni del pacchetto di installazione di Network Agent

Per configurare un pacchetto di installazione di Network Agent:

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Pacchetti di installazione**.

   La cartella **Installazione remota** è una sottocartella della cartella **Avanzate** per impostazione predefinita.

2. Nel menu di scelta rapida del pacchetto di installazione di Network Agent selezionare **Proprietà**.

Verrà visualizzata la finestra delle proprietà del pacchetto di installazione di Network Agent.

Generale

Nella sezione **Generale** vengono visualizzate informazioni generali sul pacchetto di installazione:

- Nome pacchetto di installazione
- Nome e versione dell'applicazione per cui è stato creato il pacchetto di installazione
- Dimensione del pacchetto di installazione
- Data di creazione del pacchetto di installazione
- Percorso della cartella del pacchetto di installazione

Impostazioni

Questa sezione presenta le impostazioni necessarie per assicurare il corretto funzionamento di Network Agent subito dopo essere stato installato. Le impostazioni in questa sezione sono disponibili solo nei dispositivi che eseguono Windows.

Nel gruppo di impostazioni **Cartella di destinazione** è possibile selezionare la cartella del dispositivo client in cui verrà installato Network Agent.

- **Installa nella cartella predefinita**

  Se questa opzione è selezionata, Network Agent verrà installato nella cartella <Unità>:\Programmi\Kaspersky Lab\NetworkAgent. Se la cartella non esiste, verrà creata automaticamente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Installa nella cartella specificata**

  Se questa opzione è selezionata, Network Agent verrà installato nella cartella specificata nel campo di immissione.

Nel seguente gruppo di impostazioni è possibile impostare una password per l'attività di disinstallazione remota di Network Agent:

- **Usa password di disinstallazione**

  Se questa opzione è abilitata, facendo clic sul pulsante **Modifica** è possibile immettere la password di disinstallazione (disponibile solo per Network Agent nei dispositivi che eseguono sistemi operativi Windows).

  Per impostazione predefinita, questa opzione è disabilitata.

- **Stato**

  Stato della password: **Password impostata** o **Password non impostata**.

  Per impostazione predefinita, questa password non è impostata.

- **Proteggi il servizio Network Agent dalle operazioni non autorizzate di rimozione o terminazione e impedisci la modifica delle impostazioni**

  Quando questa opzione è abilitata, dopo l'installazione di Network Agent in un dispositivo gestito, il componente non può essere rimosso o riconfigurato senza i privilegi richiesti. Il servizio Network Agent non può essere arrestato. Questa opzione non ha effetto sui controller di dominio.

  Abilitare questa opzione per proteggere Network Agent sulle workstation gestite con diritti di amministratore locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito**

  Se questa opzione è abilitata, tutti gli aggiornamenti e le patch scaricati per Administration Server, Network Agent, Administration Console, e iOS MDM Server verranno installati automaticamente.

  Se questa opzione è disabilitata, tutti gli aggiornamenti e le patch scaricati verranno installati solo dopo l'impostazione dello stato su *Approvato*. Gli aggiornamenti e le patch con lo stato *Indefinito* non verranno installati.

  Per impostazione predefinita, questa opzione è abilitata.

Connessione

In questa sezione è possibile configurare la connessione di Network Agent ad Administration Server. Per stabilire una connessione, è possibile utilizzare il protocollo SSL o UDP. Per configurare la connessione, specificare le seguenti impostazioni:

- **Administration Server**

  Indirizzo del dispositivo in cui è installato Administration Server.

- **Porta**

  Il numero di porta utilizzato per la connessione.

- **Porta SSL**

  Numero di porta utilizzato per la connessione tramite il protocollo SSL.

- **Usa certificato server**

  Se questa opzione è abilitata, l'autenticazione dell'accesso di Network Agent ad Administration Server utilizzerà il file di certificato che è possibile specificare facendo clic sul pulsante **Sfoglia**.

  Se questa opzione è disabilitata, il file di certificato verrà ricevuto da Administration Server alla prima connessione di Network Agent all'indirizzo specificato nel campo **Indirizzo server**.

  È consigliabile non disabilitare questa opzione, poiché la ricezione automatica di un certificato di Administration Server da parte di Network Agent al momento della connessione ad Administration Server è considerata non sicura.

  Per impostazione predefinita, questa casella di controllo è selezionata.

- **Usa SSL**

  Se questa opzione è abilitata, la connessione ad Administration Server viene stabilita attraverso una porta sicura tramite SSL.

  Per impostazione predefinita, questa opzione è disabilitata. È consigliabile non disabilitare questa opzione in modo che la connessione rimanga protetta.

- **Usa porta UDP**

  Se questa opzione è abilitata, Network Agent è connesso ad Administration Server tramite una porta UDP. Ciò consente di gestire i dispositivi client e ricevere informazioni in merito.

  La porta UDP deve essere aperta nei dispositivi gestiti in cui è installato Network Agent. È pertanto consigliabile non disabilitare questa opzione.

  Per impostazione predefinita, questa opzione è abilitata.

- **Numero di porta UDP**

  In questo campo è possibile specificare la porta utilizzata per la connessione di Administration Server a Network Agent tramite il protocollo UDP.

  La porta UDP predefinita è 15000.

- **Apri porte di Network Agent in Microsoft Windows Firewall**

  Se questa opzione è abilitata, le porte utilizzate da Network Agent vengono aggiunte all'elenco di esclusioni di Microsoft Windows Firewall.

  Per impostazione predefinita, questa opzione è abilitata.

- **Usa server proxy**

  Se questa opzione è abilitata, specificare i parametri del server proxy:

  - **Indirizzo server proxy**
  - **Porta server proxy**

  Se il server proxy richiede l'autenticazione, abilitare l'opzione **Autenticazione server proxy** e specificare il **Nome utente** e la **Password** dell'account con cui viene stabilita la connessione al server proxy. È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.

Per motivi di compatibilità, non è consigliabile specificare le impostazioni di connessione proxy nelle impostazioni del pacchetto di installazione di Network Agent.

Avanzate

Nella sezione **Avanzate** è possibile configurare il metodo di utilizzo del gateway di connessione. A tale scopo, è possibile eseguire le seguenti operazioni:

- Utilizzare Network Agent come gateway di connessione nella rete perimetrale per connettersi ad Administration Server, comunicare con esso e assicurare la protezione dei dati in Network Agent durante la trasmissione dei dati.
- Connettersi ad Administration Server utilizzando un gateway di connessione per ridurre il numero di connessioni ad Administration Server. In questo caso, inserire l'indirizzo del dispositivo che fungerà da gateway di connessione nel campo **Indirizzo gateway connessione**.
- Configurare la connessione per Virtual Desktop Infrastructure (VDI) se la rete include macchine virtuali. A tale scopo, eseguire le seguenti operazioni:
  - **Abilita modalità dinamica per VDI**

    Se questa opzione è abilitata, la modalità dinamica per Virtual Desktop Infrastructure (VDI) sarà abilitata per Network Agent installato in una macchina virtuale.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Ottimizza le impostazioni per VDI**

    Se questa opzione è abilitata, le seguenti funzionalità sono disabilitate nelle impostazioni di Network Agent:
    - Recupero delle informazioni sul software installato
    - Recupero delle informazioni sull'hardware
    - Recupero delle informazioni sulle vulnerabilità rilevate
    - Recupero delle informazioni sugli aggiornamenti richiesti

    Per impostazione predefinita, questa opzione è disabilitata.

- **Consenti l'esecuzione dell'utilità di registrazione utente dopo l'installazione di Network Agent**

  Se questa opzione è abilitata, la registrazione dell'utente come utilità del proprietario del dispositivo verrà eseguita dopo l'installazione di Network Agent. Per impostazione predefinita, questa opzione è disabilitata.

Componenti aggiuntivi

In questa sezione è possibile selezionare i componenti aggiuntivi per l'installazione simultanea con Network Agent.

Tag

La sezione **Tag** visualizza un elenco di parole chiave (tag) che possono essere aggiunte ai dispositivi client dopo l'installazione di Network Agent. È possibile aggiungere e rimuovere tag dall'elenco, nonché rinominarli.

Se la casella di controllo accanto a un tag è selezionata, il tag viene aggiunto automaticamente ai dispositivi gestiti durante l'installazione di Network Agent.

Se la casella di controllo accanto a un tag è deselezionata, il tag non viene aggiunto automaticamente ai dispositivi gestiti durante l'installazione di Network Agent. È possibile aggiungere manualmente il tag ai dispositivi.

Rimuovendo un tag dall'elenco, il tag viene rimosso automaticamente da tutti i dispositivi a cui è stato aggiunto.

Cronologia revisioni

In questa sezione è possibile visualizzare la cronologia delle revisioni del pacchetto di installazione. È possibile confrontare le revisioni, visualizzare le revisioni, salvare le revisioni in un file e aggiungere e modificare le descrizioni delle revisioni.

Le impostazioni del pacchetto di installazione di Network Agent disponibili per un sistema operativo specifico sono riportate nella tabella seguente.

Impostazioni del pacchetto di installazione di Network Agent

Sezione delle proprietà	Windows	Mac	Linux
Generale	✓	✓	✓
Impostazioni	✓	—	—
Connessione	✓	✓ (ad eccezione delle opzioni **Apri porte di Network Agent in Microsoft Windows Firewall** e **Usa solo il rilevamento automatico del server proxy**)	✓ (ad eccezione delle opzioni **Apri porte di Network Agent in Microsoft Windows Firewall** e **Usa solo il rilevamento automatico del server proxy**)
Avanzate	✓	✓	✓
Componenti aggiuntivi	✓	✓	✓
Tag	✓	✓ (ad eccezione delle regole di tagging automatico)	✓ (ad eccezione delle regole di tagging automatico)
Cronologia revisioni	✓	✓	✓

Visualizzazione dell'Informativa sulla privacy

L'Informativa sulla privacy è disponibile online all'indirizzo https://www.kaspersky.com/products-and-services-privacy-policy ed è disponibile anche offline. È possibile leggere l'Informativa sulla privacy ad esempio prima di installare Network Agent.

Per leggere l'Informativa sulla privacy offline:

1. Avviare il programma di installazione di Kaspersky Security Center.
2. Nella finestra del programma di installazione passare al collegamento **Estrai pacchetti di installazione**.
3. Nell'elenco visualizzato selezionare Kaspersky Security Center Network Agent, quindi fare clic su **Avanti**.

Il file privacy_policy.txt viene visualizzato nel dispositivo, nella cartella specificata, nella sottocartella NetAgent.

Distribuzione di sistemi per la gestione dei dispositivi mobili

In questa sezione viene descritta la distribuzione di sistemi per la gestione dei dispositivi mobili tramite i protocolli MDM iOS e Kaspersky Endpoint Security.

Distribuzione di un sistema per la gestione tramite il protocollo MDM iOS

Kaspersky Security Center consente di gestire i dispositivi mobili in cui viene eseguito iOS. I dispositivi MDM iOS sono dispositivi mobili iOS connessi a un server MDM iOS e gestiti da Administration Server.

I dispositivi mobili sono connessi a un server MDM iOS tramite i seguenti passaggi:

1. L'amministratore installa il server MDM iOS.
2. L'amministratore riceve un certificato Apple Push Notification Service (APNs) (Ricezione di un certificato APNs, https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   Il certificato APNs consente ad Administration Server di connettersi al server APNs per inviare notifiche push ai dispositivi MDM iOS.
3. L'amministratore installa il certificato APNs nel server per dispositivi mobili MDM iOS.
4. L'amministratore crea un profilo MDM iOS per l'utente del dispositivo mobile iOS.

   Il profilo MDM iOS contiene una raccolta di impostazioni per la connessione dei dispositivi mobili iOS all'Administration Server.

Dopo aver installato il profilo MDM iOS e aver sincronizzato il dispositivo MDM iOS con Administration Server, il dispositivo verrà visualizzato in **Mobile devices**, una sottocartella di **Mobile Device Management** nella struttura della console.

Installazione del server MDM iOS

Per installare il server MDM iOS in un dispositivo locale:

1. Eseguire il file eseguibile setup.exe.

   Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da installare.

   Nella finestra di selezione delle applicazioni fare clic sul collegamento **Installa server MDM iOS** per eseguire l'Installazione guidata del server MDM iOS.
2. Selezionare una cartella di destinazione.

   La cartella predefinita è <Unità>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. Se tale cartella non esiste, verrà creata automaticamente durante l'installazione. È possibile modificare la cartella di destinazione utilizzando il pulsante **Sfoglia**.

3. Nella finestra **Specificare le impostazioni per la connessione al server per dispositivi mobili MDM iOS** della procedura guidata, nel campo **Porta esterna per la connessione al servizio MDM iOS**, specificare una porta esterna per la connessione dei dispositivi mobili al servizio MDM iOS.

   I dispositivi mobili utilizzano la porta esterna 5223 per la comunicazione con il server APNs. Verificare che la porta 5223 sia aperta nel firewall per la connessione con l'intervallo di indirizzi 17.0.0.0/8.

   La porta 443 è utilizzata per impostazione predefinita per la connessione al server MDM iOS. Se la porta 443 è già in uso da parte di un altro servizio o un'altra applicazione, può essere sostituita, ad esempio dalla porta 9443.

   Il server MDM iOS utilizza la porta esterna 2197 per l'invio delle notifiche al server APNs.

   I server APNs vengono eseguiti in modalità di bilanciamento del carico. I dispositivi mobili non si connettono sempre agli stessi indirizzi IP per la ricezione delle notifiche. L'intervallo di indirizzi 17.0.0.0/8 è riservato per Apple, pertanto è consigliabile specificare questo intero intervallo come intervallo consentito nelle impostazioni del firewall.

4. Per configurare manualmente le porte di interazione per i componenti dell'applicazione, selezionare l'opzione **Configura porte locali manualmente** e specificare i valori per le seguenti impostazioni:

   - **Porta per la connessione a Network Agent**. In questo campo specificare una porta per la connessione del servizio MDM iOS a Network Agent. Il numero di porta predefinito è 9799.
   - **Porta locale per la connessione al servizio MDM iOS**. In questo campo specificare una porta locale per la connessione di Network Agent al servizio MDM iOS. Il numero di porta predefinito è 9899.

   È consigliabile utilizzare i valori predefiniti.

5. Nella finestra **Indirizzo esterno del server per dispositivi mobili** della procedura guidata, nel campo **Indirizzo Web per la connessione remota al server per dispositivi mobili**, specificare l'indirizzo del dispositivo client in cui deve essere installato il server per dispositivi mobili MDM iOS.

   Questo indirizzo verrà utilizzato per la connessione dei dispositivi mobili gestiti al servizio MDM iOS. Il dispositivo client deve essere disponibile per la connessione dei dispositivi MDM iOS.

   È possibile specificare l'indirizzo di un dispositivo client in qualsiasi dei seguenti formati:

   - FQDN del dispositivo (ad esempio mdm.example.com)
   - Nome NetBIOS del dispositivo

   Evitare di aggiungere lo schema URL e il numero di porta alla stringa dell'indirizzo: questi valori verranno aggiunti automaticamente.

Al termine della procedura guidata, il server MDM iOS viene installato nel dispositivo locale. Il server per dispositivi mobili MDM iOS verrà visualizzato nella cartella **Mobile Device Management** nella struttura della console.

Installazione di un server MDM iOS in modalità automatica

Kaspersky Security Center consente di installare il server MDM iOS in un dispositivo locale in modalità automatica, ovvero senza l'immissione interattiva delle impostazioni di installazione.

Per installare un server MDM iOS in un dispositivo locale in modalità automatica:

1. Leggere il Contratto di licenza con l'utente finale. Utilizzare il comando di seguito solo se sono stati compresi e accettati i termini del Contratto di licenza con l'utente finale.

2. Eseguire il seguente comando:

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <parametri_installazione>"
   ```

   dove `parametri_installazione` è un elenco di impostazioni e dei valori corrispondenti separati da spazi (`PROP1=PROP1VAL PROP2=PROP2VAL`). Il file setup.exe è posizionato nella cartella Server, appartenente al kit di distribuzione di Kaspersky Security Center.

I nomi e i possibili valori per i parametri che è possibile utilizzare durante l'installazione del server per dispositivi mobili MDM iOS in modalità automatica sono elencati nella seguente tabella. I parametri possono essere specificati in qualsiasi ordine.

I parametri di installazione del server MDM iOS in modalità automatica

Nome del parametro	Descrizione del parametro	Valori disponibili
EULA	Accettazione dei termini del Contratto di licenza con l'utente finale. Questo parametro è obbligatorio.	• 1 - Ho letto, compreso e accettato i termini del Contratto di licenza con l'utente finale. • Altri valori o nessun valore- Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita).
DONT_USE_ANSWER_FILE	Scelta di utilizzare o non utilizzare un file XML con le impostazioni di installazione del server MDM iOS. Il file XML è incluso nel pacchetto di installazione oppure viene memorizzato in Administration Server. Non è necessario specificare un percorso aggiuntivo per il file. Questo parametro è obbligatorio.	• 1 – Non utilizzare il file XML con parametri. • Altro valore o nessun valore – Utilizzare il file XML con parametri.
INSTALLDIR	Cartella di installazione del server MDM iOS. Questo parametro è facoltativo.	Valore della stringa, ad esempio `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	Porta locale per la connessione del servizio MDM iOS a Network Agent. Il numero di porta predefinito è 9799. Questo parametro è facoltativo.	Valore numerico.
LOCALSERVERPORT	Porta locale per la connessione di Network Agent al servizio MDM iOS. Il numero di porta predefinito è 9899. Questo parametro è facoltativo.	Valore numerico.
EXTERNALSERVERPORT	Porta per la connessione di un dispositivo al server MDM iOS. Il numero di porta predefinito è 443. Questo parametro è facoltativo.	Valore numerico.
EXTERNAL_SERVER_URL	Indirizzo esterno del dispositivo client in cui verrà installato il server MDM iOS. Questo indirizzo verrà utilizzato per la connessione dei dispositivi mobili gestiti al servizio MDM iOS. Il dispositivo client deve essere disponibile per la connessione tramite MDM iOS. L'indirizzo non deve includere lo schema URL e il numero della porta poiché questi valori verranno aggiunti automaticamente. Questo parametro è facoltativo.	• FQDN del dispositivo (ad esempio mdm.example.com) • Nome NetBIOS del dispositivo • Indirizzo IP dispositivo

Nome del parametro	Descrizione del parametro	Valori disponibili
WORKFOLDER	Cartella di lavoro del server MDM iOS. Se non è specificata alcuna cartella di lavoro, i dati verranno scritti nella cartella predefinita. Questo parametro è facoltativo.	Valore della stringa, ad esempio `WORKFOLDER=\"C:\work\"`
MTNCY	Utilizzo del server MDM iOS da parte di più server virtuali. Questo parametro è facoltativo.	• 1 – Il server MDM iOS verrà utilizzato da parte di più Administration Server virtuali. • Altro valore o nessun valore definito – Il server MDM iOS non verrà utilizzato da più Administration Server virtuali.

Esempio:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

I parametri di installazione del server per dispositivi mobili MDM iOS sono specificati in dettaglio nella sezione "Installazione del server per dispositivi mobili MDM iOS".

Scenari di distribuzione del server MDM iOS

Il numero di copie del server MDM iOS da installare può essere selezionato in base all'hardware disponibile o al numero totale di dispositivi mobili coperti.

Tenere presente che il numero massimo consigliato di dispositivi mobili per una singola installazione di Kaspersky Device Management for iOS è 50.000. Per ridurre il carico, l'intero pool di dispositivi può essere distribuito tra diversi server in cui è installato il server MDM iOS.

L'autenticazione dei dispositivi MDM iOS è eseguita tramite i certificati utente (qualsiasi profilo installato in un dispositivo contiene il certificato del proprietario del dispositivo). Sono pertanto possibili due schemi di distribuzione per un server MDM iOS:

- Schema semplificato
- Schema di distribuzione tramite Kerberos Constrained Delegation (KCD)

Schema di distribuzione semplificato

Durante la distribuzione di un server MDM iOS in base allo schema semplificato, i dispositivi mobili si connettono direttamente al servizio Web MDM iOS. In questo caso, i certificati utente emessi da Administration Server possono essere applicati solo per l'autenticazione dei dispositivi. L'integrazione con l'infrastruttura a chiave pubblica (PKI) è impossibile per i certificati utente.

Schema di distribuzione tramite Kerberos Constrained Delegation (KCD)

Per utilizzare lo schema di distribuzione con la delega vincolata Kerberos (KCD), è necessario soddisfare i seguenti requisiti:

- Administration Server e il server MDM iOS si trovano nella rete interna dell'organizzazione.
- È in uso un proxy inverso con supporto di KCD.

Questo schema di distribuzione offre quanto segue:

- Integrazione con il proxy inverso che supporta KCD
- Utilizzo di KCD per l'autenticazione dei dispositivi mobili
- Integrazione con PKI per l'applicazione dei certificati utente

Quando si utilizza questo schema di distribuzione, è necessario eseguire le seguenti operazioni:

- In Administration Console, nelle impostazioni del servizio Web MDM iOS, selezionare la casella di controllo **Assicura la compatibilità con la delega vincolata Kerberos**.
- Come certificato per il servizio Web MDM iOS, specificare il certificato personalizzato che è stato definito al momento della pubblicazione del servizio Web MDM iOS nel proxy inverso.
- I certificati utente per i dispositivi iOS devono essere emessi dall'Autorità di certificazione (CA) del dominio. Se il dominio contiene più Autorità di certificazione radice, i certificati utente devono essere emessi dall'Autorità di certificazione che è stata specificata al momento della pubblicazione del servizio Web MDM iOS nel proxy inverso.

  È possibile garantire che il certificato utente sia conforme con questo requisito di emissione da parte dell'Autorità di certificazione utilizzando uno dei seguenti metodi:

  - Specificare il certificato utente nella procedura guidata per la creazione di un nuovo profilo MDM iOS e nell'Installazione guidata certificato.
  - Integrare l'Administration Server con l'infrastruttura PKI del dominio e definire l'impostazione corrispondente nelle regole per l'emissione dei certificati:

    1. Nella struttura della console espandere la cartella **Mobile Device Management**, quindi selezionare la sottocartella **Certificati**.
    2. Nell'area di lavoro della cartella **Certificati** fare clic sul pulsante **Configura regole di emissione certificati** per aprire la finestra **Regole di emissione certificati**.
    3. Nella sezione **Integrazione con PKI** configurare l'integrazione con l'infrastruttura a chiave pubblica (PKI).
    4. Nella sezione **Emissione di certificati mobili** specificare l'origine dei certificati.

Di seguito è riportato un esempio di configurazione di Kerberos Constrained Delegation (KCD) con i seguenti presupposti:

- Il servizio Web MDM iOS è in esecuzione sulla porta 443.
- Il nome del dispositivo con il proxy inverso è firewall.mydom.local.
- Il nome del dispositivo con il servizio Web MDM iOS è iosmdm.mydom.local.
- Il nome della pubblicazione esterna del servizio Web MDM iOS è iosmdm.mydom.global.

Nome dell'entità servizio per http/iosmdm.mydom.local

Nel dominio è necessario registrare il nome dell'entità servizio (SPN) per il dispositivo con il servizio Web MDM iOS (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Configurazione delle proprietà di dominio del dispositivo con il proxy inverso (firewall.mydom.local)

Per delegare il traffico, impostare come attendibile il dispositivo con il proxy inverso (firewall.mydom.local) per il servizio definito dall'SPN (http/iosmdm.mydom.local).

Per impostare come attendibile il dispositivo con il proxy inverso per il servizio definito dall'SPN (http/iosmdm.mydom.local), l'amministratore deve eseguire seguenti le operazioni:

1. Nello snap-in Microsoft Management Console "Utenti e computer di Active Directory" selezionare il dispositivo in cui è installato il proxy inverso (firewall.mydom.local).
2. Nelle proprietà del dispositivo, nella scheda **Delega**, impostare l'interruttore **Computer attendibile per la delega solo ai servizi specificati** su **Utilizza un qualsiasi protocollo di autenticazione**.
3. Aggiungere l'SPN (http/iosmdm.mydom.local) all'elenco **Servizi ai quali l'account può presentare credenziali delegate**.

Speciale certificato (personalizzato) per il servizio Web pubblicato (iosmdm.mydom.global)

È necessario emettere uno speciale certificato (personalizzato) per il servizio Web MDM iOS sul nome FQDN iosmdm.mydom.global e specificare che sostituisce il certificato predefinito nelle impostazioni del servizio Web MDM iOS in Administration Console.

Il contenitore del certificato (file con estensione p12 o pfx) deve anche contenere una catena di certificati radice (chiavi pubbliche).

Pubblicazione del servizio Web MDM iOS nel proxy inverso

Nel proxy inverso, per il traffico da un dispositivo mobile alla porta 443 di iosmdm.mydom.global, è necessario configurare KCD sull'SPN (http/iosmdm.mydom.local) utilizzando il certificato emesso per il nome FQDN (iosmdm.mydom.global). Tenere presente che la pubblicazione e il servizio Web pubblicato devono condividere lo stesso certificato server.

Ricezione di un certificato APNs

> Se si dispone già di un certificato APNs, è opportuno rinnovarlo anziché crearne uno nuovo. Quando si sostituisce il certificato APNs esistente con uno appena creato, Administration Server perde la capacità di gestire i dispositivi mobili iOS connessi al momento.

Quando, nella prima fase della procedura guidata del certificato APNs, viene creata la richiesta di firma del certificato, la relativa chiave privata viene archiviata nella RAM del dispositivo. Pertanto, è necessario completare tutti i passaggi della procedura guidata in una sola sessione dell'applicazione.

Per ricevere un certificato APNs:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Server per dispositivi mobili**.

2. Nell'area di lavoro della cartella **Server per dispositivi mobili** selezionare un server per dispositivi mobili MDM iOS.

3. Nel menu di scelta rapida del server per dispositivi mobili MDM iOS selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del server MDM iOS.

4. Nella finestra delle proprietà del server per dispositivi mobili MDM iOS selezionare la sezione **Certificati**.

5. Nella sezione **Certificati**, nel gruppo di impostazioni **Certificato Apple Push Notification**, fare clic sul pulsante **Richiedi nuovo**.

   Verrà avviata la ricezione guidata del certificato APNs e verrà visualizzata la finestra **Richiedi nuovo**.

6. Creare una richiesta di firma del certificato (di seguito indicata come CSR, Certificate Signing Request). A tale scopo, eseguire le seguenti operazioni:

   a. Fare clic sul pulsante **Crea CSR**.

   b. Nella finestra **Crea CSR** visualizzata specificare un nome per la richiesta, i nomi dell'azienda e del reparto, la città, la regione e il paese.

   c. Fare clic sul pulsante **Salva** e specificare un nome per il file in cui salvare CSR.

   La chiave privata del certificato verrà salvata nella memoria del dispositivo.

7. Utilizzare il CompanyAccount per inviare il file con CSR creato a Kaspersky per la firma.

   > La firma della CSR verrà resa disponibile solo dopo aver caricato nel portale CompanyAccount una chiave che consente l'utilizzo della funzionalità Mobile Device Management.

   Al termine dell'elaborazione della richiesta online, l'utente riceverà un file CSR firmato da Kaspersky.

8. Inviare il file CSR firmato al sito Web Apple Inc. tramite un ID Apple casuale.

   È consigliabile non utilizzare un ID Apple personale. Creare un ID Apple dedicato da utilizzare come ID aziendale. Dopo aver creato un ID Apple, collegarlo alla cassetta postale dell'organizzazione, non alla cassetta postale di un dipendente.

   Al termine dell'elaborazione della CSR in Apple Inc., si riceverà la chiave pubblica del certificato APNs. Salvare il file su disco.

9. Esportare il certificato APNs insieme alla chiave privata creata durante la generazione della CSR, nel formato di file PFX. A tale scopo:

   a. Nella finestra **Richiedi nuovo certificato APNs** fare clic sul pulsante **Completa CSR**.

   b. Nella finestra **Apri** scegliere un file con la chiave pubblica del certificato ricevuto da Apple Inc. al termine dell'elaborazione della CSR, quindi fare clic sul pulsante **Apri**.

      Verrà avviato il processo di esportazione del certificato.

   c. Nella finestra successiva immettere la password della chiave privata e fare clic su **OK**.

      Questa password sarà utilizzata per l'installazione del certificato APNs nel server MDM iOS.

   d. Nella finestra **Salva certificato APNs** specificare il nome del file per il certificato APNs, scegliere una cartella e fare clic su **Salva**.

Le chiave pubblica e la chiave privata del certificato vengono combinate e il certificato APNs viene salvato in formato PFX. Successivamente è possibile installare il certificato APNs nel server per dispositivi mobili MDM iOS.

Rinnovo di un certificato APNs

Per rinnovare un certificato APNs:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Server per dispositivi mobili**.

2. Nell'area di lavoro della cartella **Server per dispositivi mobili** selezionare un server per dispositivi mobili MDM iOS.

3. Nel menu di scelta rapida del server per dispositivi mobili MDM iOS selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del server MDM iOS.

4. Nella finestra delle proprietà del server per dispositivi mobili MDM iOS selezionare la sezione **Certificati**.

5. Nella sezione **Certificati**, nel gruppo di impostazioni **Certificato Apple Push Notification** fare clic sul pulsante **Rinnova**.

   Verrà avviata la procedura guidata di rinnovo del certificato APNs e sarà visualizzata la finestra **Rinnova certificato APNs**.

6. Creare una richiesta di firma del certificato (di seguito indicata come CSR, Certificate Signing Request). A tale scopo, eseguire le seguenti operazioni:

   a. Fare clic sul pulsante **Crea CSR**.

   b. Nella finestra **Crea CSR** visualizzata specificare un nome per la richiesta, i nomi dell'azienda e del reparto, la città, la regione e il paese.

   c. Fare clic sul pulsante **Salva** e specificare un nome per il file in cui salvare CSR.

   La chiave privata del certificato verrà salvata nella memoria del dispositivo.

7. Utilizzare il CompanyAccount per inviare il file con CSR creato a Kaspersky per la firma.

   La firma della CSR verrà resa disponibile solo dopo aver caricato nel portale CompanyAccount una chiave che consente l'utilizzo della funzionalità Mobile Device Management.

   Al termine dell'elaborazione della richiesta online, l'utente riceverà un file CSR firmato da Kaspersky.

8. Inviare il file CSR firmato al sito Web Apple Inc. tramite un ID Apple casuale.

   È consigliabile non utilizzare un ID Apple personale. Creare un ID Apple dedicato da utilizzare come ID aziendale. Dopo aver creato un ID Apple, collegarlo alla cassetta postale dell'organizzazione, non alla cassetta postale di un dipendente.

   Al termine dell'elaborazione della CSR in Apple Inc., si riceverà la chiave pubblica del certificato APNs. Salvare il file su disco.

9. Richiedere la chiave pubblica del certificato. A tale scopo, eseguire le seguenti operazioni:

   a. Passare al portale Apple Push Certificates. Per accedere al portale, utilizzare l'ID Apple ricevuto al momento della richiesta iniziale del certificato.

   b. Nell'elenco dei certificati selezionare il certificato il cui nome APSP (nel formato "APSP: <numero>") corrisponde al nome APSP del certificato utilizzato dal server per dispositivi mobili MDM iOS, quindi fare clic sul pulsante **Rinnova**.

      Il certificato APNs viene rinnovato.

   c. Salvare il certificato creato nel portale.

10. Esportare il certificato APNs insieme alla chiave privata creata durante la generazione della CSR, nel formato di file PFX. A tale scopo, eseguire le seguenti operazioni:

    a. Nella finestra **Rinnova certificato APNs** fare clic sul pulsante **Completa CSR**.

    b. Nella finestra **Apri** scegliere un file con la chiave pubblica del certificato, ricevuto da Apple Inc. al termine dell'elaborazione della CSR, e fare clic sul pulsante **Apri**.

       Verrà avviato il processo di esportazione del certificato.

    c. Nella finestra successiva immettere la password della chiave privata e fare clic su **OK**.

       Questa password sarà utilizzata per l'installazione del certificato APNs nel server MDM iOS.

    d. Nella finestra **Rinnova certificato APNs** visualizzata specificare il nome del file per il certificato APNs, scegliere una cartella e fare clic su **Salva**.

Le chiave pubblica e la chiave privata del certificato vengono combinate e il certificato APNs viene salvato in formato PFX.

Configurazione di un certificato del server per dispositivi mobili MDM iOS di riserva

La funzionalità server per dispositivi mobili MDM iOS consente di emettere un certificato di riserva. Questo certificato è destinato all'utilizzo nei profili MDM iOS, per garantire il passaggio immediato dei dispositivi iOS gestiti dopo la scadenza del certificato del server per dispositivi mobili MDM iOS.

Se il server per dispositivi mobili MDM iOS utilizza un certificato predefinito emesso da Kaspersky, è possibile emettere un certificato di riserva (o specificare il certificato personalizzato in uso come di riserva) prima della scadenza del certificato del server per dispositivi mobili MDM iOS. Per impostazione predefinita, il certificato di riserva viene emesso automaticamente 60 giorni prima della scadenza del certificato del server per dispositivi mobili MDM iOS. Il certificato del server per dispositivi mobili MDM iOS di riserva diventa il certificato principale subito dopo la scadenza del certificato del server per dispositivi mobili MDM iOS. La chiave pubblica viene distribuita a tutti i dispositivi gestiti tramite i profili di configurazione, pertanto non è necessario trasmetterla manualmente.

Per emettere un certificato di riserva del server per dispositivi mobili MDM iOS o specificare un certificato di riserva personalizzato:

1. Nella struttura della console, nella cartella **Mobile Device Management**, selezionare la sottocartella **Server per dispositivi mobili**.

2. Nell'elenco dei server per dispositivi mobili selezionare il server per dispositivi mobili MDM iOS pertinente e, nel riquadro di destra, fare clic sul pulsante **Configura server per dispositivi mobili MDM iOS**.

3. Nella finestra delle impostazioni del server per dispositivi mobili MDM iOS visualizzata selezionare la sezione **Certificati**.

4. Nel gruppo di impostazioni **Certificato di riserva** eseguire una delle seguenti operazioni:

   - Se si prevede di continuare a utilizzare un certificato autofirmato (ovvero quello emesso da Kaspersky):

     a. Fare clic sul pulsante **Emetti**.

     b. Nella finestra **Data di attivazione** visualizzata selezionare una delle due opzioni per la data di applicazione del certificato di riserva:

        - Se si desidera applicare il certificato di riserva al momento della scadenza del certificato corrente, selezionare l'opzione **Allo scadere del certificato corrente**.

        - Se si desidera applicare il certificato di riserva prima della scadenza del certificato corrente, selezionare l'opzione **Dopo il periodo specificato (giorni)**. Nel campo di immissione accanto a questa opzione specificare la durata del periodo dopo il quale il certificato di riserva deve sostituire il certificato corrente.

        Il periodo di validità del certificato di riserva specificato non può superare il periodo di validità del certificato del server per dispositivi mobili MDM iOS corrente.

     c. Fare clic sul pulsante **OK**.

     Verrà emesso il certificato del server per dispositivi mobili MDM iOS di riserva.

   - Se si prevede di utilizzare un certificato personalizzato emesso dall'autorità di certificazione:

     a. Fare clic sul pulsante **Aggiungi**.

     b. Nella finestra Esplora file visualizzata specificare un file di certificato nel formato PEM, PFX o P12 archiviato nel dispositivo, quindi fare clic sul pulsante **Apri**.

     Il certificato personalizzato viene specificato come certificato del server per dispositivi mobili MDM iOS di riserva.

È stato specificato un certificato del server per dispositivi mobili MDM iOS di riserva. I dettagli del certificato di riserva sono visualizzati nel gruppo di impostazioni **Certificato di riserva** (nome del certificato, nome dell'emittente, data di scadenza e data di applicazione del certificato di riserva, se presente).

Installazione di un certificato APNs in un server MDM iOS

Dopo aver ricevuto il certificato APNs, è necessario installarlo nel server per dispositivi mobili MDM iOS.

Per installare il certificato APNs nel server MDM iOS:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Server per dispositivi mobili**.

2. Nell'area di lavoro della cartella **Server per dispositivi mobili** selezionare un server per dispositivi mobili MDM iOS.

3. Nel menu di scelta rapida del server per dispositivi mobili MDM iOS selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del server MDM iOS.

4. Nella finestra delle proprietà del server per dispositivi mobili MDM iOS selezionare la sezione **Certificati**.

5. Nella sezione **Certificati**, nel gruppo di impostazioni **Certificato Apple Push Notification**, fare clic sul pulsante **Installa**.

6. Selezionare il file PFX che contiene il certificato APNs.

7. Immettere la password della chiave privata che è stata specificata durante l'esportazione del certificato APNs.

Il certificato APNs verrà installato nel server MDM iOS. I dettagli del certificato verranno visualizzati nella finestra delle proprietà del server per dispositivi mobili MDM iOS, nella sezione **Certificati**.

Configurazione dell'accesso al servizio Apple Push Notification

Per garantire il corretto funzionamento del servizio Web MDM iOS e risposte tempestive dei dispositivi mobili ai comandi dell'amministratore, è necessario specificare un certificato del servizio Apple Push Notification (di seguito denominato certificato APNs) nelle impostazioni del server MDM iOS.

Interagendo con Apple Push Notification (di seguito denominato APNs), il servizio Web MDM iOS si connette all'indirizzo esterno api.push.apple.com tramite la porta 2197 (in uscita). Pertanto, il servizio Web MDM iOS richiede l'accesso alla porta TCP 2197 per l'intervallo di indirizzi 17.0.0.0/8. Sul lato del dispositivo iOS è necessario l'accesso alla porta TCP 5223 per l'intervallo di indirizzi 17.0.0.0/8.

Se si prevede di accedere ad APNs dal servizio Web MDM iOS tramite un server proxy, è necessario eseguire le seguenti operazioni sul dispositivo in cui è installato il servizio Web MDM iOS:

1. Aggiungere le seguenti stringhe al Registro di sistema:

   - Per i sistemi operativi a 32 bit:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Nome host proxy>"
"ApnProxyPort"="<Porta proxy>"
"ApnProxyLogin"="<Nome di accesso proxy>"
"ApnProxyPwd"="<Password proxy>"
```

   - Per i sistemi operativi a 64 bit:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Nome host proxy>"
"ApnProxyPort"="<Porta proxy>"
"ApnProxyLogin"="<Nome di accesso proxy>"
"ApnProxyPwd"="<Password proxy>"
```

2. Riavviare il servizio Web MDM iOS.

Emissione e installazione di un certificato condiviso in un dispositivo mobile

Per rilasciare un certificato condiviso a un utente:

1. Nella struttura della console, nella cartella **Account utente**, selezionare un account utente.
2. Nel menu di scelta rapida dell'account utente selezionare **Installa certificato**.

   Verrà avviata l'Installazione guidata certificato. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, verrà creato un certificato, che sarà aggiunto all'elenco dei certificati dell'utente.

Il certificato emesso verrà scaricato dall'utente, insieme al pacchetto di installazione che contiene il profilo MDM iOS.

Una volta connesso il dispositivo mobile al server MDM iOS, le impostazioni del profilo MDM iOS verranno applicate al dispositivo dell'utente. L'amministratore sarà in grado di gestire il dispositivo in seguito alla connessione.

Il dispositivo mobile dell'utente connesso al server per dispositivi mobili MDM iOS viene visualizzato nella sottocartella **Dispositivi mobili**, all'interno della cartella **Mobile Device Management** nella struttura della console.

Aggiunta di un dispositivo KES all'elenco dei dispositivi gestiti

Per aggiungere il dispositivo KES di un utente all'elenco dei dispositivi gestiti utilizzando un collegamento a Google Play™:

1. Nella struttura della console selezionare la cartella **Account utente**.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.
2. Selezionare l'account dell'utente di cui si desidera aggiungere il dispositivo mobile all'elenco dei dispositivi gestiti.
3. Nel menu di scelta rapida dell'account utente selezionare **Aggiungi dispositivo mobile**.

   Verrà avviata la Connessione guidata nuovo dispositivo mobile. Nella finestra **Origine certificato** della procedura guidata, è necessario specificare il metodo per la creazione del certificato condiviso che Administration Server utilizzerà per identificare il dispositivo mobile. È possibile specificare un certificato condiviso utilizzando una delle seguenti modalità:

   - Creare un certificato condiviso automaticamente, tramite gli strumenti di Administration Server, e quindi inviare il certificato al dispositivo.
   - Specificare il file di un certificato condiviso.
4. Nella finestra **Tipo di dispositivo** della procedura guidata selezionare **Collegamento a Google Play**.

5. Nella finestra **Metodo di notifica all'utente** della procedura guidata, definire le impostazioni per la notifica all'utente del dispositivo mobile della creazione del certificato con un messaggio SMS, tramite e-mail o visualizzando l'informazione al termine della procedura guidata.

6. Nella finestra Info sul certificato della procedura guidata, fare clic sul pulsante **Fine** per chiudere la procedura guidata.

Al termine delle attività della procedura guidata, al dispositivo mobile dell'utente verranno inviati un collegamento e un codice QR per consentire il download di Kaspersky Endpoint Security da Google Play. L'utente accede a Google Play utilizzando il collegamento o eseguendo la scansione del codice QR. Dopodiché, il sistema operativo del dispositivo richiede all'utente di accettare l'installazione di Kaspersky Endpoint Security for Android. Dopo il download e l'installazione di Kaspersky Endpoint Security for Android, il dispositivo mobile si connette ad Administration Server e scarica un certificato condiviso. Dopo l'installazione del certificato nel dispositivo mobile, il dispositivo verrà visualizzato nella cartella **Dispositivi mobili**, una sottocartella di **Mobile Device Management** nella struttura della console.

Se Kaspersky Endpoint Security for Android è già stato installato nel dispositivo, l'utente deve ricevere le impostazioni di connessione di Administration Server dall'amministratore e quindi immetterle autonomamente. Dopo la definizione delle impostazioni di connessione, il dispositivo mobile si connette ad Administration Server. L'amministratore emette un certificato condiviso per il dispositivo e invia all'utente un messaggio e-mail o un messaggio SMS con un nome utente e una password per il download del certificato. L'utente scarica e installa il certificato condiviso. Dopo l'installazione del certificato nel dispositivo mobile, il dispositivo verrà visualizzato nella cartella **Dispositivi mobili**, una sottocartella di **Mobile Device Management** nella struttura della console. In questo caso, Kaspersky Endpoint Security for Android non verrà scaricato e installato nuovamente.

Connessione dei dispositivi KES ad Administration Server

A seconda del metodo utilizzato per la connessione dei dispositivi ad Administration Server, sono possibili due schemi di distribuzione per Kaspersky Device Management for iOS per i dispositivi KES:

- Schema di distribuzione con connessione diretta dei dispositivi all'Administration Server
- Schema di distribuzione che coinvolge un proxy inverso che supporta la delega vincolata Kerberos

Connessione diretta dei dispositivi all'Administration Server

I dispositivi KES possono connettersi direttamente alla porta 13292 di Administration Server.

A seconda del metodo utilizzato per l'autenticazione, sono possibili due opzioni per la connessione dei dispositivi KES all'Administration Server:

- Connessione dei dispositivi con un certificato utente
- Connessione dei dispositivi senza un certificato utente

Connessione di un dispositivo con un certificato utente

Durante la connessione di un dispositivo con un certificato utente, il dispositivo viene associato all'account utente a cui è stato assegnato il certificato corrispondente tramite gli strumenti di Administration Server.

In questo caso verrà utilizzata l'autenticazione SSL bidirezionale (autenticazione reciproca). Sia l'Administration Server che il dispositivo verranno autenticati con certificati.

Connessione di un dispositivo senza un certificato utente

Durante la connessione di un dispositivo senza un certificato utente, il dispositivo non viene associato ad alcun account utente in Administration Server. Tuttavia, quando il dispositivo riceve un certificato, il dispositivo verrà associato all'utente a cui è stato assegnato il certificato corrispondente tramite gli strumenti di Administration Server.

Durante la connessione del dispositivo all'Administration Server, sarà applicata l'autenticazione SSL unidirezionale, il che significa che solo l'Administration Server viene autenticato con il certificato. Dopo il recupero del certificato utente da parte del dispositivo, il tipo di autenticazione diventerà autenticazione SSL bidirezionale (autenticazione SSL bidirezionale, autenticazione reciproca).

Schema per la connessione dei dispositivi KES al server tramite Kerberos Constrained Delegation (KCD)

Lo schema per la connessione dei dispositivi KES all'Administration Server tramite Kerberos Constrained Delegation (KCD) offre quanto segue:

- Integrazione con un proxy inverso che supporta KCD.
- Utilizzo di Kerberos Constrained Delegation (di seguito denominato KCD) per l'autenticazione dei dispositivi mobili.
- Integrazione con l'infrastruttura Public Key Infrastructure (di seguito denominata PKI) per l'applicazione dei certificati utente.

Quando si utilizza questo schema di connessione, tenere presente quanto segue:

- Il tipo di connessione dei dispositivi KES al proxy inverso deve essere l'autenticazione SSL bidirezionale: un dispositivo deve connettersi al proxy inverso tramite il relativo certificato utente proprietario. A tale scopo, è necessario integrare il certificato utente nel pacchetto di installazione di Kaspersky Endpoint Security for Android, che è stato installato nel dispositivo. Questo pacchetto KES deve essere creato dall'Administration Server specificamente per questo dispositivo (utente).

- È necessario specificare lo speciale certificato (personalizzato) invece del certificato server predefinito per il protocollo mobile:

  1. Nella finestra delle proprietà di Administration Server, nella sezione **Impostazioni**, selezionare la casella di controllo **Apri porta per i dispositivi mobili** e selezionare **Aggiungi certificato** nell'elenco a discesa.

  2. Nella finestra visualizzata specificare lo stesso certificato che è stato impostato nel proxy inverso al momento della pubblicazione del punto di accesso al protocollo mobile nell'Administration Server.

- I certificati utente per i dispositivi KES devono essere emessi dall'Autorità di certificazione (CA) del dominio. Tenere presente che se il dominio include più Autorità di certificazione radice, i certificati utente devono essere emessi dall'Autorità di certificazione che è stata impostata nella pubblicazione nel proxy inverso.

  È possibile garantire che il certificato utente sia conforme a tale requisito utilizzando uno dei seguenti metodi:

  - Specificare lo certificato utente speciale nella Creazione guidata nuovo pacchetto e nell'Installazione guidata certificato.

  - Integrare l'Administration Server con l'infrastruttura PKI del dominio e definire l'impostazione corrispondente nelle regole per l'emissione dei certificati:

    1. Nella struttura della console espandere la cartella **Mobile Device Management**, quindi selezionare la sottocartella **Certificati**.

    2. Nell'area di lavoro della cartella **Certificati** fare clic sul pulsante **Configura regole di emissione certificati** per aprire la finestra **Regole di emissione certificati**.

    3. Nella sezione **Integrazione con PKI** configurare l'integrazione con l'infrastruttura a chiave pubblica (PKI).

    4. Nella sezione **Emissione di certificati mobili** specificare l'origine dei certificati.

Di seguito è riportato un esempio di configurazione di Kerberos Constrained Delegation (KCD) con i seguenti presupposti:

- Il punto di accesso al protocollo mobile in Administration Server è impostato sulla porta 13292.

- Il nome del dispositivo con il proxy inverso è firewall.mydom.local.

- Il nome del dispositivo con Administration Server è ksc.mydom.local.

- Il nome della pubblicazione esterna del punto di accesso al protocollo mobile è kes4mob.mydom.global.

Account di dominio per Administration Server

È necessario creare un account di dominio (ad esempio, KSCMobileSrvcUsr) con cui verrà eseguito il servizio Administration Server. È possibile specificare un account per il servizio Administration Server al momento dell'installazione di Administration Server o tramite l'utilità klsrvswch. L'utilità klsrvswch è disponibile nella cartella di installazione di Administration Server. Il percorso di installazione predefinito: <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

È necessario specificare un account di dominio per i motivi seguenti:

- La funzionalità di gestione dei dispositivi KES è una parte integrante di Administration Server.
- Per garantire il corretto funzionamento di Kerberos Constrained Delegation (KCD), la parte ricevente (ovvero, Administration Server) deve essere in esecuzione con un account di dominio.

Nome dell'entità servizio per http/kes4mob.mydom.local

Nel dominio, con l'account KSCMobileSrvcUsr, aggiungere un SPN per pubblicare il servizio del protocollo mobile sulla porta 13292 del dispositivo con Administration Server. Per il dispositivo kes4mob.mydom.local con Administration Server, si presenta come segue:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Configurazione delle proprietà di dominio del dispositivo con il proxy inverso (firewall.mydom.local)

Per delegare il traffico, è necessario impostare come attendibile il dispositivo con il proxy inverso (firewall.mydom.local) per il servizio definito dall'SPN (http/kes4mob.mydom.local:13292).

Per impostare come attendibile il dispositivo con il proxy inverso per il servizio definito dall'SPN (http/kes4mob.mydom.local:13292), l'amministratore deve eseguire seguenti le operazioni:

1. Nello snap-in Microsoft Management Console "Utenti e computer di Active Directory" selezionare il dispositivo in cui è installato il proxy inverso (firewall.mydom.local).
2. Nelle proprietà del dispositivo, nella scheda **Delega**, impostare l'interruttore **Computer attendibile per la delega solo ai servizi specificati** su **Utilizza un qualsiasi protocollo di autenticazione**.
3. Nell'elenco **Servizi ai quali l'account può presentare credenziali delegate** aggiungere l'SPN http/kes4mob.mydom.local:13292.

Speciale certificato (personalizzato) per la pubblicazione (kes4mob.mydom.global)

Per pubblicare il protocollo mobile di Administration Server, è necessario emettere uno speciale certificato (personalizzato) per il nome FQDN kes4mob.mydom.global e specificarlo invece del certificato server predefinito nelle impostazioni del protocollo mobile di Administration Server in Administration Console. A tale scopo, nella finestra delle proprietà di Administration Server, nella sezione **Impostazioni**, selezionare la casella di controllo **Apri porta per i dispositivi mobili** e quindi selezionare **Aggiungi certificato** nell'elenco a discesa.

Il contenitore del certificato server (file con estensione p12 o pfx) deve anche contenere una catena di certificati radice (chiavi pubbliche).

Configurazione della pubblicazione nel proxy inverso

Nel proxy inverso, per il traffico dal dispositivo mobile alla porta 13292 kes4mob.mydom.global, è necessario configurare KCD sull'SPN (http/kes4mob.mydom.local:13292) utilizzando il certificato server emesso per il nome FQDN kes4mob.mydom.global. La pubblicazione e il punto di accesso pubblicato (la porta 13292 di Administration Server) devono condividere lo stesso certificato server.

Utilizzo di Firebase Cloud Messaging

Per garantire l'invio tempestivo dei comandi ai dispositivi KES gestiti dal sistema operativo Android, Kaspersky Security Center usa il meccanismo delle notifiche push. Le notifiche push vengono scambiate tra i dispositivi KES e Administration Server tramite Firebase Cloud Messaging (di seguito FCM). In Kaspersky Security Center Administration Console è possibile specificare le impostazioni di Cloud Firebase Messaging per la connessione dei dispositivi KES al servizio.

Per recuperare le impostazioni di Firebase Cloud Messaging, è necessario disporre di un account Google.

Per abilitare l'utilizzo di FCM:

1. In Administration Console selezionare il nodo **Mobile Device Management** e la cartella **Dispositivi mobili**.
2. Dal menu di scelta rapida della cartella **Dispositivi mobili** selezionare **Proprietà**.
3. Nelle proprietà della cartella selezionare la sezione **Impostazioni di Firebase Cloud Messaging**.
4. Nel campo **Numero progetto Firebase**, specificare l'ID del mittente FCM.
5. Nel campo **File della chiave privata (in formato JSON)**, selezionare il file della chiave privata.

   Alla successiva sincronizzazione con Administration Server, i dispositivi KES gestiti da sistemi operativi Android verranno connessi a Firebase Cloud Messaging.

È possibile modificare le impostazioni di Firebase Cloud Messaging facendo clic sul pulsante **Ripristina impostazioni**.

Quando si passa a un progetto Firebase diverso, è necessario attendere 10 minuti per il ripristino di FCM.

Il servizio FCM viene eseguito nei seguenti intervalli di indirizzi:

- Sul lato del dispositivo KES, è necessario l'accesso alle porte 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) e 5230 (HTTPS) dei seguenti indirizzi:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Tutti gli indirizzi IP elencati nell'ASN Google numero 15169
- Sul lato dell'Administration Server, è necessario l'accesso alla porta 443 (HTTPS) dei seguenti indirizzi:
  - fcm.googleapis.com
  - Tutti gli indirizzi IP elencati nell'ASN Google numero 15169

Se le impostazioni del server proxy (**Avanzate** / **Configurazione dell'accesso a Internet**) sono state specificate nelle proprietà di Administration Server in Administration Console, saranno utilizzate per l'interazione con FCM.

Configurazione di FCM: ottenere l'ID del mittente e il file della chiave privata

Per configurare il FCM:

1. Eseguire la registrazione nel portale Google.
2. Passare alla console Firebase.
3. Eseguire una delle seguenti operazioni:
   - Per creare un nuovo progetto, fare clic su **Crea un progetto** e seguire le istruzioni sullo schermo.
   - Aprire un progetto esistente.
4. Fare clic sull'icona a forma di ingranaggio e selezionare **Impostazioni progetto**.

   Verrà visualizzata la **finestra Impostazioni progetto**.
5. Selezionare la scheda **Cloud Messaging**.
6. Recuperare l'ID del mittente pertinente dal campo **ID mittente** nella sezione **Firebase Cloud Messaging API (V1)**.
7. Selezionare la scheda **Account di servizio** e fare clic su **Genera nuova chiave privata**.
8. Nella finestra visualizzata, fare clic su **Genera chiave** per generare e scaricare un file di chiave privata.

Firebase Cloud Messaging è ora configurato.

Integrazione con PKI (Public Key Infrastructure)

L'integrazione con l'infrastruttura Public Key Infrastructure (di seguito denominata PKI) ha principalmente l'obiettivo di semplificare l'emissione dei certificati utente di dominio da parte di Administration Server.

L'amministratore può assegnare un certificato di dominio per un utente in Administration Console. A tale scopo, è possibile utilizzare uno dei seguenti metodi:

- Assegnare all'utente uno speciale certificato (personalizzato) da un file nell'Installazione guidata certificato.
- Eseguire l'integrazione con PKI e assegnare a PKI il ruolo di origine dei certificati per un tipo specifico di certificati o per tutti i tipi di certificati.

Le impostazioni dell'integrazione con PKI sono disponibili nell'area di lavoro della cartella **Mobile Device Management** / **Certificati** facendo clic sul collegamento **Integra con infrastruttura a chiave pubblica (PKI)**.

Principio generale di integrazione con PKI per l'emissione dei certificati utente di dominio

In Administration Console fare clic sul collegamento **Integra con infrastruttura a chiave pubblica (PKI)** nell'area di lavoro della cartella **Mobile Device Management** / **Certificati** per specificare un account di dominio che sarà utilizzato da Administration Server per emettere i certificati utente di dominio tramite l'Autorità di certificazione del dominio (di seguito denominato account utilizzato per l'integrazione con PKI).

Tenere presente quanto segue:

- Le impostazioni di integrazione con PKI offrono la possibilità di specificare il modello predefinito per tutti i tipi di certificati. Le regole per l'emissione dei certificati (disponibili nell'area di lavoro della cartella **Mobile Device Management** / **Certificati** facendo clic sul pulsante **Configura regole di emissione certificati**) consentono di specificare un singolo modello per ogni tipo di certificati.
- Un speciale certificato Enrollment Agent (EA) deve essere installato nel dispositivo con Administration Server, nell'archivio di certificati dell'account utilizzato per l'integrazione con PKI. Il certificato Enrollment Agent (EA) viene emesso dall'amministratore dell'Autorità di certificazione del dominio.

L'account utilizzato per l'integrazione con PKI deve soddisfare i seguenti criteri:

- È un utente di dominio.
- È un amministratore locale del dispositivo con Administration Server da cui viene avviata l'integrazione con PKI.
- Ha il diritto di *accesso come servizio*.
- Il dispositivo in cui è installato Administration Server deve essere in esecuzione almeno una volta con questo account per creare un profilo utente permanente.

Server Web di Kaspersky Security Center

Il Server Web di Kaspersky Security Center (di seguito denominato server Web) è un componente di Kaspersky Security Center. Il server Web è progettato per la pubblicazione di pacchetti di installazione indipendenti, pacchetti di installazione indipendenti per dispositivi mobili, profili MDM iOS e file da una cartella condivisa.

I profili MDM iOS e i pacchetti di installazione creati vengono pubblicati automaticamente sul server Web e sono rimossi dopo il primo download. L'amministratore può inviare il nuovo collegamento all'utente con qualsiasi sistema (ad esempio, tramite e-mail).

Facendo clic su questo collegamento, l'utente può scaricare le informazioni richieste in un dispositivo mobile.

Impostazioni del server Web

Se è necessario modificare la configurazione del server Web, le proprietà del server Web di Administration Console offrono la possibilità di modificare le porte per HTTP (8060) e HTTPS (8061). Oltre a modificare le porte, è possibile sostituire il certificato server per HTTPS e modificare il nome FQDN del server Web per HTTP.

Installazione di Kaspersky Security Center

In questa sezione viene descritta l'installazione dei componenti di Kaspersky Security Center. Se si desidera installare l'applicazione in locale in un solo dispositivo, sono disponibili due opzioni di installazione:

- **Standard**. L'opzione è consigliabile se si desidera provare a utilizzare Kaspersky Security Center, ad esempio verificandone il funzionamento in un'area delimitata all'interno della rete aziendale. Durante l'installazione standard, è possibile esclusivamente configurare il database. È inoltre possibile installare solo il set predefinito di plug-in di gestione delle applicazioni Kaspersky. È inoltre possibile utilizzare l'installazione standard se si dispone già di una certa esperienza nell'utilizzo di Kaspersky Security Center in modo da poter specificare tutte le impostazioni pertinenti dopo l'installazione standard.

- **Personalizzato**. L'opzione è consigliabile se si intende modificare le impostazioni di Kaspersky Security Center, ad esempio il percorso della cartella condivisa, gli account e le porte per la connessione ad Administration Server, nonché le impostazioni del database. L'installazione personalizzata consente di specificare quali plug-in di gestione di Kaspersky installare. Se necessario, è possibile avviare l'installazione personalizzata in modalità automatica.

Se almeno un Administration Server è installato nella rete, i server possono essere installati in altri dispositivi in remoto tramite l'attività di installazione remota utilizzando l'installazione forzata. Quando si crea l'attività di installazione remota, è necessario utilizzare il pacchetto di installazione di Administration Server: ksc_<numero_versione> .<numero build> _full_<lingua localizzazione> .exe.

Utilizzare questo pacchetto se si desidera installare tutti i componenti richiesti per usufruire delle funzionalità complete di Kaspersky Security Center o per eseguire l'upgrade delle versioni correnti dei componenti.

Se si desidera distribuire il cluster di failover Kaspersky Security Center, è necessario installare Kaspersky Security Center in tutti i nodi del cluster.

Preparazione dell'installazione

Eseguire le seguenti azioni prima di avviare l'installazione.

- **Verificare i requisiti hardware e software**

  Verificare che l'hardware e il software del dispositivo soddisfino i requisiti di Administration Server e Administration Console.

- **Selezione e installazione del sistema di gestione database (DBMS)**

  Kaspersky Security Center archivia le informazioni in un database gestito da un DBMS. Installare il DBMS nella rete prima di Kaspersky Security Center (ulteriori informazioni su come selezionare un DBMS). Se si decide di installare il DBMS di PostgreSQL o Postgres Pro, specificare una password per l'utente con privilegi avanzati. Se la password non viene specificata, Administration Server potrebbe non essere in grado di connettersi al database.

  È consigliabile installare Administration Server in un server dedicato anziché in un controller di dominio. Se tuttavia si installa Kaspersky Security Center in un server che opera come controller di dominio di sola lettura (RODC), Microsoft SQL Server (SQL Express) non deve essere installato in locale (nello stesso dispositivo). In questo caso, è consigliabile installare Microsoft SQL Server (SQL Express) in remoto (su un altro dispositivo) o utilizzare MySQL, MariaDB o PostgreSQL se è necessario installare il DBMS in locale.

- **Preparare le cartelle per Administration Server, Network Agent e Administration Console**

  Administration Server, Network Agent e Administration Console devono essere installati nelle cartelle in cui la distinzione tra maiuscole e minuscole è disabilitata. La distinzione tra maiuscole e minuscole deve inoltre essere disabilitata per la cartella condivisa di Administration Server e la cartella nascosta di Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

- **Rimuovere Network Agent precedente**

  La versione server di Network Agent è installata nel dispositivo insieme ad Administration Server. Non è possibile installare Administration Server con la versione standard di Network Agent. Se la versione server di Network Agent è già installata nel dispositivo, rimuoverla e riavviare l'installazione di Administration Server. Per dettagli sulla versione server di Network Agent, fare riferimento a Modifiche apportate al sistema dopo l'installazione di Kaspersky Security Center.

- **Controllo degli account**

  L'installazione di Kaspersky Security Center richiede diritti di amministratore nel dispositivo in cui deve essere eseguita l'installazione.

  Kaspersky Security Center supporta gli account del servizio gestito e gli account del servizio gestito di gruppo. Se questi tipi di account vengono utilizzati nel dominio e si desidera specificarne uno come account per il servizio Administration Server, installare prima l'account nello stesso dispositivo in cui si desidera installare Administration Server. Per informazioni dettagliate sull'installazione degli account del servizio gestito in un dispositivo locale, consultare la documentazione ufficiale di Microsoft.

Account per l'utilizzo del DBMS

Per installare e utilizzare Administration Server, è necessario un account Windows con cui eseguire il programma di installazione di Administration Server (di seguito denominato anche programma di installazione), un account Windows con cui avviare il servizio Administration Server e un account DBMS interno per accedere al DBMS. È possibile creare nuovi account o utilizzare quelli esistenti. Tutti questi account richiedono diritti specifici. Un insieme degli account richiesti e dei relativi diritti dipende dai seguenti criteri:

- Tipo di DBMS:
  - Microsoft SQL Server (con autenticazione di Windows o con autenticazione di SQL Server)
  - MySQL o MariaDB
  - PostgreSQL o Postgres Pro
- Posizione del DBMS:
  - **DBMS locale**. Il *DBMS locale* è un DBMS installato nello stesso dispositivo di Administration Server.
  - **DBMS remoto**. Il *DBMS remoto* è un DBMS installato in un altro dispositivo.
- Metodo di creazione del database di Administration Server:
  - **Automatico**. Durante l'installazione di Administration Server, è possibile creare automaticamente un database di Administration Server (di seguito denominato anche database del server) utilizzando il programma di installazione.
  - **Manuale**. È possibile utilizzare un'applicazione di terzi (ad esempio, SQL Server Management Studio) o uno script per creare un database vuoto. Successivamente, è possibile specificare questo database come database del server durante l'installazione di Administration Server.

Seguire il principio del privilegio minimo quando si concedono diritti e autorizzazioni agli account. Ciò significa che i diritti concessi devono essere sufficienti solo per eseguire le azioni richieste.

Le tabelle seguenti contengono informazioni sui diritti di sistema e sui diritti del DBMS che è necessario concedere agli account prima di installare e avviare Administration Server.

Microsoft SQL Server con autenticazione di Windows

Se si sceglie SQL Server come DBMS, è possibile utilizzare l'autenticazione di Windows per accedere a SQL Server. Configurare i diritti di sistema per un account Windows utilizzato per eseguire il programma di installazione e un account Windows utilizzato per avviare il servizio Administration Server. In SQL Server, creare credenziali di accesso per entrambi gli account Windows. A seconda del metodo di creazione del database del server, concedere i diritti di SQL Server richiesti a tali account come descritto nella tabella seguente. Per ulteriori informazioni su come configurare i diritti degli account, consultare Configurazione degli account per l'utilizzo di SQL Server (autenticazione di Windows).

DBMS: Microsoft SQL Server (tra cui Express Edition) con autenticazione Windows

	Creazione automatica del database (con il programma di installazione)	Creazione manuale del database (da parte dell'amministratore)
Account con cui viene eseguito il programma di installazione	• DBMS remoto: solo un account di dominio del dispositivo remoto in cui è installato il DBMS. • DBMS locale: un account amministratore locale o un account di dominio.	• DBMS remoto: solo un account di dominio del dispositivo remoto in cui è installato il DBMS. • DBMS locale: un account amministratore locale o un account di dominio.

Diritti dell'account con cui viene eseguito il programma di installazione	• Diritti di sistema: diritti di amministratore locale.
	• Diritti di SQL Server:
	  • Ruolo a livello di server: sysadmin.
		• Diritti di sistema: diritti di amministratore locale.
		• Diritti di SQL Server:
		  • ruolo a livello di server: pubblico.
		  • Appartenenza al ruolo del database per il database del server: db_owner, public.
		  • Schema predefinito per il database del server: dbo.

Account del servizio di Administration Server	• DBMS remoto: solo un account di dominio del dispositivo remoto in cui è installato il DBMS.
	• DBMS locale:
	  • Un account Windows scelto dall'amministratore.
	  • Un account nel formato KL-AK-* creato automaticamente dal programma di installazione.
		• DBMS remoto: solo un account di dominio del dispositivo remoto in cui è installato il DBMS.
		• DBMS locale:
		  • Un account Windows scelto dall'amministratore.
		  • Un account nel formato KL-AK-* creato automaticamente dal programma di installazione (in questo caso, si sconsiglia di generare un account KL-AK-*).

Diritti dell'account del servizio di Administration Server	• Diritti di sistema: diritti richiesti assegnati dal programma di installazione
	• Diritti di SQL Server: diritti richiesti assegnati dal programma di installazione
		• Diritti di sistema: diritti richiesti assegnati dal programma di installazione
		• Diritti di SQL Server:
		  • ruolo a livello di server: pubblico.
		  • Appartenenza al ruolo del database per il database del server: db_owner, public.
		  • Schema predefinito per il database del server: dbo.

Microsoft SQL Server con autenticazione di SQL Server

Se si sceglie SQL Server come DBMS, è possibile utilizzare l'autenticazione di SQL Server per accedere a SQL Server. Configurare i diritti di sistema per un account Windows utilizzato per eseguire il programma di installazione e per un account Windows utilizzato per avviare il servizio Administration Server. In SQL Server, creare un account di accesso con una password da utilizzare per l'autenticazione. Quindi, concedere a questo account SQL Server i diritti richiesti elencati nella tabella seguente. Per ulteriori informazioni su come configurare i diritti degli account, consultare Configurazione degli account per l'utilizzo di SQL Server (autenticazione di SQL Server).

DBMS: Microsoft SQL Server (tra cui Express Edition) con autenticazione di SQL Server

	Creazione automatica del database (con il programma di installazione)	Creazione manuale del database (da parte dell'amministratore)
Account con cui viene eseguito il programma di installazione	• DBMS remoto: solo un account di dominio del dispositivo remoto in cui è installato il DBMS. • DBMS locale: un account amministratore locale o un account di dominio.	• DBMS remoto: solo un account di dominio del dispositivo remoto in cui è installato il DBMS. • DBMS locale: un account amministratore locale o un account di dominio.
Diritti dell'account con cui viene eseguito il programma di installazione	Diritti di sistema: diritti di amministratore locale.	Diritti di sistema: diritti di amministratore locale.

	Creazione automatica del database (con il programma di installazione)	Creazione manuale del database (da parte dell'amministratore)

Account del servizio di Administration Server	• DBMS remoto: solo un account di dominio del dispositivo remoto in cui è installato il DBMS.
	• DBMS locale:
	  • Un account Windows scelto dall'amministratore.
	  • Un account nel formato KL-AK-* creato automaticamente dal programma di installazione.
		• DBMS remoto: solo un account di dominio del dispositivo remoto in cui è installato il DBMS.
		• DBMS locale:
		  • Un account utente di Windows scelto dall'amministratore.
		  • Un account nel formato KL-AK-* creato automaticamente dal programma di installazione.

Diritti dell'account del servizio di Administration Server	Diritti di sistema: diritti richiesti assegnati dal programma di installazione	Diritti di sistema: diritti richiesti assegnati dal programma di installazione

Diritti dell'account di accesso utilizzato per l'autenticazione di SQL Server	Diritti di SQL Server richiesti per creare un database e installare Administration Server:
	• ruolo a livello di server: pubblico.
	• Appartenenza al ruolo del database per il database *master*: db_owner.
	• - Schema predefinito per il database *master*: dbo.
	• Autorizzazioni:
	  • CONNECT ANY DATABASE
	  • CONNECT SQL
	  • CREATE ANY DATABASE
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE (se l'opzione **Always On** è abilitata)
	Diritti di SQL Server necessari per utilizzare Administration Server:
	• ruolo a livello di server: pubblico.
	• Appartenenza al ruolo del database per il database del server: db_owner.
	• Schema predefinito per il database del server: dbo.
	• Autorizzazioni:
	  • CONNECT SQL
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE (se l'opzione **Always On** è abilitata)
	  • VIEW ANY DEFINITION
		Diritti di SQL Server:
		• ruolo a livello di server: pubblico.
		• Appartenenza al ruolo del database per il database del server: db_owner.
		• Schema predefinito per il database del server: dbo.
		• Autorizzazioni:
		  • CONNECT SQL
		  • VIEW ANY DATABASE
		  • VIEW ANY DEFINITION

Configurazione dei diritti di SQL Server per il ripristino dei dati di Administration Server

Per ripristinare i dati di Administration Server dal backup, eseguire l'utilità klbackup con l'account Windows utilizzato per installare Administration Server. Prima di avviare l'utilità klbackup, in SQL Server concedere i diritti alle credenziali di accesso di SQL Server associate a questo account Windows. I diritti di SQL Server variano a seconda della versione di Administration Server. Per Administration Server versione 14.2 o successiva, è possibile concedere il ruolo a livello di server sysadmin o il ruolo a livello di server dbcreator.

Diritti di SQL Server per il ripristino del database di Administration Server

Administration Server versione 14.2 o successiva	Altre versioni di Administration Server

• Diritti di SQL Server:
  • Ruolo a livello di server: dbcreator.
• Autorizzazioni:
  • VIEW ANY DEFINITION
Prima di avviare l'utilità klbackup, specificare il contrassegno del server KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center. Successivamente, eseguire il comando seguente nella riga di comando:
`klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL e MariaDB

Se si sceglie MySQL o MariaDB come DBMS, creare un account DBMS interno e concedere a questo account i diritti richiesti elencati nella tabella seguente. Il programma di installazione e il servizio Administration Server utilizzano questo account DBMS interno per accedere al DBMS. Si noti che il metodo di creazione del database non influisce sull'insieme dei diritti richiesti. Per ulteriori informazioni su come configurare i diritti dell'account, consultare Configurazione degli account per l'utilizzo di MySQL e MariaDB.

DBMS: MySQL e MariaDB

	Creazione automatica o manuale del database
Account con cui viene eseguito il programma di installazione	• DBMS remoto: solo un account di dominio del dispositivo remoto con il DBMS installato. • DBMS locale: un account amministratore locale o un account di dominio.
Diritti dell'account con cui viene eseguito il programma di installazione	Diritti di sistema: diritti di amministratore locale.

Account del servizio di Administration Server	• DBMS remoto: solo un account di dominio del dispositivo remoto con il DBMS installato.
	• DBMS locale:
	  • Un account Windows scelto dall'amministratore.
	  • Un account nel formato KL-AK-* creato automaticamente dal programma di installazione.

Diritti dell'account del servizio di Administration Server	Diritti di sistema: diritti richiesti assegnati dal programma di installazione
Diritti dell'account interno DBMS	Privilegi dello schema: • Database di Administration Server: ALL (ad eseclusione di GRANT OPTION). • Schemi di sistema (mysql e sys): SELECT, SHOW VIEW. • La procedura memorizzata di sys.table_exists: EXECUTE (se si usa MariaDB 10.5 o versione precedente come DBMS, non è necessario concedere il privilegio EXECUTE). Privilegi globali per tutti gli schemi: PROCESS, SUPER.

Spostamento dei dati da un tablespace condiviso a una tablespace file per tabella nei DBMS MySQL e MariaDBPer informazioni dettagliate su come spostare i dati da un tablespace condiviso a un tablespace file per tabella, vedere Spostamento dei dati da un tablespace condiviso a una tablespace file per tabella nei DBMS MySQL e MariaDB.

Configurazione dei privilegi per il ripristino dei dati di Administration Server

I diritti concessi all'account DBMS interno sono sufficienti per ripristinare i dati di Administration Server dal backup. Per avviare il ripristino, eseguire l'utilità klbackup con l'account Windows utilizzato per installare Administration Server.

PostgreSQL o Postgres Pro

Se si sceglie PostgreSQL o Postgres Pro come DBMS, è possibile utilizzare l'utente *Postgres* (il ruolo Postgres predefinito) o creare un nuovo ruolo Postgres (di seguito denominato anche ruolo) per accedere al DBMS. A seconda del metodo di creazione del database del server, concedere i diritti richiesti al ruolo come descritto nella tabella seguente. Per ulteriori informazioni su come configurare i diritti del ruolo, consultare Configurazione degli account per l'utilizzo di PostgreSQL o Postgres Pro.

DBMS: PostgreSQL o Postgres Pro

	Creazione automatica del database		Creazione manuale del database
Account con cui viene eseguito il programma di installazione	• DBMS remoto: solo un account di dominio del dispositivo remoto con il DBMS installato. • DBMS locale: un account amministratore locale o un account di dominio.		• DBMS remoto: solo un account di dominio del dispositivo remoto con il DBMS installato. • DBMS locale: un account amministratore locale o un account di dominio.
Diritti dell'account con cui viene eseguito il programma di installazione	Diritti di sistema: diritti di amministratore locale.		Diritti di sistema: diritti di amministratore locale.

Account del servizio di Administration Server	• DBMS remoto: solo un account di dominio del dispositivo remoto con il DBMS installato.
	• DBMS locale:
	  • Un account Windows scelto dall'amministratore.
	  • Un account nel formato KL-AK-* creato automaticamente dal programma di installazione.
			• DBMS remoto: solo un account di dominio del dispositivo remoto con il DBMS installato.
			• DBMS locale:
			  • Un account Windows scelto dall'amministratore.
			  • Un account nel formato KL-AK-* creato automaticamente dal programma di installazione.

Diritti dell'account del servizio di Administration Server	Diritti di sistema: diritti richiesti assegnati dal programma di installazione		Diritti di sistema: diritti richiesti assegnati dal programma di installazione
Diritti del ruolo Postgres	L'utente *Postgres* non richiede diritti aggiuntivi.	Privilegi per un nuovo ruolo: `CREATEDB`.	Per un nuovo ruolo: • Privilegi sul database di Administration Server: `ALL`. • Privilegi su tutte le tabelle nello schema pubblico: `ALL`. • Privilegi su tutte le sequenze nello schema pubblico: `ALL`.

Configurazione dei privilegi per il ripristino dei dati di Administration Server

Per ripristinare i dati di Administration Server dal backup, eseguire l'utilità klbackup con l'account Windows utilizzato per installare Administration Server. Si noti che il ruolo Postgres utilizzato per accedere al DBMS deve disporre dei diritti di proprietario sul database di Administration Server.

Configurazione degli account per l'utilizzo di SQL Server (autenticazione di Windows)

Prerequisiti

Prima di assegnare i diritti agli account, eseguire le azioni seguenti:

1. Assicurarsi di accedere al sistema con l'account di amministratore locale.
2. Installare un ambiente per l'utilizzo di SQL Server.
3. Assicurarsi di disporre di un account Windows con cui installare Administration Server.
4. Assicurarsi di disporre di un account Windows con cui avviare il servizio Administration Server.
5. In SQL Server, creare un accesso per l'account Windows utilizzato per eseguire il programma di installazione di Administration Server (di seguito denominato anche programma di installazione). Creare anche un accesso per l'account Windows utilizzato per avviare il servizio Administration Server.

Se si utilizza SQL Server Management Studio, nella pagina **Generale** della finestra delle proprietà di accesso, selezionare l'opzione **Autenticazione Windows**.

Se si desidera installare Administration Server e SQL Server in dispositivi che si trovano in domini Windows separati, tenere presente che questi domini devono disporre di relazioni di attendibilità bidirezionali per assicurare il corretto funzionamento di Administration Server, inclusa l'esecuzione di attività e l'applicazione dei criteri. Per informazioni sugli account richiesti per le informazioni dei vari DBMS e sui diritti degli account, vedere Account per l'utilizzo del DBMS.

Configurazione degli account per l'installazione di Administration Server (creazione automatica del database di Administration Server)

Per configurare gli account per l'installazione di Administration Server:

1. In SQL Server, assegnare il ruolo a livello di server sysadmin all'accesso dell'account Windows utilizzato per eseguire il programma di installazione.
2. Accedere al sistema con l'account Windows utilizzato per eseguire il programma di installazione.
3. Eseguire il programma di installazione di Administration Server.

   Viene avviata l'installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.
4. Selezionare l'opzione dell'installazione personalizzata di Administration Server.
5. Selezionare Microsoft SQL Server come DBMS che archivia il database di Administration Server.

6. Selezionare la modalità di autenticazione di Microsoft Windows per stabilire una connessione tra Administration Server e SQL Server tramite un account Windows.

7. Specificare l'account Windows utilizzato per avviare il servizio Administration Server.

   È possibile selezionare l'account utente di Windows per il quale è stato creato in precedenza un accesso a SQL Server. In alternativa, è possibile creare automaticamente un nuovo account Windows nel formato KL-AK-* utilizzando il programma di installazione. In questo caso, il programma di installazione crea automaticamente un accesso a SQL Server per questo account. Indipendentemente dalla scelta dell'account, il programma di installazione assegna i diritti di sistema richiesti e i diritti di SQL Server all'account di servizio di Administration Server.

Al termine dell'installazione, viene creato il database del server e tutti i diritti di sistema richiesti e i diritti di SQL Server vengono assegnati all'account di servizio di Administration Server. Administration Server è pronto per l'uso.

Configurazione degli account per l'installazione di Administration Server (creazione manuale del database di Administration Server)

Per configurare gli account per l'installazione di Administration Server:

1. In SQL Server, creare un database vuoto. Questo database verrà utilizzato come database di Administration Server (di seguito denominato anche database del server).

2. Per entrambi gli accessi di SQL Server creati per gli account Windows, specificare il ruolo a livello di server pubblico, quindi configurare il mapping al database creato:

   - ruolo a livello di server: pubblico
   - Appartenenza al ruolo del database: db_owner, public
   - Schema predefinito: dbo

3. Accedere al sistema con l'account Windows utilizzato per eseguire il programma di installazione.

4. Eseguire il programma di installazione di Administration Server.

   Viene avviata l'installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

5. Selezionare l'opzione dell'installazione personalizzata di Administration Server.

6. Selezionare Microsoft SQL Server come DBMS che archivia il database di Administration Server.

7. Specificare il nome del database creato come nome del database di Administration Server.

8. Selezionare la modalità di autenticazione di Microsoft Windows per stabilire una connessione tra Administration Server e SQL Server tramite un account Windows.

9. Specificare l'account Windows utilizzato per avviare il servizio Administration Server.

   È possibile selezionare l'account utente di Windows per il quale è stato creato un accesso di SQL Server e sono stati precedentemente configurati i diritti di accesso.

Non è consigliabile creare automaticamente un nuovo account Windows nel formato KL-AK-*. In questo caso, il programma di installazione crea un nuovo account Windows per il quale non è stato creato e configurato un account SQL Server. Administration Server non può utilizzare questo account per avviare il servizio Administration Server. Se è necessario creare un account Windows KL-AK-*, non avviare Administration Console dopo l'installazione. Eseguire invece quanto segue:

1. Arrestare il servizio kladminserver.
2. In SQL Server, creare un accesso di SQL Server per l'account Windows KL-AK-* creato.
3. Concedere i diritti a questo accesso di SQL Server e configurare il mapping al database creato:
   - ruolo a livello di server: pubblico
   - Appartenenza al ruolo del database: db_owner, public
   - Schema predefinito: dbo
4. Riavviare il servizio kladminserver, quindi eseguire l'Administration Console.

Al termine dell'installazione, Administration Server utilizzerà il database creato per archiviare i dati del server. Administration Server è pronto per l'uso.

Configurazione degli account per l'utilizzo di SQL Server (autenticazione di SQL Server)

Prerequisiti

Prima di assegnare i diritti agli account, eseguire le azioni seguenti:

1. Assicurarsi di accedere al sistema con l'account di amministratore locale.
2. Installare un ambiente per l'utilizzo di SQL Server.
3. Assicurarsi di disporre di un account Windows con cui installare Administration Server.
4. Assicurarsi di disporre di un account Windows con cui avviare il servizio Administration Server.
5. In SQL Server, abilitare la modalità di autenticazione di SQL Server.

   Se si utilizza SQL Server Management Studio, nella finestra delle proprietà di SQL Server, nella pagina **Sicurezza**, selezionare l'opzione **Modalità di autenticazione di SQL Server e Windows**.
6. In SQL Server, creare un account di accesso con una password. Il programma di installazione di Administration Server (di seguito denominato anche programma di installazione) e il servizio Administration Server utilizzeranno questo account di SQL Server per accedere a SQL Server.

   Se si utilizza SQL Server Management Studio, nella pagina **Generale** della finestra delle proprietà di accesso, selezionare l'opzione **Autenticazione SQL Server**.

Se si desidera installare Administration Server e SQL Server in dispositivi che si trovano in domini Windows separati, tenere presente che questi domini devono disporre di relazioni di attendibilità bidirezionali per assicurare il corretto funzionamento di Administration Server, inclusa l'esecuzione di attività e l'applicazione dei criteri. Per informazioni sugli account richiesti per le informazioni dei vari DBMS e sui diritti degli account, vedere Account per l'utilizzo del DBMS.

Configurazione degli account per l'installazione di Administration Server (creazione automatica del database di Administration Server)

Per configurare gli account per l'installazione di Administration Server:

1. In SQL Server, mappare l'account SQL Server al database *master* predefinito. Il database *master* è un modello per il database di Administration Server (di seguito denominato anche database del server). Il database *master* viene utilizzato per la mappatura finché il programma di installazione non crea un database del server. Concedere i seguenti diritti e autorizzazioni all'account SQL Server:
   - ruolo a livello di server: pubblico
   - Appartenenza al ruolo del database per il database *master*: db_owner.
   - Schema predefinito per il database *master*: dbo.
   - Autorizzazioni:
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE
2. Accedere al sistema con l'account Windows utilizzato per eseguire il programma di installazione.
3. Eseguire il programma di installazione.

   Viene avviata l'installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.
4. Selezionare l'opzione dell'installazione personalizzata di Administration Server.
5. Selezionare Microsoft SQL Server come DBMS che archivia il database di Administration Server.
6. Specificare il nome del database di Administration Server.
7. Selezionare la modalità di autenticazione di SQL Server per stabilire una connessione tra Administration Server e SQL Server tramite l'account SQL Server creato. Quindi, specificare le credenziali dell'account SQL Server.
8. Specificare l'account Windows utilizzato per avviare il servizio Administration Server.

   È possibile selezionare un account utente Windows esistente o crearne uno nuovo nel formato KL-AK-* utilizzando il programma di installazione. Indipendentemente dall'account scelto, il programma di installazione assegna i diritti di sistema richiesti all'account di servizio di Administration Server.

Al termine dell'installazione, viene creato il database del server e tutti i diritti di sistema richiesti vengono assegnati all'account di servizio di Administration Server. Administration Server è pronto per l'uso.

È possibile annullare la mappatura al database *master*, poiché il programma di installazione ha creato un database del server e configurato il mapping a questo database durante l'installazione di Administration Server.

Poiché la creazione automatica del database richiede più autorizzazioni rispetto al normale utilizzo di Administration Server, è possibile revocare alcune autorizzazioni. In SQL Server, selezionare l'account SQL Server, quindi concedere i seguenti diritti per l'utilizzo Administration Server:

- ruolo a livello di server: pubblico
- Appartenenza al ruolo del database per il database del server: db_owner
- Schema predefinito per il database del server: dbo
- Autorizzazioni:
  - CONNECT SQL
  - VIEW ANY DATABASE

Configurazione degli account per l'installazione di Administration Server (creazione manuale del database di Administration Server)

Per configurare gli account per l'installazione di Administration Server:

1. In SQL Server, creare un database vuoto. Questo database verrà utilizzato come database di Administration Server.
2. In SQL Server, concedere i seguenti diritti e autorizzazioni all'account SQL Server:
   - ruolo a livello di server: pubblico.
   - Appartenenza al ruolo del database per il database creato: db_owner.
   - Schema predefinito per il database creato: dbo.
   - Autorizzazioni:
     - CONNECT SQL
     - VIEW ANY DATABASE
3. Accedere al sistema con l'account Windows utilizzato per eseguire il programma di installazione.
4. Eseguire il programma di installazione.

   Viene avviata l'installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.
5. Selezionare l'opzione dell'installazione personalizzata di Administration Server.
6. Selezionare Microsoft SQL Server come DBMS che archivia il database di Administration Server.
7. Specificare il nome del database creato come nome del database di Administration Server.
8. Selezionare la modalità di autenticazione di SQL Server per stabilire una connessione tra Administration Server e SQL Server tramite l'account SQL Server creato. Quindi, specificare le credenziali dell'account SQL Server.
9. Specificare l'account Windows utilizzato per avviare il servizio Administration Server.

   È possibile selezionare un account utente Windows esistente o crearne uno nuovo nel formato KL-AK-* utilizzando il programma di installazione. Indipendentemente dall'account scelto, il programma di installazione assegna i diritti di sistema richiesti all'account di servizio di Administration Server.

Al termine dell'installazione, Administration Server utilizzerà il database creato per archiviare i dati di Administration Server. Tutti i diritti di sistema richiesti vengono assegnati all'account di servizio di Administration Server. Administration Server è pronto per l'uso.

Configurazione degli account per l'utilizzo di MySQL e MariaDB

Prerequisiti

Prima di assegnare i diritti agli account, eseguire le azioni seguenti:

1. Assicurarsi di accedere al sistema con l'account di amministratore locale.
2. Installare un ambiente per l'utilizzo di MySQL o MariaDB.
3. Assicurarsi di disporre di un account Windows con cui installare Administration Server.
4. Assicurarsi di disporre di un account Windows con cui avviare il servizio Administration Server.

Configurazione degli account per l'installazione di Administration Server

Per configurare gli account per l'installazione di Administration Server:

1. Eseguire un ambiente per l'utilizzo di MySQL o MariaDB con l'account root creato durante l'installazione del DBMS.

2. Creare un account DBMS interno con una password. Il programma di installazione di Administration Server (di seguito denominato anche programma di installazione) e il servizio Administration Server utilizzeranno questo account DBMS interno per accedere al DBMS. Concedere i seguenti privilegi a questo account:

   - Privilegi dello schema:
     - Database di Administration Server: ALL (ad eseclusione di `GRANT OPTION`)
     - Schemi di sistema (mysql e sys): `SELECT`, `SHOW VIEW`
     - Procedura memorizzata di sys.table_exists: `EXECUTE`
   - Privilegi globali per tutti gli schemi: `PROCESS`, `SUPER`

   Per creare un account DBMS interno e concedere i privilegi richiesti a questo account, eseguire lo script seguente (in questo script, l'accesso al DBMS è *KCSAdmin* e il nome del database di Administration Server è *kav*):

```
/* Create a user named KSCAdmin */
CREATE USER 'KSCAdmin'
/* Specify a password for KSCAdmin */
IDENTIFIED BY '<password>';
```

   Se si utilizza MySQL 8.0 o versioni precedenti come DBMS, si noti che per queste versioni l'autenticazione "Caching SHA2 password" non è supportata. Modificare l'autenticazione predefinita da “Caching SHA2 password” a “MySQL native password”:

   - Per creare un account DBMS che utilizzi l'autenticazione "MySQL native password", eseguire il comando seguente:

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
     ```

   - Per modificare l'autenticazione per un account DBMS esistente, eseguire il comando seguente:

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<password>';
     ```

```
/* Grant privileges to KSCAdmin */
GRANT USAGE ON *.* TO 'KSCAdmin';
GRANT ALL ON kav.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON mysql.* TO 'KSCAdmin';
GRANT SELECT, SHOW VIEW ON sys.* TO 'KSCAdmin';
GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin';
GRANT PROCESS ON *.* TO 'KSCAdmin';
GRANT SUPER ON *.* TO 'KSCAdmin';
```

Se si usa MariaDB 10.5 o versione precedente come DBMS, non è necessario concedere il privilegio EXECUTE. In questo caso, escludere il seguente comando dallo script: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

3. Per visualizzare l'elenco dei privilegi concessi all'account DBMS, eseguire il seguente script:

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. Per creare manualmente un database di Administration Server, eseguire lo script seguente (in questo script, il nome del database di Administration Server è *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   Utilizzare lo stesso nome di database specificato nello script che crea l'account DBMS.

5. Accedere al sistema con l'account Windows utilizzato per eseguire il programma di installazione.

6. Eseguire il programma di installazione.

   Viene avviata l'installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

7. Selezionare l'opzione dell'installazione personalizzata di Administration Server.

8. Selezionare MySQL o MariaDB come DBMS che archivia il database di Administration Server.

9. Specificare il nome del database di Administration Server. Utilizzare lo stesso nome del database specificato nello script.

10. Specificare le credenziali dell'account DBMS creato dallo script.

11. Specificare l'account Windows utilizzato per avviare il servizio Administration Server.

    È possibile selezionare un account utente Windows esistente o crearne automaticamente uno nuovo nel formato KL-AK-* utilizzando il programma di installazione. Indipendentemente dall'account scelto, il programma di installazione assegna i diritti di sistema richiesti all'account di servizio di Administration Server.

Al termine dell'installazione, viene creato il database di Administration Server e Administration Server è pronto per l'uso.

Spostamento dei dati da un tablespace condiviso a un tablespace file per tabella in un DBMS MySQL e MariaDB

Per i DBMS MySQL e MariaDB, è possibile archiviare i dati nei seguenti modi:

- Come tablespace condiviso, quando i dati di tutti i database utente sono archiviati in un singolo file (in genere, nel file `ibdata1`).
- Come tablespace file per tabella, quando per ogni tabella viene creato uno spazio dati separato come file separato.

L'utilizzo di un tablespace condiviso aumenta il rischio di frammentazione del tablespace. Poiché non è possibile eseguire un'operazione `SHRINK`, un file in un tablespace condiviso potrebbe occupare circa il 90% dello spazio su disco. Ciò influisce negativamente sulle prestazioni del sottosistema del disco. Pertanto, è utile optare per un tablespace file per tabella.

Questo articolo descrive come spostare i dati da un tablespace condiviso a un tablespace file per tabella. Se i DBMS MySQL o MariaDB vengono utilizzati anche da altre applicazioni, è necessario spostare i database di queste applicazioni nel tablespace file per tabella.

> È consigliabile eseguire questa procedura solo se si utilizzano DBMS MySQL o MariaDB per Administration Server.
> Lo spostamento dei dati da un tablespace condiviso a un tablespace file per tabella può aumentare il carico sul sottosistema del disco.

Prerequisiti

Prima di iniziare, assicurarsi che:

- Sia stata creata una copia di backup dei dati di Administration Server eseguendo un'attività di backup dei dati o l'utilità klbackup.
- Sia stata creata una copia di backup di altre applicazioni i cui database sono gestiti dal DBMS MySQL o MariaDB (se presente).
- Nel dispositivo in cui è installato il DBMS, nella partizione con il database sia disponibile spazio su disco.

Lo spazio su disco richiesto corrisponde al 150% della dimensione totale corrente dei database (dimensione corrente del file `ibdata1`).

Processo

Per spostare i dati da un tablespace condiviso a un tablespace file per tabella:

1. Arrestare il servizio Kaspersky Security Center Administration Server e le altre applicazioni che utilizzano l'istanza del DBMS per cui si desidera eseguire questa procedura.

2. In base alla versione del DBMS, accedere al DBMS come utente con privilegi avanzati, quindi eseguire lo script `fix_tablespace.sql` in qualsiasi applicazione utile.

   È possibile visualizzare gli script `fix_tablespace.sql` facendo clic su questi collegamenti:

   Visualizzare lo script per MySQL 5.7 e MariaDB 10.1+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Visualizzare lo script per MySQL 8.0+

```
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
DELIMITER //
CREATE PROCEDURE `upgd_alter_all_tables_for_all_databases_to_innodb` ()
BEGIN
    DECLARE __st_FETCH_STATUS INT;
    DECLARE `schemaName` VARCHAR(192);
    DECLARE `tableName` VARCHAR(192);
    DECLARE `curIX` CURSOR FOR
    SELECT `TABLE_SCHEMA` , `TABLE_NAME`
    FROM information_schema.TABLES
    WHERE `TABLE_SCHEMA` NOT IN ('mysql', 'performance_schema', 'sys') AND TABLE_TYPE = 'BASE TABLE';
    DECLARE CONTINUE HANDLER FOR SQLSTATE '02000' SET __st_FETCH_STATUS = 1;

    OPEN `curIX`;
    SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    while1 : WHILE (0 = 0 AND __st_FETCH_STATUS = 0 ) DO
        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` ENGINE=''InnoDB'';'
);
        PREPARE stmt1 FROM @`strSQL`;
        EXECUTE stmt1;
        DEALLOCATE PREPARE stmt1;

        SET @`strSQL` = CONCAT( 'ALTER TABLE `' , `schemaName`, '`.`',`tableName`, '` TABLESPACE =
innodb_file_per_table;' );
        PREPARE stmt2 FROM @`strSQL`;
        EXECUTE stmt2;
        DEALLOCATE PREPARE stmt2;

        SET `__st_FETCH_STATUS` = 0; FETCH `curIX` INTO `schemaName`, `tableName`;
    END WHILE;
    CLOSE `curIX`;
END
//
DELIMITER ;
SET GLOBAL innodb_file_per_table = 1;
CALL upgd_alter_all_tables_for_all_databases_to_innodb();
DROP PROCEDURE IF EXISTS upgd_alter_all_tables_for_all_databases_to_innodb;
```

Non è necessario arrestare l'esecuzione dello script.
Se non si sono verificati errori del DBMS, ma l'esecuzione dello script è stata terminata, eseguire nuovamente lo script o interrompere l'esecuzione dei passaggi di questa procedura, riavviare il servizio DBMS e ripristinare i dati di Administration Server dal backup.

3. Nella sezione `[mysqld]` del file my.cnf, impostare il parametro `innodb_file_per_table` su `1`.

4. Riavviare il servizio MySQL o MariaDB.

5. Riavviare il servizio Kaspersky Security Center Administration Server.

I dati vengono spostati da un tablespace condiviso a un tablespace file per tabella.

Configurazione degli account per l'utilizzo di PostgreSQL e Postgres Pro

Prerequisiti

Prima di assegnare i diritti agli account, eseguire le azioni seguenti:

1. Assicurarsi di accedere al sistema con l'account di amministratore locale.
2. Installare un ambiente per l'utilizzo di PostgreSQL e Postgres Pro.
3. Configurare il server PostgreSQL o Postgres per l'utilizzo con Kaspersky Security Center 15.1.
4. Assicurarsi di disporre di un account Windows con cui installare Administration Server.
5. Assicurarsi di disporre di un account Windows con cui avviare il servizio Administration Server.

Configurazione degli account per l'installazione di Administration Server (creazione automatica del database di Administration Server)

Per configurare gli account per l'installazione di Administration Server:

1. Eseguire un ambiente per l'utilizzo di PostgreSQL e Postgres Pro.
2. Scegliere un ruolo di Postgres per accedere al DBMS. È possibile utilizzare uno dei seguenti ruoli:
   - L'utente *Postgres* (il ruolo predefinito di Postgres).

     Se si usa l'utente *Postgres*, non è necessario concedergli ulteriori diritti.
   - Un nuovo ruolo di Postgres.

     Se si desidera utilizzare un nuovo ruolo di Postgres, creare tale ruolo e concedergli il privilegio CREATEDB. A tale scopo, eseguire il seguente script (in questo script, il ruolo è *KCSAdmin*):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<password>' CREATEDB;
     ```

     Il ruolo creato verrà utilizzato come proprietario del database di Administration Server (di seguito denominato anche database del server).
3. Accedere al sistema con l'account Windows utilizzato per eseguire il programma di installazione di Administration Server (di seguito denominato anche programma di installazione).
4. Eseguire il programma di installazione.

   Viene avviata l'installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.
5. Selezionare l'opzione dell'installazione personalizzata di Administration Server.
6. Selezionare PostgreSQL o Postgres Pro come DBMS che archivia il database di Administration Server.
7. Specificare il nome del database del server. Il programma di installazione creerà automaticamente il database del server.

8. Specificare le credenziali del ruolo di Postgres.

9. Specificare l'account Windows utilizzato per avviare il servizio Administration Server.

   È possibile selezionare un account utente Windows esistente o crearne automaticamente uno nuovo nel formato KL-AK-* utilizzando il programma di installazione. Indipendentemente dall'account scelto, il programma di installazione assegna i diritti di sistema richiesti all'account di servizio di Administration Server.

Al termine dell'installazione, il database del server viene creato automaticamente e Administration Server è pronto per l'uso.

Configurazione degli account per l'installazione di Administration Server (creazione manuale del database di Administration Server)

Per configurare gli account per l'installazione di Administration Server:

1. Eseguire un ambiente per l'utilizzo di Postgres.

2. Accedere come utente *Postgres* nel database *Postgres*.

3. Creare un nuovo ruolo Postgres (in questo esempio il ruolo è *KSCAdmin*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '< password >';
   ```

4. Creare un database di Administration Server (in questo *esempio* il nome del database di Administration Server è *KAV*):

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   > Se si verifica l'errore "La nuova codifica (UTF8) non è compatibile con la codifica del database modello", creare un database utilizzando il comando:
   > `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
   > anziché:
   > `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

5. Concedere tutti i privilegi al ruolo nel database di Administration Server.

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   > Verificare che il ruolo disponga dei privilegi CONNECT e TEMPORARY predefiniti nel database di Administration Server.

6. Concedere i seguenti privilegi al ruolo di Postgres creato:

   - Privilegi su tutte le tabelle nello schema pubblico: ALL
   - Privilegi su tutte le sequenze nello schema pubblico: ALL

   A tale scopo, accedere come utente *Postgres* al database del server ed eseguire il seguente script (in questo script, il ruolo è *KCSAdmin*):

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

7. Accedere al sistema con l'account Windows utilizzato per eseguire il programma di installazione.

8. Eseguire il programma di installazione di Administration Server.

   Viene avviata l'installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

9. Selezionare l'opzione dell'installazione personalizzata di Administration Server.

10. Selezionare PostgreSQL o Postgres Pro come DBMS che archivia il database di Administration Server.

11. Specificare il nome del database del server. Utilizzare lo stesso nome del database specificato nello script. Si noti che nel nome del database viene operata la distinzione tra maiuscole e minuscole.

12. Specificare le credenziali del ruolo di Postgres.

13. Specificare l'account Windows utilizzato per avviare il servizio Administration Server.

    È possibile selezionare un account utente Windows esistente o crearne automaticamente uno nuovo nel formato KL-AK-* utilizzando il programma di installazione. Indipendentemente dall'account scelto, il programma di installazione assegna i diritti di sistema richiesti all'account di servizio di Administration Server.

Al termine dell'installazione, Administration Server utilizzerà il database creato per archiviare i dati di Administration Server. Administration Server è pronto per l'uso.

Scenario: Autenticazione di Microsoft SQL Server

Le informazioni contenute in questa sezione sono applicabili solo alle configurazioni in cui Kaspersky Security Center utilizza Microsoft SQL Server come sistema di gestione database.

Per proteggere i dati Kaspersky Security Center trasferiti da o verso il database e i dati archiviati nel database da accessi non autorizzati, è necessario proteggere le comunicazioni tra Kaspersky Security Center e SQL Server. Il modo più affidabile per garantire comunicazioni sicure è installare Kaspersky Security Center e SQL Server nello stesso dispositivo e utilizzare il meccanismo di memoria condivisa per entrambe le applicazioni. In tutti gli altri casi, è consigliabile utilizzare un certificato SSL o TLS per autenticare l'istanza di SQL Server. È possibile utilizzare un certificato di un'autorità di certificazione attendibile o un certificato autofirmato. È consigliabile utilizzare un certificato di un'autorità di certificazione attendibile perché un certificato autofirmato garantisce solo una protezione limitata.

L'autenticazione di SQL Server procede per fasi:

1. **Generazione di un certificato SSL o TLS autofirmato per SQL Server in base ai requisiti del certificato**

   Se si dispone già di un certificato per SQL Server, saltare questo passaggio.

   Un certificato SSL è applicabile solo alle versioni di SQL Server precedenti al 2016 (13.x). In SQL Server 2016 (13.x) e versioni successive, utilizzare un certificato TLS.

   Ad esempio, per generare un certificato TLS immettere il comando seguente in PowerShell:

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

   Nel comando, anziché SQL_HOST_NAME è necessario digitare il nome host di SQL Server se l'host è incluso nel dominio o digitare il *nome di dominio completo* dell'host se l'host non è incluso nel dominio. Lo stesso nome, nome host o nome di dominio completo, deve essere specificato come nome di istanza di SQL nell'Installazione guidata di Administration Server.

2. **Aggiunta del certificato nell'istanza SQL Server**

   Le istruzioni per questo passaggio dipendono dalla piattaforma in cui è in esecuzione SQL Server. Fare riferimento alla documentazione ufficiale per ulteriori dettagli:

   - Windows
   - Linux
   - Servizio di database relazionale Amazon
   - Windows Azure

   Per utilizzare il certificato in un cluster di failover, è necessario installare il certificato in ciascun nodo del cluster di failover. Per i dettagli, consultare la documentazione Microsoft.

3. **Assegnazione delle autorizzazioni dell'account del servizio**

   Assicurarsi che l'account del servizio con cui viene eseguito il servizio SQL Server disponga dell'autorizzazione di controllo completo per accedere alle chiavi private. Per i dettagli, consultare la documentazione Microsoft.

4. **Aggiunta del certificato all'elenco dei certificati attendibili per Kaspersky Security Center**

   Nel dispositivo Administration Server aggiungere il certificato all'elenco dei certificati attendibili. Per i dettagli, consultare la documentazione Microsoft.

5. **Abilitazione delle connessioni criptate tra l'istanza di SQL Server e Kaspersky Security Center**

   Nel dispositivo Administration Server impostare il valore `1` per la variabile di ambiente `KLDBADO_UseEncryption`. Ad esempio, in Windows Server 2012 R2 è possibile modificare le variabili di ambiente facendo clic su **Variabili di ambiente** nella scheda **Avanzate** della finestra **Proprietà di sistema**. Aggiungere una nuova variabile, denominarla `KLDBADO_UseEncryption`, quindi impostare il valore `1`.

6. **Configurazione aggiuntiva per l'utilizzo del protocollo TLS 1.2**

   Se si utilizza il protocollo TLS 1.2, eseguire anche le seguenti operazioni:

   - Assicurarsi che la versione installata di SQL Server sia un'applicazione a 64 bit.
   - Installare il driver Microsoft OLE DB nel dispositivo Administration Server. Per i dettagli, consultare la documentazione Microsoft.
   - Nel dispositivo Administration Server impostare il valore `1` per la variabile di ambiente `KLDBADO_UseMSOLEDBSQL`. Ad esempio, in Windows Server 2012 R2 è possibile modificare le variabili di ambiente facendo clic su **Variabili di ambiente** nella scheda **Avanzate** della finestra **Proprietà di sistema**. Aggiungere una nuova variabile, denominarla `KLDBADO_UseMSOLEDBSQL`, quindi impostare il valore `1`.

     Se la versione del driver OLE DB è 19 o successiva, impostare anche il valore `MSOLEDBSQL19` sulla variabile di ambiente `KLDBADO_ProviderName`.

7. **Abilitazione dell'utilizzo del protocollo TCP/IP in un'istanza denominata di SQL Server**

   Se si utilizza un'istanza denominata di SQL Server, abilitare inoltre l'utilizzo del protocollo TCP/IP e assegnare un numero di porta TCP/IP al motore del database di SQL Server. Quando si configura la connessione SQL Server nell'Installazione guidata di Administration Server, specificare il nome host di SQL Server e il numero di porta nel campo **Nome istanza SQL Server**.

Scenario: autenticazione di MySQL Server

Si consiglia di utilizzare un certificato TLS per autenticare MySQL Server. È possibile utilizzare un certificato di un'autorità di certificazione attendibile o un certificato autofirmato.

Administration Server supporta l'autenticazione SSL unidirezionale e bidirezionale per MySQL.

Abilitazione dell'autenticazione SSL unidirezionale

Seguire questi passaggi per configurare l'autenticazione SSL unidirezionale per MySQL:

1. **Generare un certificato TLS autofirmato per il server MySQL**

   In PowerShell, cambiare directory nella cartella in cui si desidera archiviare i certificati. Eseguire i seguenti comandi:

```
$CertCA = New-SelfSignedCertificate `
-Subject "CN=CertCA" `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-NotAfter (Get-Date).AddDays(365)

$CertCABase64 = [System.Convert]::ToBase64String($CertCA.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeaf = New-SelfSignedCertificate `
-Subject "CN=CertLeaf" `
-Signer $CertCA `
-CertStoreLocation "Cert:\CurrentUser\My" `
-HashAlgorithm "SHA256" `
-KeyExportPolicy Exportable `
-NotAfter (Get-Date).AddDays(365)

$CertLeafBase64 = [System.Convert]::ToBase64String($CertLeaf.RawData,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertLeafRSACng =
[System.Security.Cryptography.X509Certificates.RSACertificateExtensions]::GetRSAPrivateKey($CertLeaf)
$CertLeafKeyBytes =
$CertLeafRSACng.Key.Export([System.Security.Cryptography.CngKeyBlobFormat]::Pkcs8PrivateBlob)
$CertLeafKeyBase64 = [System.Convert]::ToBase64String($CertLeafKeyBytes,
[System.Base64FormattingOptions]::InsertLineBreaks)

$CertCAPemCert = @"
-----BEGIN CERTIFICATE-----
$CertCABase64
-----END CERTIFICATE-----
"@

$CertLeafPemKey = @"
-----BEGIN PRIVATE KEY-----
$CertLeafKeyBase64
-----END PRIVATE KEY-----
"@

$CertLeafPemCert = @"
-----BEGIN CERTIFICATE-----
$CertLeafBase64
-----END CERTIFICATE-----
"@

# Output to file

$CertCAPemCert | Out-File -FilePath ca-cert.pem -Encoding Ascii

$CertLeafPemKey | Out-File -FilePath server-key.pem -Encoding Ascii
$CertLeafPemCert | Out-File -FilePath server-cert.pem -Encoding Ascii
```

Questi comandi creano i certificati per l'utente corrente ed esportano i certificati nel formato PEM. Per autenticare il server sono necessari solo i file PEM esportati. Per rimuovere i certificati creati da Windows, eseguire il seguente comando in PowerShell:

```
certmgr.msc
```

Individuare i certificati creati nella cartella **Personale** → **Certificati** ed eliminarli.

2. **Creare un file flag del server**

   Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Utilizzare l'utilità klscflag per creare il contrassegno del server KLSRV_MYSQL_OPT_SSL_CA e specificare il percorso del certificato come valore.

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <percorso di ca-cert.pem> -t s
   ```

3. **Configurare il database**

   Specificare i certificati nel file my.cnf. Aprire il file my.cnf in un editor di testo e aggiungere le seguenti righe nella sezione [mysqld]:

   ```
   [mysqld]
   ssl-ca="...\mysqlcerts\ca-cert.pem"
   ssl-cert="...\mysqlcerts\server-cert.pem"
   ssl-key="...\mysqlcerts\server-key.pem"
   ```

Abilitazione dell'autenticazione SSL bidirezionale

Seguire questi passaggi per configurare l'autenticazione SSL bidirezionale per MySQL:

1. **Creare file flag del server**

   Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Utilizzare l'utilità klscflag per creare i contrassegni del server e specificare il percorso dei file del certificato come valori:

   ```
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CA -v <percorso di ca-cert.pem> -t
   s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_CERT -v <percorso di server-
   cert.pem> -t s
   klscflag -fset -pv klserver -n KLSRV_MYSQL_OPT_SSL_KEY -v <percorso di server-key.pem>
   -t s
   ```

2. **Specificare la passphrase (facoltativo)**

   Se server-key.pem richiede una passphrase, creare un contrassegno KLSRV_MARIADB_OPT_TLS_PASPHRASE e specificare la passphrase come valore:

   ```
   klscflag -fset -pv klserver -n KLSRV_MARIADB_OPT_TLS_PASPHRASE -v <passphrase> -t s
   ```

3. **Configurare il database**

Specificare i certificati nel file my.cnf. Aprire il file my.cnf in un editor di testo e aggiungere le seguenti righe nella sezione [mysqld]:

```
[mysqld]
ssl-ca="...\ca-cert.pem"
ssl-cert="...\server-cert.pem"
ssl-key="...\server-key.pem"
```

Scenario: autenticazione del server PostgreSQL

Si consiglia di utilizzare un certificato TLS per autenticare il server PostgreSQL. È possibile utilizzare un certificato di un'autorità di certificazione attendibile o un certificato autofirmato. Utilizzare un certificato di un'autorità di certificazione attendibile perché un certificato autofirmato fornisce solo una protezione limitata.

Administration Server supporta l'autenticazione SSL unidirezionale e bidirezionale per PostgreSQL.

L'autenticazione del server PostgreSQL avviene in fasi:

1. **Generazione di un certificato per il server PostgreSQL**

   In un'utilità multipiattaforma basata su OpenSSL, eseguire i seguenti comandi:

   ```
   openssl req -new -x509 -days 365 -nodes -text -out psql.crt -keyout psql.key -subj "/CN=psql"
   chmod og-rwx psql.key
   ```

2. **Generazione di un certificato per Administration Server**

   Eseguire i seguenti comandi. Il valore CN deve corrispondere al nome dell'utente che si connette a PostgreSQL per conto di Administration Server. Il nome utente è impostato su postgres per impostazione predefinita.

   ```
   openssl req -new -x509 -days 365 -nodes -text -out postgres.crt -keyout postgres.key -subj "/CN=postgres"
   chmod og-rwx postgres.key
   ```

3. **Configurazione dell'autenticazione del certificato client**

   Modificare pg_hba.conf come segue:

   ```
   hostssl all all 0.0.0.0/0 md5
   ```

   Assicurarsi che pg_hba.conf non includa un record che inizia con `host`.

4. **Specifica del certificato PostgreSQL**

   Autenticazione SSL unidirezionale

   Modificare postgresql.conf come segue (specificare il percorso corretto dei file .crt e .key):

   ```
   listen_addresses ='localhost, server-ip'
   ssl = on
   ssl_cert_file = '<psql.crt>'
   ssl_key_file = '<psql.key>'
   ```

   Autenticazione SSL bidirezionale

Modificare postgresql.conf come segue (specificare il percorso corretto dei file .crt e .key):

```
listen_addresses ='localhost, server-ip'
ssl = on
ssl_ca_file = '<postgres.crt>'
ssl_cert_file = '<psql.crt>'
ssl_key_file = '<psql.key>'
```

5. **Riavvio del daemon PostgreSQL**

   Eseguire il seguente comando:

   ```
   systemctl restart postgresql-14.service
   ```

6. **Specifica del flag del server per Administration Server**

   Autenticazione SSL unidirezionale

   Utilizzare l'utilità klscflag per creare il contrassegno del server KLSRV_POSTGRES_OPT_SSL_CA e specificare il percorso del certificato come valore.

   Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Eseguire il seguente comando:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <percorso di psql.crt> -t s
   ```

   Autenticazione SSL bidirezionale

   Utilizzare l'utilità klscflag per creare i contrassegni del server e specificare il percorso dei file del certificato come valori.

   Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Eseguire i seguenti comandi:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CA -v <percorso di psql.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_CERT -v <percorso di postgres.crt> -t s
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_SSL_KEY -v <percorso di postgres.key> -t s
   ```

   Se `postgres.key` richiede una passphrase, creare un contrassegno KLSRV_POSTGRES_OPT_TLS_PASPHRASE e specificare la passphrase come valore:

   ```
   klscflag -fset -pv klserver -n KLSRV_POSTGRES_OPT_TLS_PASPHRASE -v <passphrase> -t s
   ```

7. **Riavvio del servizio Administration Server**

Raccomandazioni sull'installazione di Administration Server

Questa sezione contiene raccomandazioni su come installare Administration Server. Vengono inoltre illustrati gli scenari per l'utilizzo di una cartella condivisa nel dispositivo con Administration Server per distribuire Network Agent nei dispositivi client.

Creazione degli account per i servizi di Administration Server in un cluster di failover

Per impostazione predefinita, il programma di installazione crea automaticamente account senza privilegi per i servizi di Administration Server. Questo comportamento è il più appropriato per l'installazione di Administration Server in un normale dispositivo.

Tuttavia, l'installazione di Administration Server in un cluster di failover richiede uno scenario diverso:

1. Creare account di dominio senza privilegi per i servizi di Administration Server e includerli in un gruppo di sicurezza di dominio globale denominato KLAdmins.

2. Nel programma di installazione di Administration Server specificare gli account di dominio che sono stati creati per i servizi.

Definizione di una cartella condivisa

Durante l'installazione di Administration Server, è possibile specificare il percorso della cartella condivisa. È anche possibile specificare il percorso della cartella condivisa dopo l'installazione, nelle proprietà di Administration Server. Per impostazione predefinita, la cartella condivisa verrà creata sul dispositivo con Administration Server (con diritti di lettura per il sottogruppo **Everyone**). Tuttavia, in alcuni casi (ad esempio, carico elevato o esigenza di accesso da una rete isolata) è consigliabile posizionare la cartella condivisa in una risorsa file dedicata.

La cartella condivisa viene utilizzata occasionalmente durante la distribuzione di Network Agent.

La distinzione tra maiuscole e minuscole per la cartella condivisa deve essere disabilitata.

Installazione remota con gli strumenti di Administration Server tramite i criteri di gruppo di Active Directory

Se i dispositivi di destinazione appartengono a un dominio Windows (non sono presenti gruppi di lavoro), la distribuzione iniziale (l'installazione di Network Agent e dell'applicazione di protezione nei dispositivi che non sono ancora gestiti) deve essere eseguita tramite i criteri di gruppo di Active Directory. La distribuzione viene eseguita utilizzando l'attività standard per l'installazione remota di Kaspersky Security Center. Se la rete è di grandi dimensioni, è consigliabile posizionare la cartella condivisa in una risorsa file dedicata per ridurre il carico sul sottosistema del disco del dispositivo con Administration Server.

Installazione remota tramite l'invio del percorso UNC di un pacchetto indipendente

Se gli utenti dei dispositivi in rete nell'organizzazione dispongono di diritti di amministratore locale, un altro metodo di distribuzione iniziale è la creazione di un pacchetto indipendente di Network Agent (o perfino di un pacchetto di Network Agent "associato" all'applicazione di protezione). Dopo aver creato un pacchetto indipendente, inviare agli utenti un collegamento al pacchetto, archiviato nella cartella condivisa. L'installazione ha inizio quando gli utenti fanno clic sul collegamento.

Aggiornamento dalla cartella condivisa di Administration Server

Nell'attività di aggiornamento dell'anti-virus è possibile configurare l'aggiornamento dalla cartella condivisa di Administration Server. Se l'attività è stata assegnata a numerosi di dispositivi, è consigliabile posizionare la cartella condivisa in una risorsa file dedicata.

Installazione di immagini dei sistemi operativi

Le immagini del sistema operativo vengono sempre installate tramite la cartella condivisa: i dispositivi leggono le immagini del sistema operativo dalla cartella condivisa. Se si prevede di distribuire le immagini su numerosi dispositivi aziendali, è consigliabile posizionare la cartella condivisa in una risorsa file dedicata.

Specificazione dell'indirizzo dell'Administration Server

Durante l'installazione di Administration Server, è possibile specificare l'indirizzo di Administration Server. Questo indirizzo sarà utilizzato come indirizzo predefinito al momento della creazione dei pacchetti di installazione di Network Agent.

Come indirizzo di Administration Server è possibile specificare quanto segue:

- Nome NetBIOS di Administration Server, specificato per impostazione predefinita
- Nome di dominio completo (FQDN) di Administration Server se il DNS (Domain Name System) nella rete dell'organizzazione è stato configurato e funziona correttamente
- Indirizzo esterno se Administration Server è installato nella rete perimetrale

Sarà quindi possibile modificare l'indirizzo di Administration Server utilizzando gli strumenti di Administration Console. L'indirizzo non sarà modificato automaticamente nei pacchetti di installazione di Network Agent che sono stati già creati.

Installazione standard

L'installazione standard è un tipo di installazione di Administration Server che utilizza i percorsi predefiniti dei file dell'applicazione, installa il set di plug-in predefinito e non abilita Mobile Device Management.

Per installare Kaspersky Security Center Administration Server in un dispositivo locale:

Eseguire il file eseguibile ksc_<numero versione>.<numero build>_full_<lingua localizzazione>.exe.

Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da installare. Nella finestra di selezione delle applicazioni, fare clic sul collegamento **Installa Kaspersky Security Center Administration Server** per avviare l'Installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

Passaggio 1. Visualizzazione del Contratto di licenza e dell'Informativa sulla privacy

A questo punto dell'Installazione guidata, è necessario leggere il Contratto di licenza tra l'utente e Kaspersky, nonché l'Informativa sulla privacy.

È inoltre possibile che venga richiesto di visualizzare i Contratti di licenza e le Informative sulla privacy per i plug-in di gestione dell'applicazione nel kit di distribuzione di Kaspersky Security Center.

Leggere attentamente il Contratto di licenza e l'Informativa sulla privacy. Se si accettano tutti i termini del Contratto di licenza e dell'Informativa sulla privacy, confermare selezionando le caselle di controllo appropriate.

L'installazione dell'applicazione nel dispositivo continuerà dopo la selezione di entrambe le caselle di controllo.

Se non si accetta il Contratto di licenza o l'Informativa sulla privacy, annullare l'installazione facendo clic sul pulsante **Annulla**.

Passaggio 2. Selezione del metodo di installazione

Nella finestra di selezione del tipo di installazione selezionare **Standard**.

L'installazione standard è consigliabile se si desidera provare a utilizzare Kaspersky Security Center, ad esempio verificandone il funzionamento in un'area delimitata all'interno della rete aziendale. Durante l'installazione standard, è possibile esclusivamente configurare il database. Non è necessario specificare le impostazioni di Administration Server poiché verranno utilizzati i valori predefiniti. L'installazione standard non consente di selezionare i plug-in di gestione da installare e viene installato solo il set di plug-in predefinito. Durante l'installazione standard non vengono creati pacchetti di installazione per i dispositivi mobili. Tuttavia, è possibile crearli successivamente in Administration Console.

Passaggio 3. Installazione di Kaspersky Security Center Web Console

Questo passaggio viene visualizzato solo se si utilizza un sistema operativo a 64 bit. In caso contrario questo passaggio non viene visualizzato, dal momento che Kaspersky Security Center Web Console non funziona con i sistemi operativi a 32 bit.

Per impostazione predefinita, verrà eseguita l'installazione sia di Kaspersky Security Center Web Console che di Administration Console basata su MMC.

Se si desidera installare solo Kaspersky Security Center Web Console:

1. Selezionare **Installa solo questa**.
2. Scegliere **Console basata sul Web** nell'elenco a discesa.

L'installazione di Kaspersky Security Center Web Console viene avviata automaticamente al termine dell'installazione di Administration Server.

Se si desidera installare solo la Administration Console basata su MMC:

1. Selezionare **Installa solo questa**.
2. Scegliere **Console basata su MMC** nell'elenco a discesa.

Passaggio 4. Selezione delle dimensioni della rete

Specificare le dimensioni della rete in cui è in corso l'installazione di Kaspersky Security Center. A seconda del numero di dispositivi nella rete, la procedura guidata configura l'installazione e l'aspetto dell'interfaccia dell'applicazione in modo che corrispondano.

Nella tabella seguente sono elencate le impostazioni di installazione dell'applicazione e relative all'aspetto dell'interfaccia, a seconda delle diverse dimensioni della rete.

Dipendenza delle impostazioni di installazione dalle dimensioni della rete selezionate

Impostazioni	Da 1 a 100 dispositivi gestiti	Da 101 a 1000 dispositivi gestiti	Da 1001 a 5000 dispositivi gestiti	Più di 5000 dispositivi gestiti
Visualizzazione nella struttura della console con il nodo degli Administration Server secondari e virtuali e di tutte le impostazioni correlate agli Administration Server secondari e virtuali (disponibile solo in Administration Console basato su MMC)	Non disponibile	Non disponibile	Disponibile	Disponibile
Visualizzare con le sezioni **Sicurezza** nelle finestre delle proprietà dell'Administration Server e dei gruppi di amministrazione (disponibile solo in Administration Console basato su MMC)	Non disponibile	Non disponibile	Disponibile	Disponibile
Distribuzione casuale del tempo di avvio per l'attività di aggiornamento nei dispositivi client	Non disponibile	In un intervallo di 5 minuti	In un intervallo di 10 minuti	In un intervallo di 10 minuti

Se si connette Administration Server a un server database MySQL 5.7 o SQL Express, è consigliabile evitare di utilizzare l'applicazione per gestire più di 10.000 dispositivi. Per il sistema di gestione database MariaDB, il numero massimo di dispositivi gestiti consigliato è 20.000.

Passaggio 5. Selezione di un database

In questo passaggio della procedura guidata, selezionare uno dei seguenti sistemi di gestione dei database (DBMS) che verrà utilizzato per archiviare il database di Administration Server:

- **Microsoft SQL Server o SQL Server Express**
- **MySQL o MariaDB**
- **PostgreSQL o Postgres Pro**

È consigliabile installare Administration Server in un server dedicato anziché in un controller di dominio. Se tuttavia si installa Kaspersky Security Center in un server che opera come controller di dominio di sola lettura (RODC), Microsoft SQL Server (SQL Express) non deve essere installato in locale (nello stesso dispositivo). In questo caso, è consigliabile installare Microsoft SQL Server (SQL Express) in remoto (su un altro dispositivo) o utilizzare MySQL, MariaDB o PostgreSQL se è necessario installare il DBMS in locale.

La struttura del database di Administration Server è disponibile nel file klakdb.chm, ubicato nella cartella di installazione di Kaspersky Security Center. Questo file è disponibile anche in un archivio sul portale Kaspersky: klakdb.zip.

Passaggio 6. Configurazione di SQL Server

In questa fase della procedura guidata, specificare le seguenti impostazioni di connessione, a seconda del sistema di gestione del database (DBMS) selezionato:

- Se è stato selezionato **Microsoft SQL Server o SQL Server Express** nel passaggio precedente:

  - Nel campo **Nome istanza SQL Server** specificare il nome di SQL Server nella rete. Per visualizzare un elenco di tutti gli SQL Server presenti nella rete, fare clic sul pulsante **Sfoglia**. Questo campo è vuoto per impostazione predefinita.

    Se ci si connette a SQL Server tramite una porta personalizzata, oltre al nome host di SQL Server specificare il numero di porta separato da una virgola, ad esempio:

    ```
    SQL_Server_host_name,1433
    ```

    Se si protegge la comunicazione tra Administration Server e SQL Server tramite un certificato, specificare nel campo **Nome istanza SQL Server** lo stesso nome host utilizzato durante la generazione del certificato. Se si utilizza un'istanza denominata di SQL Server, oltre al nome host di SQL Server specificare il numero di porta separato da una virgola, ad esempio:

    ```
    SQL_Server_name,1433
    ```

    Se si utilizzano più istanze SQL Server nello stesso host, specificare anche il nome dell'istanza separato da una barra rovesciata, ad esempio:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Se in un SQL Server nella rete aziendale è abilitata la funzionalità Always On, specificare il nome del listener del gruppo di disponibilità nel campo **Nome istanza SQL Server**. Administration Server supporta solo la modalità di disponibilità con commit sincrono quando la funzionalità Always On è abilitata.

  - Nel campo **Nome database** specificare il nome del DBMS creato per l'archiviazione dei dati di Administration Server. Il valore predefinito è *KAV*.

  Se in questo passaggio si desidera installare SQL Server nel dispositivo da cui si esegue l'installazione di Kaspersky Security Center, è necessario arrestare l'installazione e riavviarla dopo l'installazione di SQL Server. Le versioni di SQL Server supportate sono elencate nei requisiti di sistema.

  Se si desidera installare SQL Server in un dispositivo remoto, non è necessario interrompere l'Installazione guidata di Kaspersky Security Center. Installare SQL Server e riprendere l'installazione di Kaspersky Security Center.

- Se è stato selezionato **MySQL o MariaDB** nel passaggio precedente:

  - Nel campo **Nome istanza SQL Server** specificare il nome dell'istanza DBMS. Per impostazione predefinita, il nome è l'indirizzo IP del dispositivo in cui deve essere installato Kaspersky Security Center.

  - Nel campo **Porta** specificare la porta per la connessione di Administration Server al DBMS. Il numero di porta predefinito è 3306.

  - Nel campo **Nome database** specificare il nome del DBMS creato per l'archiviazione dei dati di Administration Server. Il valore predefinito è *KAV*.

- Se è stato selezionato **PostgreSQL o Postgres Pro** nel passaggio precedente:

  - Nel campo **PostgreSQL o Postgres Pro Server** specificare il nome dell'istanza DBMS. Per impostazione predefinita, il nome è l'indirizzo IP del dispositivo in cui deve essere installato Kaspersky Security Center.

- Nel campo **Porta** specificare la porta per la connessione di Administration Server al DBMS. Il numero di porta predefinito è 5432.

- Nel campo **Nome database** specificare il nome del DBMS creato per l'archiviazione dei dati di Administration Server. Il valore predefinito è *KAV*.

Passaggio 7. Selezione di un metodo di autenticazione

Determinare la modalità di autenticazione che verrà utilizzata durante la connessione di Administration Server al sistema di gestione dei database (DBMS).

A seconda del DBMS selezionato, è possibile scegliere tra le seguenti modalità di autenticazione:

- Per SQL Express o Microsoft SQL Server selezionare una delle seguenti opzioni:

  - **Modalità di autenticazione Microsoft Windows**. Per la verifica dei diritti viene utilizzato l'account utilizzato per l'avvio di Administration Server.

  - **Modalità di autenticazione SQL Server**. Se si seleziona questa opzione, per verificare i diritti di accesso verrà utilizzato l'account specificato nella finestra. Compilare i campi **Account** e **Password**.

    Per visualizzare la password immessa, tenere premuto il pulsante **Mostra**.

  Per entrambe le modalità di autenticazione, l'applicazione verifica se il database è disponibile. Se il database non è disponibile, viene visualizzato un messaggio di errore ed è necessario fornire le credenziali corrette.

  Se il database di Administration Server è memorizzato in un altro dispositivo e l'account di Administration Server non dispone dell'accesso al server di database, è necessario utilizzare la modalità di autenticazione SQL Server durante l'installazione o l'upgrade di Administration Server. Questa situazione può verificarsi quando il dispositivo in cui è memorizzato il database è esterno al dominio o quando Administration Server viene installato utilizzando un account LocalSystem.

- Per MySQL, MariaDB, PostgreSQL o Postgres Pro, specificare l'account e la password.

Passaggio 8. Decompressione e installazione dei file nel disco rigido

Al termine della configurazione dell'installazione dei componenti di Kaspersky Security Center, è possibile avviare l'installazione dei file sul disco rigido.

Se l'installazione richiede ulteriori programmi, verrà visualizzata una notifica nella pagina **Installazione prerequisiti**, prima dell'inizio dell'installazione di Kaspersky Security Center. I programmi richiesti verranno installati automaticamente facendo clic sul pulsante **Avanti**.

Nell'ultima pagina è possibile selezionare quale console avviare per l'utilizzo di Kaspersky Security Center:

- **Avvia Administration Console basata su MMC**

- **Avvia Kaspersky Security Center Web Console**

  Questa opzione è disponibile solo se si è scelto di installare Kaspersky Security Center Web Console in uno dei passaggi precedenti.

È inoltre possibile fare clic su **Fine** per chiudere la procedura guidata senza avviare l'utilizzo di Kaspersky Security Center. È possibile avviare l'utilizzo in qualsiasi momento.

Al primo avvio di Administration Console o di Kaspersky Security Center Web Console è possibile eseguire la configurazione iniziale dell'applicazione.

Al termine dell'Installazione guidata, i seguenti componenti dell'applicazione vengono installati nel disco rigido in cui è installato il sistema operativo:

- Administration Server (insieme alla versione server di Network Agent)
- Administration Console basata su Microsoft Management Console
- Kaspersky Security Center Web Console (se si sceglie di installarla)
- Plug-in di gestione dell'applicazione disponibili nel kit di distribuzione

Inoltre, se non è stato installato in precedenza, verrà installato Microsoft Windows Installer 4.5.

Installazione personalizzata

L'installazione personalizzata è un tipo di installazione di Administration Server durante cui viene richiesto di selezionare i componenti da installare e specificare la cartella in cui installare l'applicazione.

Utilizzando questo tipo di installazione, è possibile configurare il database e Administration Server, nonché installare i componenti non inclusi nell'installazione standard o i plug-in di gestione per diverse applicazioni di protezione Kaspersky. È inoltre possibile abilitare Mobile Device Management.

Per installare Kaspersky Security Center Administration Server in un dispositivo locale:

Eseguire il file eseguibile ksc_<numero versione>.<numero build>_full_<lingua localizzazione>.exe.

Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da installare. Nella finestra di selezione delle applicazioni, fare clic sul collegamento **Installa Kaspersky Security Center Administration Server** per avviare l'Installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

Passaggio 1. Visualizzazione del Contratto di licenza e dell'Informativa sulla privacy

A questo punto dell'Installazione guidata, è necessario leggere il Contratto di licenza tra l'utente e Kaspersky, nonché l'Informativa sulla privacy.

È inoltre possibile che venga richiesto di visualizzare i Contratti di licenza e le Informative sulla privacy per i plug-in di gestione dell'applicazione nel kit di distribuzione di Kaspersky Security Center.

Leggere attentamente il Contratto di licenza e l'Informativa sulla privacy. Se si accettano tutti i termini del Contratto di licenza e dell'Informativa sulla privacy, confermare selezionando le caselle di controllo appropriate.

L'installazione dell'applicazione nel dispositivo continuerà dopo la selezione di entrambe le caselle di controllo.

Se non si accetta il Contratto di licenza o l'Informativa sulla privacy, annullare l'installazione facendo clic sul pulsante **Annulla**.

Passaggio 2. Selezione del metodo di installazione

Nella finestra di selezione del tipo di installazione specificare **Personalizzata**.

L'installazione personalizzata consente di modificare le impostazioni di Kaspersky Security Center, ad esempio il percorso della cartella condivisa, gli account e le porte per la connessione ad Administration Server, nonché le impostazioni del database. L'installazione personalizzata consente di specificare quali plug-in di gestione di Kaspersky installare. Durante l'installazione personalizzata è possibile creare pacchetti di installazione per i dispositivi mobili attivando l'opzione corrispondente.

Passaggio 3. Selezione dei componenti da installare

Selezionare i componenti di Kaspersky Security Center Administration Server che si desidera installare:

- **Mobile Device Management**. Selezionare questa casella di controllo se è necessario creare pacchetti di installazione per i dispositivi mobili durante l'esecuzione dell'Installazione guidata di Kaspersky Security Center. È inoltre possibile creare pacchetti di installazione per i dispositivi mobili manualmente, dopo l'installazione di Administration Server, utilizzando gli strumenti di Administration Console.

- **Agente SNMP**. Questo componente riceve informazioni statistiche per Administration Server tramite il protocollo SNMP. Il componente è disponibile se l'applicazione viene installata in un dispositivo in cui è installato SNMP.

  > Dopo l'installazione di Kaspersky Security Center, i file .mib necessari per la ricezione delle statistiche saranno disponibili nella sottocartella SNMP della cartella di installazione dell'applicazione.

Network Agent e Administration Console non vengono visualizzati nell'elenco dei componenti. Questi componenti vengono installati automaticamente e non è possibile annullarne l'installazione.

In questo passaggio è necessario specificare una cartella per l'installazione dei componenti di Administration Server. Per impostazione predefinita, i componenti vengono installati in <Unità>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Se la cartella non esiste, verrà creata automaticamente durante l'installazione. È possibile modificare la cartella di destinazione utilizzando il pulsante **Sfoglia**.

Passaggio 4. Installazione di Kaspersky Security Center Web Console

> Questo passaggio viene visualizzato solo se si utilizza un sistema operativo a 64 bit. In caso contrario questo passaggio non viene visualizzato, dal momento che Kaspersky Security Center Web Console non funziona con i sistemi operativi a 32 bit.

Per impostazione predefinita, verrà eseguita l'installazione sia di Kaspersky Security Center Web Console che di Administration Console basata su MMC.

Se si desidera installare solo Kaspersky Security Center Web Console:

1. Selezionare **Installa solo questa**.
2. Scegliere **Console basata sul Web** nell'elenco a discesa.

L'installazione di Kaspersky Security Center Web Console viene avviata automaticamente al termine dell'installazione di Administration Server.

Se si desidera installare solo la Administration Console basata su MMC:

1. Selezionare **Installa solo questa**.
2. Scegliere **Console basata su MMC** nell'elenco a discesa.

Passaggio 5. Selezione delle dimensioni della rete

Specificare le dimensioni della rete in cui è in corso l'installazione di Kaspersky Security Center. A seconda del numero di dispositivi nella rete, la procedura guidata configura l'installazione e l'aspetto dell'interfaccia dell'applicazione in modo che corrispondano.

Nella tabella seguente sono elencate le impostazioni di installazione dell'applicazione e relative all'aspetto dell'interfaccia, a seconda delle diverse dimensioni della rete.

Dipendenza delle impostazioni di installazione dalle dimensioni della rete selezionate

Impostazioni	Da 1 a 100 dispositivi gestiti	Da 101 a 1000 dispositivi gestiti	Da 1001 a 5000 dispositivi gestiti	Più di 5000 dispositivi gestiti
Visualizzazione nella struttura della console con il nodo degli Administration Server secondari e virtuali e di tutte le impostazioni correlate agli Administration Server secondari e virtuali (disponibile solo in Administration Console basato su MMC)	Non disponibile	Non disponibile	Disponibile	Disponibile
Visualizzare con le sezioni **Sicurezza** nelle finestre delle proprietà dell'Administration Server e dei gruppi di amministrazione (disponibile solo in Administration Console basato su MMC)	Non disponibile	Non disponibile	Disponibile	Disponibile
Distribuzione casuale del tempo di avvio per l'attività di aggiornamento nei dispositivi client	Non disponibile	In un intervallo di 5 minuti	In un intervallo di 10 minuti	In un intervallo di 10 minuti

Se si connette Administration Server a un server database MySQL 5.7 o SQL Express, è consigliabile evitare di utilizzare l'applicazione per gestire più di 10.000 dispositivi. Per il sistema di gestione database MariaDB, il numero massimo di dispositivi gestiti consigliato è 20.000.

Passaggio 6. Selezione di un database

In questo passaggio della procedura guidata, selezionare uno dei seguenti sistemi di gestione dei database (DBMS) che verrà utilizzato per archiviare il database di Administration Server:

- **Microsoft SQL Server o SQL Server Express**
- **MySQL o MariaDB**
- **PostgreSQL o Postgres Pro**

È consigliabile installare Administration Server in un server dedicato anziché in un controller di dominio. Se tuttavia si installa Kaspersky Security Center in un server che opera come controller di dominio di sola lettura (RODC), Microsoft SQL Server (SQL Express) non deve essere installato in locale (nello stesso dispositivo). In questo caso, è consigliabile installare Microsoft SQL Server (SQL Express) in remoto (su un altro dispositivo) o utilizzare MySQL, MariaDB o PostgreSQL se è necessario installare il DBMS in locale.

La struttura del database di Administration Server è disponibile nel file klakdb.chm, ubicato nella cartella di installazione di Kaspersky Security Center. Questo file è disponibile anche in un archivio sul portale Kaspersky: klakdb.zip.

Passaggio 7. Configurazione di SQL Server

In questa fase della procedura guidata, specificare le seguenti impostazioni di connessione, a seconda del sistema di gestione del database (DBMS) selezionato:

- Se è stato selezionato **Microsoft SQL Server o SQL Server Express** nel passaggio precedente:

  - Nel campo **Nome istanza SQL Server** specificare il nome di SQL Server nella rete. Per visualizzare un elenco di tutti gli SQL Server presenti nella rete, fare clic sul pulsante **Sfoglia**. Questo campo è vuoto per impostazione predefinita.

    Se ci si connette a SQL Server tramite una porta personalizzata, oltre al nome host di SQL Server specificare il numero di porta separato da una virgola, ad esempio:

    ```
    SQL_Server_host_name,1433
    ```

    Se si protegge la comunicazione tra Administration Server e SQL Server tramite un certificato, specificare nel campo **Nome istanza SQL Server** lo stesso nome host utilizzato durante la generazione del certificato. Se si utilizza un'istanza denominata di SQL Server, oltre al nome host di SQL Server specificare il numero di porta separato da una virgola, ad esempio:

    ```
    SQL_Server_name,1433
    ```

    Se si utilizzano più istanze SQL Server nello stesso host, specificare anche il nome dell'istanza separato da una barra rovesciata, ad esempio:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Se in un SQL Server nella rete aziendale è abilitata la funzionalità Always On, specificare il nome del listener del gruppo di disponibilità nel campo **Nome istanza SQL Server**. Administration Server supporta solo la modalità di disponibilità con commit sincrono quando la funzionalità Always On è abilitata.

  - Nel campo **Nome database** specificare il nome del DBMS creato per l'archiviazione dei dati di Administration Server. Il valore predefinito è *KAV*.

  Se in questo passaggio si desidera installare SQL Server nel dispositivo da cui si esegue l'installazione di Kaspersky Security Center, è necessario arrestare l'installazione e riavviarla dopo l'installazione di SQL Server. Le versioni di SQL Server supportate sono elencate nei requisiti di sistema.

  Se si desidera installare SQL Server in un dispositivo remoto, non è necessario interrompere l'Installazione guidata di Kaspersky Security Center. Installare SQL Server e riprendere l'installazione di Kaspersky Security Center.

- Se è stato selezionato **MySQL o MariaDB** nel passaggio precedente:

  - Nel campo **Nome istanza SQL Server** specificare il nome dell'istanza DBMS. Per impostazione predefinita, il nome è l'indirizzo IP del dispositivo in cui deve essere installato Kaspersky Security Center.

  - Nel campo **Porta** specificare la porta per la connessione di Administration Server al DBMS. Il numero di porta predefinito è 3306.

  - Nel campo **Nome database** specificare il nome del DBMS creato per l'archiviazione dei dati di Administration Server. Il valore predefinito è *KAV*.

- Se è stato selezionato **PostgreSQL o Postgres Pro** nel passaggio precedente:

  - Nel campo **PostgreSQL o Postgres Pro Server** specificare il nome dell'istanza DBMS. Per impostazione predefinita, il nome è l'indirizzo IP del dispositivo in cui deve essere installato Kaspersky Security Center.

- Nel campo **Porta** specificare la porta per la connessione di Administration Server al DBMS. Il numero di porta predefinito è 5432.

- Nel campo **Nome database** specificare il nome del DBMS creato per l'archiviazione dei dati di Administration Server. Il valore predefinito è *KAV*.

Passaggio 8. Selezione di un metodo di autenticazione

Determinare la modalità di autenticazione che verrà utilizzata durante la connessione di Administration Server al sistema di gestione dei database (DBMS).

A seconda del DBMS selezionato, è possibile scegliere tra le seguenti modalità di autenticazione:

- Per SQL Express o Microsoft SQL Server selezionare una delle seguenti opzioni:

  - **Modalità di autenticazione Microsoft Windows**. Per la verifica dei diritti viene utilizzato l'account utilizzato per l'avvio di Administration Server.

  - **Modalità di autenticazione SQL Server**. Se si seleziona questa opzione, per verificare i diritti di accesso verrà utilizzato l'account specificato nella finestra. Compilare i campi **Account** e **Password**.

    Per visualizzare la password immessa, tenere premuto il pulsante **Mostra**.

  Per entrambe le modalità di autenticazione, l'applicazione verifica se il database è disponibile. Se il database non è disponibile, viene visualizzato un messaggio di errore ed è necessario fornire le credenziali corrette.

  Se il database di Administration Server è memorizzato in un altro dispositivo e l'account di Administration Server non dispone dell'accesso al server di database, è necessario utilizzare la modalità di autenticazione SQL Server durante l'installazione o l'upgrade di Administration Server. Questa situazione può verificarsi quando il dispositivo in cui è memorizzato il database è esterno al dominio o quando Administration Server viene installato utilizzando un account LocalSystem.

- Per MySQL, MariaDB, PostgreSQL o Postgres Pro, specificare l'account e la password.

Passaggio 9. Selezione dell'account per l'avvio di Administration Server

Selezionare l'account che verrà utilizzato per avviare Administration Server come servizio.

- **Genera automaticamente l'account**. L'applicazione crea un account denominato KL-AK-* che verrà utilizzato per l'esecuzione del servizio kladminserver.

  È possibile selezionare questa opzione se si intende collocare la cartella condivisa e il DBMS nello stesso dispositivo di Administration Server.

- **Selezionare un account**. Il servizio Administration Server (kladminserver) verrà eseguito utilizzando l'account selezionato.

  Sarà necessario selezionare un account di dominio se ad esempio si intende utilizzare come DBMS un'istanza di SQL Server di qualsiasi versione, tra cui SQL Express, che si trova in un altro dispositivo e/o si intende collocare la cartella condivisa in un altro dispositivo.

  Kaspersky Security Center supporta gli account del servizio gestito (MSA) e gli account del servizio gestito di gruppo (gMSA). Se nel dominio vengono utilizzati questi tipi di account, è possibile selezionarne uno come account del servizio Administration Server.

  Prima di specificare un account MSA o gMSA, è necessario installare l'account nello stesso dispositivo in cui si desidera installare Administration Server. Se l'account non è ancora stato installato, annullare l'installazione di Administration Server, installare l'account e quindi riavviare l'installazione di Administration Server. Per informazioni dettagliate sull'installazione degli account del servizio gestito in un dispositivo locale, consultare la documentazione ufficiale di Microsoft.

  Per specificare un account MSA o gMSA:

  1. Fare clic sul pulsante **Sfoglia**.
  2. Nella finestra visualizzata fare clic sul pulsante **Tipo di oggetto**.
  3. Selezionare il tipo **Account per servizi** e fare clic su **OK**.
  4. Selezionare l'account desiderato, quindi fare clic su **OK**.

L'account selezionato deve disporre di diverse autorizzazioni, a seconda del DBMS che si intende utilizzare.

Per motivi di sicurezza, non assegnare lo stato privilegiato all'account utilizzato per l'esecuzione di Administration Server.

L'account di Administration Server non potrà essere modificato in seguito. È necessario reinstallare il cluster di failover per utilizzare un altro account di Administration Server.

Passaggio 10. Selezione dell'account per l'esecuzione dei servizi di Kaspersky Security Center

Selezionare l'account con cui verranno eseguiti i servizi di Kaspersky Security Center nel dispositivo:

- **Genera automaticamente l'account**. Kaspersky Security Center crea un account locale denominato KlScSvc nel dispositivo nel gruppo kladmins. I servizi di Kaspersky Security Center verranno eseguiti utilizzando l'account creato.

- **Selezionare un account**. I servizi di Kaspersky Security Center verranno eseguiti tramite l'account selezionato.

  Sarà necessario selezionare un account di dominio se si intende, ad esempio, salvare i rapporti in una cartella disponibile in un altro dispositivo o se questo è richiesto dal criterio di protezione dell'organizzazione. È inoltre necessario selezionare un account di dominio se si installa Administration Server in un cluster di failover.

Per motivi di sicurezza, non concedere lo stato di privilegiato all'account con cui vengono eseguiti i servizi.

Il servizio proxy KSN (ksnproxy), il servizio proxy di attivazione Kaspersky (klactprx) e il servizio del portale di autenticazione Kaspersky (klwebsrv) verranno eseguiti utilizzando l'account selezionato.

Passaggio 11. Selezione di una cartella condivisa

Definire il percorso e il nome della cartella condivisa che verrà utilizzata per:

- Memorizzare i file necessari per l'installazione remota delle applicazioni (i file vengono copiati in Administration Server durante la creazione dei pacchetti di installazione).

- Memorizzare gli aggiornamenti che sono stati scaricati da una sorgente degli aggiornamenti in Administration Server.

La condivisione file (in sola lettura) sarà abilitata per tutti gli utenti.

È possibile selezionare una delle seguenti opzioni:

- **Crea cartella condivisa**. Verrà creata una nuova cartella. Nella casella di testo specificare il percorso della cartella.

- **Selezionare una cartella condivisa esistente**. Selezionare una cartella condivisa già esistente.

La cartella condivisa può essere una cartella locale nel dispositivo utilizzato per l'installazione o una directory remota in qualsiasi dispositivo client nella rete aziendale. È possibile utilizzare il pulsante **Sfoglia** per selezionare la cartella condivisa o specificarla manualmente immettendone il percorso UNC (ad esempio, \\server\Share) nel campo corrispondente.

Per impostazione predefinita, il programma di installazione crea una sottocartella locale KLSHARE nella cartella del programma che contiene i componenti di Kaspersky Security Center.

È possibile definire una cartella condivisa successivamente, se necessario.

Passaggio 12. Configurazione della connessione ad Administration Server

Configurare la connessione ad Administration Server:

- **Porta**

  il numero della porta utilizzata per la connessione ad Administration Server.

  Il numero di porta predefinito è 14000.

- **Porta SSL**

  Numero della porta SSL (Secure Sockets Layer) utilizzata per la connessione protetta ad Administration Server tramite SSL.

  Il numero di porta predefinito è 13000.

- **Lunghezza della chiave di criptaggio**

  Selezionare la lunghezza della chiave di criptaggio: 1024 o 2048 bit.

  Una chiave di criptaggio a 1024 bit genera un carico inferiore sulla CPU, ma viene considerata obsoleta poiché non è in grado di garantire un criptaggio affidabile per via delle specifiche tecniche. Inoltre, è possibile che l'hardware esistente risulti incompatibile con i certificati SSL dotati di chiavi a 1024 bit.

  Una chiave di criptaggio a 2048 bit soddisfa tutti i più avanzati standard di criptaggio. Tuttavia, l'utilizzo di una chiave di criptaggio a 2048 bit può incrementare il carico sulla CPU.

  Per impostazione predefinita, l'opzione **2048 bit (migliore protezione)** è selezionata.

È inoltre possibile modificare i parametri per la connessione ad Administration Server in un secondo momento come segue:

- È possibile modificare i numeri di porta e SSL nella sezione **Porte di connessione** delle proprietà di Administration Server. Per ulteriori informazioni sulle porte di connessione di Administration Server, vedere Porte utilizzate da Kaspersky Security Center.

- È possibile modificare la lunghezza della chiave di criptaggio quando si sostituisce il certificato di Administration Server con l'utilità klsetsrvcert utilizzando il parametro `-o RsaKeyLen:<lunghezza della chiave>`.

Passaggio 13. Definizione dell'indirizzo di Administration Server

Specificare l'indirizzo di Administration Server in uno dei seguenti modi:

- **Nome dominio DNS**. È possibile utilizzare questo metodo quando la rete include un server DNS e i dispositivi client possono utilizzarlo per ricevere l'indirizzo di Administration Server.

- **Nome NetBIOS**. È possibile utilizzare questo metodo quando i dispositivi client ricevono l'indirizzo di Administration Server tramite il protocollo NetBIOS o se nella rete è disponibile un server WINS.

- **Indirizzo IP**. È possibile utilizzare questo metodo se Administration Server ha un indirizzo IP statico, che non verrà modificato in futuro.

Se si installa Kaspersky Security Center nel nodo attivo del cluster di failover Kaspersky Security Center ed è stata creata una scheda di rete secondario durante la preparazione dei nodi del cluster, specificare l'indirizzo IP della scheda. In caso contrario, inserire l'indirizzo IP del sistema di bilanciamento del carico di terze parti in uso.

Passaggio 14. Indirizzo di Administration Server per la connessione dei dispositivi mobili

Questo passaggio dell'Installazione guidata è disponibile se si seleziona per l'installazione Mobile Device Management.

Nella finestra **Indirizzo per la connessione dei dispositivi mobili** specificare l'indirizzo esterno di Administration Server per la connessione dei dispositivi mobili che sono all'esterno della rete locale. È possibile specificare l'indirizzo IP o il DNS (Domain Name System) di Administration Server.

Passaggio 15. Selezione dei plug-in di gestione dell'applicazione

Selezionare i plug-in di gestione dell'applicazione da installare con Kaspersky Security Center.

Per semplificare la ricerca, i plug-in sono divisi in gruppi a seconda del tipo di oggetti protetti.

Passaggio 16. Decompressione e installazione dei file nel disco rigido

Al termine della configurazione dell'installazione dei componenti di Kaspersky Security Center, è possibile avviare l'installazione dei file sul disco rigido.

Se l'installazione richiede ulteriori programmi, verrà visualizzata una notifica nella pagina **Installazione prerequisiti**, prima dell'inizio dell'installazione di Kaspersky Security Center. I programmi richiesti verranno installati automaticamente facendo clic sul pulsante **Avanti**.

Nell'ultima pagina è possibile selezionare quale console avviare per l'utilizzo di Kaspersky Security Center:

- **Avvia Administration Console basata su MMC**
- **Avvia Kaspersky Security Center Web Console**

  Questa opzione è disponibile solo se si è scelto di installare Kaspersky Security Center Web Console in uno dei passaggi precedenti.

È inoltre possibile fare clic su **Fine** per chiudere la procedura guidata senza avviare l'utilizzo di Kaspersky Security Center. È possibile avviare l'utilizzo in qualsiasi momento.

Al primo avvio di Administration Console o di Kaspersky Security Center Web Console è possibile eseguire la configurazione iniziale dell'applicazione.

Distribuzione del cluster di failover Kaspersky Security Center

Questa sezione contiene sia informazioni generali sul cluster di failover Kaspersky Security Center che istruzioni sulla preparazione e sulla distribuzione del cluster di failover Kaspersky Security Center nella rete.

Scenario: Distribuzione di un cluster di failover Kaspersky Security Center

Un cluster di failover Kaspersky Security Center garantisce un'elevata disponibilità di Kaspersky Security Center e riduce al minimo i tempi di inattività di Administration Server in caso di errore. Il cluster di failover si basa su due istanze identiche di Kaspersky Security Center installate in due computer. Una delle istanze funge da nodo attivo e l'altra da nodo passivo. Il nodo attivo gestisce la protezione dei dispositivi client, mentre quello passivo è predisposto a svolgere tutte le funzioni del nodo attivo in caso di errore del nodo attivo. Quando si verifica un errore, il nodo passivo diventa attivo e il nodo attivo diventa passivo.

Prerequisiti

È necessario disporre di hardware che soddisfi i requisiti per il cluster di failover.

Passaggi

La distribuzione delle applicazioni Kaspersky prevede diversi passaggi:

1. **Creazione di un account per i servizi di Kaspersky Security Center**

   Creare un nuovo gruppo di dominio, (in questo scenario viene utilizzato il nome "KLAdmins" per il gruppo), quindi concedere le autorizzazioni di amministratore locale al gruppo in entrambi i nodi e nel file server. A questo punto creare due nuovi account utente di dominio (in questo scenario vengono utilizzati i nomi "ksc" e "rightless" per gli account) e aggiungere gli account al gruppo di dominio KLAdmins.

   Aggiungere l'account utente con cui verrà installato Kaspersky Security Center al gruppo di dominio KLAdmins creato in precedenza.

2. **Preparazione del file server**

   Preparare il file server affinché funzioni come componente del cluster di failover Kaspersky Security Center. Assicurarsi che il file server soddisfi i requisiti hardware e software, creare due cartelle condivise per i dati di Kaspersky Security Center e configurare le autorizzazioni per accedere alle cartelle condivise.

   Istruzioni dettagliate: Preparazione di un file server per il cluster di failover Kaspersky Security Center

3. **Preparazione di nodi attivi e passivi**

   Preparare due dispositivi con hardware e software identici in modo che fungano da nodi attivi e passivi.

   Istruzioni dettagliate: Preparazione dei nodi per il cluster di failover Kaspersky Security Center

4. **Installazione del DBMS (Database Management System)**

   Selezionare uno dei DBMS supportati, quindi installare il DBMS in un dispositivo dedicato. Per informazioni su come installare il DBMS, consultare la relativa documentazione.

5. **Installazione di Kaspersky Security Center**

   Installare Kaspersky Security Center in modalità cluster di failover in entrambi i nodi. È prima necessario installare Kaspersky Security Center nel dispositivo che si desidera che sia l'host attivo, quindi installarlo in quello passivo.

   È necessario installare Kaspersky Security Center Web Console in un dispositivo separato che non sia un nodo del cluster.

   Istruzioni dettagliate: Installazione di Kaspersky Security Center nei nodi del cluster di failover Kaspersky Security Center

6 **Test del cluster di failover**

Verificare di aver configurato correttamente il cluster di failover e che funzioni correttamente. È ad esempio possibile arrestare uno dei servizi di Kaspersky Security Center nel nodo attivo: kladminserver, klnagent, ksnproxy, klactprx o klwebsrv. Dopo l'arresto del servizio, la gestione della protezione deve passare automaticamente al nodo passivo.

Risultati

Il cluster di failover Kaspersky Security Center viene distribuito. Esaminare gli eventi che determinano il passaggio dai nodi attivi a quelli passivi.

Informazioni sul cluster di failover Kaspersky Security Center

Un cluster di failover Kaspersky Security Center garantisce un'elevata disponibilità di Kaspersky Security Center e riduce al minimo i tempi di inattività di Administration Server in caso di errore. Il cluster di failover si basa su due istanze identiche di Kaspersky Security Center installate in due computer. Una delle istanze funge da nodo attivo e l'altra da nodo passivo. Il nodo attivo gestisce la protezione dei dispositivi client, mentre quello passivo è predisposto a svolgere tutte le funzioni del nodo attivo in caso di errore del nodo attivo. Quando si verifica un errore, il nodo passivo diventa attivo e il nodo attivo diventa passivo.

L'utilizzo del cluster di failover non influisce sui calcoli basati sulla Guida per il dimensionamento.

Utilizzare la funzionalità Registro eventi Kaspersky per la risoluzione dei problemi.

Condizioni per il passaggio

Il cluster di failover passa la gestione della protezione dei dispositivi client dal nodo attivo al nodo passivo se si verifica uno dei seguenti eventi nel nodo attivo:

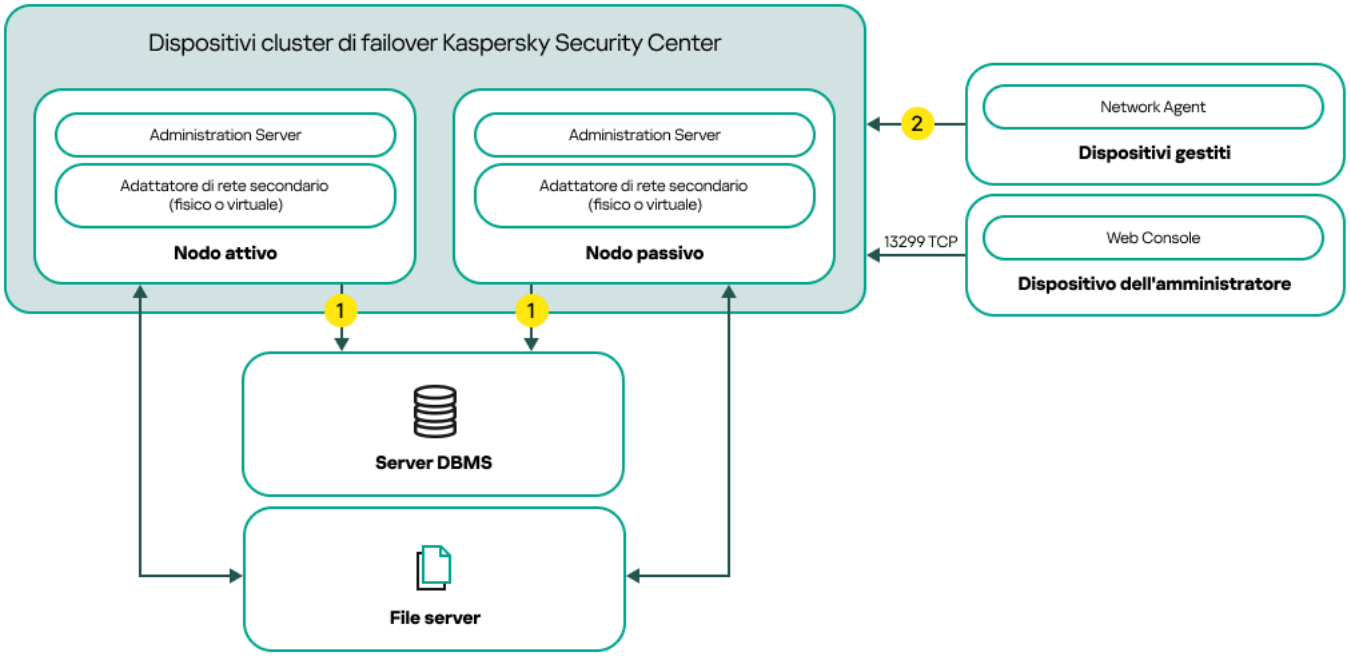
- Il nodo attivo è danneggiato a causa di un errore software o hardware.
- Il nodo attivo è stato temporaneamente arrestato per attività di manutenzione.
- Almeno uno dei servizi (o processi) di Kaspersky Security Center non è riuscito o è stato deliberatamente terminato dall'utente. I servizi di Kaspersky Security Center sono i seguenti: kladminserver, klnagent, klactprx e klwebsrv.
- La connessione di rete tra il nodo attivo e l'archivio nel file server è stata interrotta o terminata.

Il cluster di failover di Kaspersky Security Center gestisce automaticamente tutti i servizi di Kaspersky Security Center. Non riavviare i servizi manualmente.

Schemi di distribuzione

È possibile scegliere uno dei seguenti schemi per distribuire il cluster di failover Kaspersky Security Center:

- Uno schema che utilizza una scheda di rete secondaria.
- Uno schema che utilizza un sistema di bilanciamento del carico di terze parti.

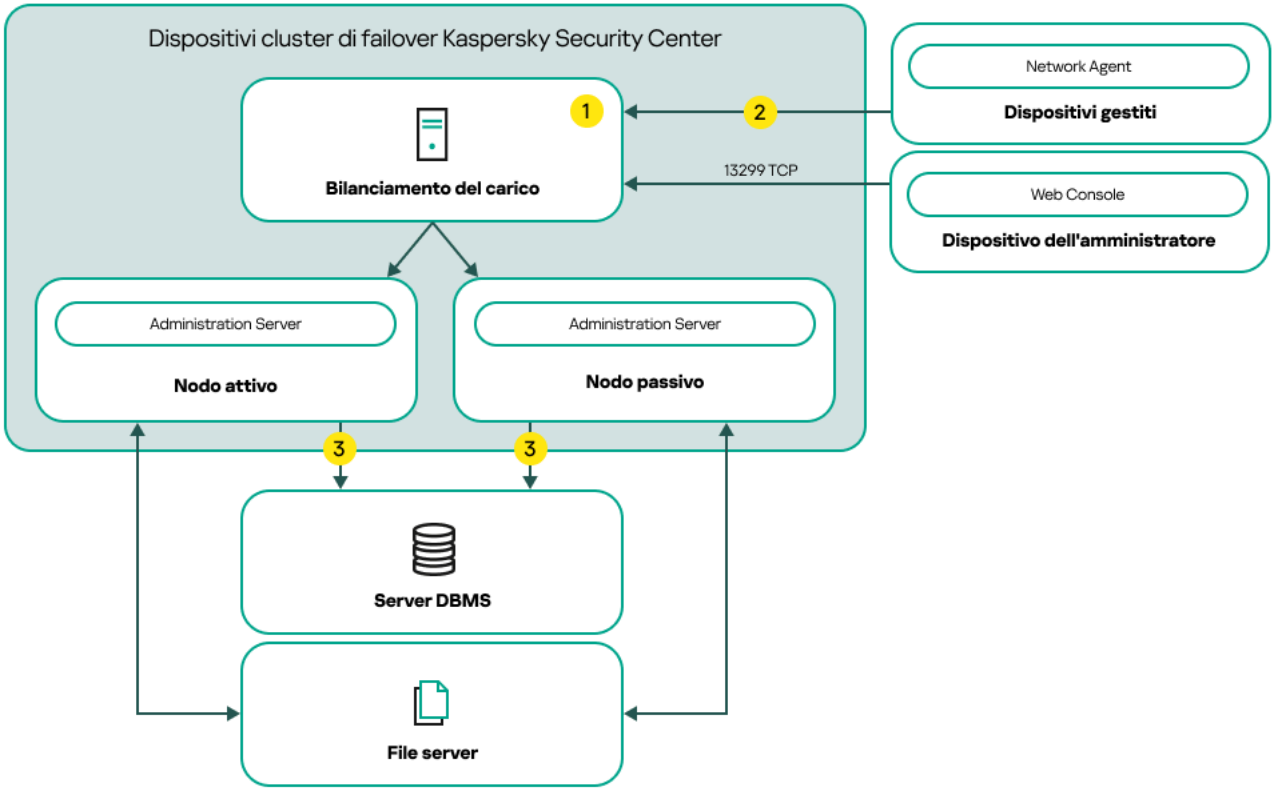


Uno schema che utilizza una scheda di rete secondaria

Legenda schema:

1 Administration Server invia i dati al database. Aprire le porte necessarie nel dispositivo in cui si trova il database, ad esempio la porta 3306 per MySQL Server o la porta 1433 per Microsoft SQL Server. Fare riferimento alla documentazione DBMS per le informazioni attinenti.

2 Nei dispositivi gestiti aprire le seguenti porte: TCP 13000, UDP 13000 e TCP 17000.



Uno schema che utilizza un sistema di bilanciamento del carico di terze parti

Legenda schema:

1 Nel dispositivo di bilanciamento del carico aprire tutte le porte di Administration Server: TCP 13000, UDP 13000, TCP 13299 e TCP 17000.

> Se si desidera utilizzare l'utilità klakaut per l'automazione, è necessario aprire anche la porta TCP 13291.

2 Nei dispositivi gestiti aprire le seguenti porte: TCP 13000, UDP 13000 e TCP 17000.

3 Administration Server invia i dati al database. Aprire le porte necessarie nel dispositivo in cui si trova il database, ad esempio la porta 3306 per MySQL Server o la porta 1433 per Microsoft SQL Server. Fare riferimento alla documentazione DBMS per le informazioni attinenti.

Preparazione di un file server per un cluster di failover Kaspersky Security Center

Un file server funge da componente necessario di un cluster di failover Kaspersky Security Center.

Per preparare un file server:

1. Assicurarsi che il file server soddisfi i requisiti hardware e software.
2. Assicurarsi che il file server ed entrambi i nodi (attivo e passivo) siano inclusi nello stesso dominio o che il file server sia il controller di dominio.

3. Nel file server creare due cartelle condivise. Una di queste verrà utilizzata per conservare le informazioni sullo stato del cluster di failover. L'altra verrà utilizzata per archiviare i dati e le impostazioni di Kaspersky Security Center. Specificare i percorsi delle cartelle condivise durante la configurazione dell'installazione di Kaspersky Security Center.

4. Concedere le autorizzazioni per l'accesso completo (sia le autorizzazioni di condivisione che le autorizzazioni NTFS) alle cartelle condivise create per i seguenti account utente e gruppi:

   - Gruppo di domini KLAdmins.
   - Account utente $<node1> e $<node2>. Qui, <node1> e <node2> sono i nomi dei dispositivi dei nodi attivi e passivi.

Il file server è pronto. Per distribuire il cluster di failover Kaspersky Security Center, seguire le istruzioni aggiuntive in questo scenario.

Preparazione dei nodi per un cluster di failover Kaspersky Security Center

Preparare due dispositivi affinché fungano da nodi attivi e passivi per un cluster di failover Kaspersky Security Center.

Per preparare i nodi per un cluster di failover Kaspersky Security Center:

1. Assicurarsi di avere due dispositivi che soddisfino i requisiti hardware e software. Questi dispositivi fungeranno da nodi attivi e passivi del cluster di failover.

2. Assicurarsi che il file server ed entrambi i nodi siano inclusi nello stesso dominio.

3. Eseguire una delle seguenti operazioni:

   - In ogni nodo, configurare una scheda di rete secondaria.

     Una scheda di rete secondaria può essere fisica o virtuale. Se si desidera utilizzare una scheda di rete fisica, connetterla e configurarla con gli strumenti standard del sistema operativo. Se si desidera utilizzare una scheda di rete virtuale, crearla utilizzando software di terzi.

     Assicurarsi che vengano soddisfatte le seguenti condizioni:

     - Le schede di rete secondarie sono disabilitate.

       È possibile creare le schede di rete secondarie nello stato disabilitato o disabilitarle dopo la creazione.

     - Le schede di rete secondario in entrambi i nodi hanno lo stesso indirizzo IP.

   - Utilizzare un sistema di bilanciamento del carico di terze parti. È ad esempio possibile utilizzare un server nginx. In questo caso, procedere come segue:

     a. Mettere a disposizione un dispositivo basato su Linux dedicato con nginx installato.

     b. Configurare il bilanciamento del carico. Impostare il nodo attivo come server principale e il nodo passivo come server di backup.

     c. Nel server nginx aprire tutte le porte di Administration Server: TCP 13000, UDP 13000, TCP 13299 e TCP 17000.

        > Se si desidera utilizzare l'utilità klakaut per l'automazione, è necessario aprire anche la porta TCP 13291.

4. Riavviare entrambi i nodi e il file server.

5. Mappare le due cartelle condivise create durante la fase di preparazione del file server a ciascuno dei nodi. È necessario mappare le cartelle condivise come unità di rete. Durante il mapping delle cartelle è possibile selezionare eventuali lettere di unità libere. Per accedere alle cartelle condivise, utilizzare le credenziali dell'account utente creato durante il passaggio 1 dello scenario.

I nodi sono pronti. Per distribuire il cluster di failover Kaspersky Security Center, seguire le istruzioni aggiuntive dello scenario.

Installazione di Kaspersky Security Center nei nodi del cluster di failover Kaspersky Security Center

Kaspersky Security Center viene installato separatamente in entrambi i nodi del cluster di failover Kaspersky Security Center. Prima si installa l'applicazione nel nodo attivo, poi su quello passivo. Durante l'installazione, è necessario scegliere quale nodo sarà attivo e quale sarà passivo.

> Solo un utente del gruppo di domini KLAdmins può installare Kaspersky Security Center in ogni nodo.

Per installare Kaspersky Security Center nel nodo attivo del cluster di failover Kaspersky Security Center:

1. Eseguire il file eseguibile ksc_15.1_<numero build>_full_<lingua>.exe.

   Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da installare. Nella finestra di selezione delle applicazioni fare clic sul collegamento **Installazione di Kaspersky Security Center Administration Server** per avviare l'Installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

2. Leggere attentamente il Contratto di licenza e l'Informativa sulla privacy. Se si accettano tutte le condizioni del Contratto di licenza e dell'Informativa sulla privacy, selezionare le seguenti caselle di controllo nella sezione **Confermo di aver letto e compreso integralmente e di accettare quanto segue**:

   - **Termini e condizioni del presente Contratto di licenza con l'utente finale**
   - **Informativa sulla privacy in cui viene descritta la gestione dei dati**

   L'installazione dell'applicazione nel dispositivo continuerà dopo la selezione di entrambe le caselle di controllo.

   Se non si accetta il Contratto di licenza o l'Informativa sulla privacy, annullare l'installazione facendo clic sul pulsante **Annulla**.

3. Selezionare **Nodo primario del cluster di failover di Kaspersky Security Center** per installare l'applicazione nel nodo attivo.

4. Nella finestra **Cartella condivisa** procedere come segue:

   - Nei campi **Condivisione dello stato** e **Condivisione dei dati** specificare i percorsi delle cartelle condivise create nel file server durante la relativa preparazione.
   - Nei campi **Unità della condivisione dello stato** e **Unità della condivisione dei dati** selezionare le unità di rete a cui sono state mappate le cartelle condivise durante la preparazione dei nodi.
   - Selezionare la modalità di connettività del cluster: tramite una scheda di rete secondaria o un sistema di bilanciamento del carico di terzi.

5. Eseguire gli altri passaggi dell'installazione personalizzata, a partire dal passaggio 3.

   Nel passaggio 13 specificare l'indirizzo IP di una scheda di rete secondaria se è stata creata una scheda durante la preparazione dei nodi del cluster. In caso contrario, inserire l'indirizzo IP del sistema di bilanciamento del carico di terze parti in uso.

Kaspersky Security Center è installato nel nodo attivo.

Per installare Kaspersky Security Center nel nodo passivo del cluster di failover Kaspersky Security Center:

1. Eseguire il file eseguibile ksc_15.1_<numero build>_full_<lingua>.exe.

   Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da installare. Nella finestra di selezione delle applicazioni fare clic sul collegamento **Installazione di Kaspersky Security Center Administration Server** per avviare l'Installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

2. Leggere attentamente il Contratto di licenza e l'Informativa sulla privacy. Se si accettano tutte le condizioni del Contratto di licenza e dell'Informativa sulla privacy, selezionare le seguenti caselle di controllo nella sezione **Confermo di aver letto e compreso integralmente e di accettare quanto segue**:

   - **Termini e condizioni del presente Contratto di licenza con l'utente finale**
   - **Informativa sulla privacy in cui viene descritta la gestione dei dati**

   L'installazione dell'applicazione nel dispositivo continuerà dopo la selezione di entrambe le caselle di controllo.

   Se non si accetta il Contratto di licenza o l'Informativa sulla privacy, annullare l'installazione facendo clic sul pulsante **Annulla**.

3. Selezionare **Nodo secondario del cluster di failover di Kaspersky Security Center** per installare l'applicazione nel nodo passivo.

4. Nella finestra **Cartella condivisa**, nel campo **Condivisione dello stato**, specificare un percorso della cartella condivisa con le informazioni sullo stato del cluster creato nel file server durante la relativa preparazione.

5. Fare clic sul pulsante **Installa**. Al termine dell'installazione, fare clic sul pulsante **Fine**.

Kaspersky Security Center è installato nel nodo passivo. Adesso è possibile testare il cluster di failover Kaspersky Security Center per assicurarsi di averlo configurato correttamente e che il cluster funzioni nel modo adeguato.

Avvio e arresto manuale dei nodi del cluster

Potrebbe essere necessario arrestare l'intero cluster di failover Kaspersky Security Center o scollegare temporaneamente uno dei nodi del cluster per la manutenzione. In tal caso, seguire le istruzioni contenute in questa sezione. Non tentare di avviare o arrestare i servizi o i processi relativi al cluster di failover utilizzando altri metodi. Questo potrebbe determinare la perdita di dati.

Avvio e arresto dell'intero cluster di failover per la manutenzione

Per avviare o arrestare l'intero cluster di failover:

1. Nel nodo attivo accedere a <Disco>:\Programmi (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Aprire la riga di comando, quindi eseguire uno dei seguenti comandi:

   - Per arrestare il cluster, eseguire: `klfoc -stopcluster --stp klfoc`
   - Per avviare il cluster, eseguire: `klfoc -startcluster --stp klfoc`

   Il cluster di failover viene avviato o arrestato, a seconda del comando eseguito.

Manutenzione di uno dei nodi

Per eseguire la manutenzione di uno dei nodi:

1. Nel nodo attivo arrestare il cluster di failover utilizzando il comando `klfoc -stopcluster --stp klfoc`.
2. Nel nodo di cui si desidera eseguire la manutenzione accedere a <Disco>:\Programmi (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Aprire la riga di comando, quindi scollegare il nodo dal cluster eseguendo il comando `detach_node.cmd`.
4. Nel nodo attivo avviare il cluster di failover utilizzando il comando `klfoc -startcluster --stp klfoc`.
5. Eseguire le attività di manutenzione.
6. Nel nodo attivo arrestare il cluster di failover utilizzando il comando `klfoc -stopcluster --stp klfoc`.
7. Nel nodo di cui è stata eseguita la manutenzione accedere a <Disco>:\Programmi (x86)\Kaspersky Lab\Kaspersky Security Center.
8. Aprire la riga di comando, quindi collegare il nodo al cluster eseguendo il comando `attach_node.cmd`.
9. Nel nodo attivo avviare il cluster di failover utilizzando il comando `klfoc -startcluster --stp klfoc`.

Viene eseguita la manutenzione del nodo, che viene quindi collegato al cluster di failover.

Installazione di Administration Server in un cluster di failover di Windows Server

La procedura di installazione di Administration Server in un cluster di failover è diversa dall'installazione standard e personalizzata in un dispositivo indipendente.

Eseguire la procedura descritta in questa sezione nel nodo contenente un archivio dati comune del cluster.

Per installare Kaspersky Security Center Administration Server in un cluster:

Eseguire il file eseguibile ksc_<numero versione>.<numero build>_full_<lingua localizzazione>.exe.

Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da installare. Nella finestra di selezione delle applicazioni, fare clic sul collegamento **Installa Kaspersky Security Center Administration Server** per avviare l'Installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

Passaggio 1. Visualizzazione del Contratto di licenza e dell'Informativa sulla privacy

A questo punto dell'Installazione guidata, è necessario leggere il Contratto di licenza tra l'utente e Kaspersky, nonché l'Informativa sulla privacy.

È inoltre possibile che venga richiesto di visualizzare i Contratti di licenza e le Informative sulla privacy per i plug-in di gestione dell'applicazione nel kit di distribuzione di Kaspersky Security Center.

Leggere attentamente il Contratto di licenza e l'Informativa sulla privacy. Se si accettano tutti i termini del Contratto di licenza e dell'Informativa sulla privacy, confermare selezionando le caselle di controllo appropriate.

L'installazione dell'applicazione nel dispositivo continuerà dopo la selezione di entrambe le caselle di controllo.

Se non si accetta il Contratto di licenza o l'Informativa sulla privacy, annullare l'installazione facendo clic sul pulsante **Annulla**.

Passaggio 2. Selezionare il tipo di installazione nel cluster

Selezionare il tipo di installazione nel cluster:

- **Cluster (installa in tutti i nodi del cluster)**

  Questa è l'opzione consigliata. Se si seleziona questa opzione, Administration Server verrà installato in tutti i nodi del cluster contemporaneamente.

  > Nel passaggio in cui si seleziona l'Administration Console per l'installazione, sarà necessario selezionare la console che verrà installata nel nodo del cluster corrente. Se si installa una console solo nel nodo del cluster, in caso di errore del nodo si perderà l'accesso ad Administration Server. Durante questo passaggio, si consiglia di selezionare l'Administration Console basata su MMC per l'installazione in tutti i nodi del cluster. Dopo aver installato Administration Server, installare Kaspersky Security Center Web Console in un dispositivo separato che non sia un nodo del cluster. In questo modo, è possibile gestire Administration Server utilizzando Kaspersky Security Center Web Console in caso di errore dei nodi del cluster.

- **In locale (installa solo in questo dispositivo)**

  Se si seleziona questa opzione, Administration Server verrà installato solo nel nodo corrente, come in un server indipendente, e Administration Server non funzionerà come un'applicazione che riconosce i cluster. È ad esempio possibile scegliere questa opzione per risparmiare spazio di archiviazione condiviso, se la tolleranza agli errori non è necessaria per Administration Server. In caso di errore del nodo corrente sarà necessario installare Administration Server in un altro nodo e ripristinare lo stato di Administration Server da un backup.

Gli altri passaggi sono gli stessi di quando si utilizza il metodo di installazione standard o personalizzato, a partire dal passaggio di selezione del metodo di installazione.

Passaggio 3. Definizione del nome dell'Administration Server virtuale

Specificare il nome di rete del nuovo Administration Server virtuale. Sarà possibile utilizzare questo nome per connettere Administration Console o Kaspersky Security Center Web Console ad Administration Server.

Il nome specificato deve essere diverso dal nome del cluster.

Passaggio 4. Definizione dei dettagli di rete dell'Administration Server virtuale

Per specificare i dettagli di rete della nuova istanza dell'Administration Server virtuale:

1. In **Rete da utilizzare** selezionare la rete del dominio a cui è connesso il nodo del cluster corrente.
2. Eseguire una delle seguenti operazioni:
   - Se il server DHCP viene utilizzato nella rete selezionata per assegnare gli indirizzi IP, selezionare l'opzione **Usa DHCP**.
   - Se il server DHCP non viene utilizzato nella rete selezionata, specificare l'indirizzo IP richiesto.

     L'indirizzo IP specificato deve essere diverso dall'indirizzo IP del cluster.
3. Fare clic su **Aggiungi** per applicare le impostazioni specificate.

Sarà possibile utilizzare l'indirizzo IP assegnato automaticamente o specificato per connettere Administration Console o Kaspersky Security Center Web Console ad Administration Server.

Passaggio 5. Definizione di un gruppo di cluster

Un gruppo di cluster è uno speciale ruolo del cluster di failover che contiene risorse comuni per tutti i nodi. Sono disponibili due opzioni:

- Creazione di un nuovo gruppo di cluster.

  Questa opzione è consigliata nella maggior parte dei casi. Il nuovo gruppo di cluster conterrà tutte le risorse comuni relative all'istanza di Administration Server.

- Selezione di un gruppo di cluster esistente.

  Selezionare questa opzione se si desidera utilizzare una risorsa comune già associata a un gruppo di cluster esistente. È ad esempio possibile utilizzare questa opzione se si desidera utilizzare un archivio associato a un gruppo di cluster esistente e se non sono disponibili altri archivi per un nuovo gruppo di cluster.

Passaggio 6. Per selezionare un archivio dati del cluster

Per selezionare un archivio dati del cluster:

1. In **Archivi disponibili** selezionare l'archivio dati in cui verranno installate le risorse comuni dell'istanza dell'Administration Server virtuale.
2. Se l'archivio dati selezionato contiene diversi volumi, in **Sezioni disponibili nell'unità disco** selezionare il volume desiderato.
3. In **Percorso di installazione** immettere il percorso nell'archivio dati comune in cui verranno installate le risorse dell'istanza dell'Administration Server virtuale.

L'archivio dati è selezionato.

Passaggio 7. Definizione di un account per l'installazione remota

Specificare il nome utente e la password che verranno utilizzati per l'installazione remota dell'istanza dell'Administration Server virtuale in un nodo passivo del cluster.

All'account specificato devono essere concessi privilegi amministrativi in tutti i nodi del cluster.

Passaggio 8. Selezione dei componenti da installare

Selezionare i componenti di Kaspersky Security Center Administration Server che si desidera installare:

- **Mobile Device Management**. Selezionare questa casella di controllo se è necessario creare pacchetti di installazione per i dispositivi mobili durante l'esecuzione dell'Installazione guidata di Kaspersky Security Center. È inoltre possibile creare pacchetti di installazione per i dispositivi mobili manualmente, dopo l'installazione di Administration Server, utilizzando gli strumenti di Administration Console.

- **Agente SNMP**. Questo componente riceve informazioni statistiche per Administration Server tramite il protocollo SNMP. Il componente è disponibile se l'applicazione viene installata in un dispositivo in cui è installato SNMP.

  Dopo l'installazione di Kaspersky Security Center, i file .mib necessari per la ricezione delle statistiche saranno disponibili nella sottocartella SNMP della cartella di installazione dell'applicazione.

Network Agent e Administration Console non vengono visualizzati nell'elenco dei componenti. Questi componenti vengono installati automaticamente e non è possibile annullarne l'installazione.

In questo passaggio è necessario specificare una cartella per l'installazione dei componenti di Administration Server. Per impostazione predefinita, i componenti vengono installati in <Unità>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Se la cartella non esiste, verrà creata automaticamente durante l'installazione. È possibile modificare la cartella di destinazione utilizzando il pulsante **Sfoglia**.

Passaggio 9. Selezione delle dimensioni della rete

Specificare le dimensioni della rete in cui è in corso l'installazione di Kaspersky Security Center. A seconda del numero di dispositivi nella rete, la procedura guidata configura l'installazione e l'aspetto dell'interfaccia dell'applicazione in modo che corrispondano.

Nella tabella seguente sono elencate le impostazioni di installazione dell'applicazione e relative all'aspetto dell'interfaccia, a seconda delle diverse dimensioni della rete.

Dipendenza delle impostazioni di installazione dalle dimensioni della rete selezionate

Impostazioni	Da 1 a 100 dispositivi gestiti	Da 101 a 1000 dispositivi gestiti	Da 1001 a 5000 dispositivi gestiti	Più di 5000 dispositivi gestiti
Visualizzazione nella struttura della console con il nodo degli Administration Server secondari e virtuali e di tutte le impostazioni correlate agli Administration Server secondari e virtuali (disponibile solo in Administration Console basato su MMC)	Non disponibile	Non disponibile	Disponibile	Disponibile
Visualizzare con le sezioni **Sicurezza** nelle finestre delle proprietà dell'Administration Server e dei gruppi di amministrazione (disponibile solo in Administration Console basato su MMC)	Non disponibile	Non disponibile	Disponibile	Disponibile
Distribuzione casuale del tempo di avvio per l'attività di aggiornamento nei dispositivi client	Non disponibile	In un intervallo di 5 minuti	In un intervallo di 10 minuti	In un intervallo di 10 minuti

Se si connette Administration Server a un server database MySQL 5.7 o SQL Express, è consigliabile evitare di utilizzare l'applicazione per gestire più di 10.000 dispositivi. Per il sistema di gestione database MariaDB, il numero massimo di dispositivi gestiti consigliato è 20.000.

Passaggio 10. Selezione di un database

In questo passaggio della procedura guidata, selezionare uno dei seguenti sistemi di gestione dei database (DBMS) che verrà utilizzato per archiviare il database di Administration Server:

- **Microsoft SQL Server o SQL Server Express**
- **MySQL o MariaDB**
- **PostgreSQL o Postgres Pro**

È consigliabile installare Administration Server in un server dedicato anziché in un controller di dominio. Se tuttavia si installa Kaspersky Security Center in un server che opera come controller di dominio di sola lettura (RODC), Microsoft SQL Server (SQL Express) non deve essere installato in locale (nello stesso dispositivo). In questo caso, è consigliabile installare Microsoft SQL Server (SQL Express) in remoto (su un altro dispositivo) o utilizzare MySQL, MariaDB o PostgreSQL se è necessario installare il DBMS in locale.

La struttura del database di Administration Server è disponibile nel file klakdb.chm, ubicato nella cartella di installazione di Kaspersky Security Center. Questo file è disponibile anche in un archivio sul portale Kaspersky: klakdb.zip.

Passaggio 11. Configurazione di SQL Server

In questa fase della procedura guidata, specificare le seguenti impostazioni di connessione, a seconda del sistema di gestione del database (DBMS) selezionato:

- Se è stato selezionato **Microsoft SQL Server o SQL Server Express** nel passaggio precedente:

  - Nel campo **Nome istanza SQL Server** specificare il nome di SQL Server nella rete. Per visualizzare un elenco di tutti gli SQL Server presenti nella rete, fare clic sul pulsante **Sfoglia**. Questo campo è vuoto per impostazione predefinita.

    Se ci si connette a SQL Server tramite una porta personalizzata, oltre al nome host di SQL Server specificare il numero di porta separato da una virgola, ad esempio:

    ```
    SQL_Server_host_name,1433
    ```

    Se si protegge la comunicazione tra Administration Server e SQL Server tramite un certificato, specificare nel campo **Nome istanza SQL Server** lo stesso nome host utilizzato durante la generazione del certificato. Se si utilizza un'istanza denominata di SQL Server, oltre al nome host di SQL Server specificare il numero di porta separato da una virgola, ad esempio:

    ```
    SQL_Server_name,1433
    ```

    Se si utilizzano più istanze SQL Server nello stesso host, specificare anche il nome dell'istanza separato da una barra rovesciata, ad esempio:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Se in un SQL Server nella rete aziendale è abilitata la funzionalità Always On, specificare il nome del listener del gruppo di disponibilità nel campo **Nome istanza SQL Server**. Administration Server supporta solo la modalità di disponibilità con commit sincrono quando la funzionalità Always On è abilitata.

  - Nel campo **Nome database** specificare il nome del DBMS creato per l'archiviazione dei dati di Administration Server. Il valore predefinito è *KAV*.

  Se in questo passaggio si desidera installare SQL Server nel dispositivo da cui si esegue l'installazione di Kaspersky Security Center, è necessario arrestare l'installazione e riavviarla dopo l'installazione di SQL Server. Le versioni di SQL Server supportate sono elencate nei requisiti di sistema.

  Se si desidera installare SQL Server in un dispositivo remoto, non è necessario interrompere l'Installazione guidata di Kaspersky Security Center. Installare SQL Server e riprendere l'installazione di Kaspersky Security Center.

- Se è stato selezionato **MySQL o MariaDB** nel passaggio precedente:

  - Nel campo **Nome istanza SQL Server** specificare il nome dell'istanza DBMS. Per impostazione predefinita, il nome è l'indirizzo IP del dispositivo in cui deve essere installato Kaspersky Security Center.

  - Nel campo **Porta** specificare la porta per la connessione di Administration Server al DBMS. Il numero di porta predefinito è 3306.

  - Nel campo **Nome database** specificare il nome del DBMS creato per l'archiviazione dei dati di Administration Server. Il valore predefinito è *KAV*.

- Se è stato selezionato **PostgreSQL o Postgres Pro** nel passaggio precedente:

  - Nel campo **PostgreSQL o Postgres Pro Server** specificare il nome dell'istanza DBMS. Per impostazione predefinita, il nome è l'indirizzo IP del dispositivo in cui deve essere installato Kaspersky Security Center.

- Nel campo **Porta** specificare la porta per la connessione di Administration Server al DBMS. Il numero di porta predefinito è 5432.

Nel campo **Nome database** specificare il nome del DBMS creato per l'archiviazione dei dati di Administration Server. Il valore predefinito è *KAV*.

Passaggio 12. Selezione di un metodo di autenticazione

Determinare la modalità di autenticazione che verrà utilizzata durante la connessione di Administration Server al sistema di gestione dei database (DBMS).

A seconda del DBMS selezionato, è possibile scegliere tra le seguenti modalità di autenticazione:

- Per SQL Express o Microsoft SQL Server selezionare una delle seguenti opzioni:

  - **Modalità di autenticazione Microsoft Windows**. Per la verifica dei diritti viene utilizzato l'account utilizzato per l'avvio di Administration Server.

  - **Modalità di autenticazione SQL Server**. Se si seleziona questa opzione, per verificare i diritti di accesso verrà utilizzato l'account specificato nella finestra. Compilare i campi **Account** e **Password**.

    Per visualizzare la password immessa, tenere premuto il pulsante **Mostra**.

  Per entrambe le modalità di autenticazione, l'applicazione verifica se il database è disponibile. Se il database non è disponibile, viene visualizzato un messaggio di errore ed è necessario fornire le credenziali corrette.

  Se il database di Administration Server è memorizzato in un altro dispositivo e l'account di Administration Server non dispone dell'accesso al server di database, è necessario utilizzare la modalità di autenticazione SQL Server durante l'installazione o l'upgrade di Administration Server. Questa situazione può verificarsi quando il dispositivo in cui è memorizzato il database è esterno al dominio o quando Administration Server viene installato utilizzando un account LocalSystem.

Per MySQL, MariaDB, PostgreSQL o Postgres Pro, specificare l'account e la password.

Passaggio 13. Selezione dell'account per l'avvio di Administration Server

Selezionare l'account che verrà utilizzato per avviare Administration Server come servizio.

- **Genera automaticamente l'account**. L'applicazione crea un account denominato KL-AK-* che verrà utilizzato per l'esecuzione del servizio kladminserver.

  È possibile selezionare questa opzione se si intende collocare la cartella condivisa e il DBMS nello stesso dispositivo di Administration Server.

- **Selezionare un account**. Il servizio Administration Server (kladminserver) verrà eseguito utilizzando l'account selezionato.

  Sarà necessario selezionare un account di dominio se ad esempio si intende utilizzare come DBMS un'istanza di SQL Server di qualsiasi versione, tra cui SQL Express, che si trova in un altro dispositivo e/o si intende collocare la cartella condivisa in un altro dispositivo.

  Kaspersky Security Center supporta gli account del servizio gestito (MSA) e gli account del servizio gestito di gruppo (gMSA). Se nel dominio vengono utilizzati questi tipi di account, è possibile selezionarne uno come account del servizio Administration Server.

  Prima di specificare un account MSA o gMSA, è necessario installare l'account nello stesso dispositivo in cui si desidera installare Administration Server. Se l'account non è ancora stato installato, annullare l'installazione di Administration Server, installare l'account e quindi riavviare l'installazione di Administration Server. Per informazioni dettagliate sull'installazione degli account del servizio gestito in un dispositivo locale, consultare la documentazione ufficiale di Microsoft.

  Per specificare un account MSA o gMSA:

  1. Fare clic sul pulsante **Sfoglia**.
  2. Nella finestra visualizzata fare clic sul pulsante **Tipo di oggetto**.
  3. Selezionare il tipo **Account per servizi** e fare clic su **OK**.
  4. Selezionare l'account desiderato, quindi fare clic su **OK**.

L'account selezionato deve disporre di diverse autorizzazioni, a seconda del DBMS che si intende utilizzare.

Per motivi di sicurezza, non assegnare lo stato privilegiato all'account utilizzato per l'esecuzione di Administration Server.

L'account di Administration Server non potrà essere modificato in seguito. È necessario reinstallare il cluster di failover per utilizzare un altro account di Administration Server.

Passaggio 14. Selezione dell'account per l'esecuzione dei servizi di Kaspersky Security Center

Selezionare l'account con cui verranno eseguiti i servizi di Kaspersky Security Center nel dispositivo:

- **Genera automaticamente l'account**. Kaspersky Security Center crea un account locale denominato KlScSvc nel dispositivo nel gruppo kladmins. I servizi di Kaspersky Security Center verranno eseguiti utilizzando l'account creato.

- **Selezionare un account**. I servizi di Kaspersky Security Center verranno eseguiti tramite l'account selezionato.

  Sarà necessario selezionare un account di dominio se si intende, ad esempio, salvare i rapporti in una cartella disponibile in un altro dispositivo o se questo è richiesto dal criterio di protezione dell'organizzazione. È inoltre necessario selezionare un account di dominio se si installa Administration Server in un cluster di failover.

Per motivi di sicurezza, non concedere lo stato di privilegiato all'account con cui vengono eseguiti i servizi.

Il servizio proxy KSN (ksnproxy), il servizio proxy di attivazione Kaspersky (klactprx) e il servizio del portale di autenticazione Kaspersky (klwebsrv) verranno eseguiti utilizzando l'account selezionato.

Passaggio 15. Selezione di una cartella condivisa

Definire il percorso e il nome della cartella condivisa che verrà utilizzata per:

- Memorizzare i file necessari per l'installazione remota delle applicazioni (i file vengono copiati in Administration Server durante la creazione dei pacchetti di installazione).

- Memorizzare gli aggiornamenti che sono stati scaricati da una sorgente degli aggiornamenti in Administration Server.

La condivisione file (in sola lettura) sarà abilitata per tutti gli utenti.

È possibile selezionare una delle seguenti opzioni:

- **Crea cartella condivisa**. Verrà creata una nuova cartella. Nella casella di testo specificare il percorso della cartella.

- **Selezionare una cartella condivisa esistente**. Selezionare una cartella condivisa già esistente.

La cartella condivisa può essere una cartella locale nel dispositivo utilizzato per l'installazione o una directory remota in qualsiasi dispositivo client nella rete aziendale. È possibile utilizzare il pulsante **Sfoglia** per selezionare la cartella condivisa o specificarla manualmente immettendone il percorso UNC (ad esempio, \\server\Share) nel campo corrispondente.

Per impostazione predefinita, il programma di installazione crea una sottocartella locale KLSHARE nella cartella del programma che contiene i componenti di Kaspersky Security Center.

È possibile definire una cartella condivisa successivamente, se necessario.

Passaggio 16. Configurazione della connessione ad Administration Server

Configurare la connessione ad Administration Server:

- **Porta**

  il numero della porta utilizzata per la connessione ad Administration Server.

  Il numero di porta predefinito è 14000.

- **Porta SSL**

  Numero della porta SSL (Secure Sockets Layer) utilizzata per la connessione protetta ad Administration Server tramite SSL.

  Il numero di porta predefinito è 13000.

- **Lunghezza della chiave di criptaggio**

  Selezionare la lunghezza della chiave di criptaggio: 1024 o 2048 bit.

  Una chiave di criptaggio a 1024 bit genera un carico inferiore sulla CPU, ma viene considerata obsoleta poiché non è in grado di garantire un criptaggio affidabile per via delle specifiche tecniche. Inoltre, è possibile che l'hardware esistente risulti incompatibile con i certificati SSL dotati di chiavi a 1024 bit.

  Una chiave di criptaggio a 2048 bit soddisfa tutti i più avanzati standard di criptaggio. Tuttavia, l'utilizzo di una chiave di criptaggio a 2048 bit può incrementare il carico sulla CPU.

  Per impostazione predefinita, l'opzione **2048 bit (migliore protezione)** è selezionata.

È inoltre possibile modificare i parametri per la connessione ad Administration Server in un secondo momento come segue:

- È possibile modificare i numeri di porta e SSL nella sezione **Porte di connessione** delle proprietà di Administration Server. Per ulteriori informazioni sulle porte di connessione di Administration Server, vedere Porte utilizzate da Kaspersky Security Center.

- È possibile modificare la lunghezza della chiave di criptaggio quando si sostituisce il certificato di Administration Server con l'utilità klsetsrvcert utilizzando il parametro `-o RsaKeyLen:<lunghezza della chiave>`.

Passaggio 17. Definizione dell'indirizzo di Administration Server

Specificare l'indirizzo di Administration Server. È possibile selezionare una delle seguenti opzioni:

- **Nome dominio DNS**. È possibile utilizzare questo metodo quando la rete include un server DNS e i dispositivi client possono utilizzarlo per ricevere l'indirizzo di Administration Server.

- **Nome NetBIOS**. È possibile utilizzare questo metodo quando i dispositivi client ricevono l'indirizzo di Administration Server tramite il protocollo NetBIOS o se nella rete è disponibile un server WINS.

- **Indirizzo IP**. È possibile utilizzare questo metodo se Administration Server ha un indirizzo IP statico, che non verrà modificato in futuro.

Passaggio 18. Indirizzo di Administration Server per la connessione dei dispositivi mobili

Questo passaggio dell'Installazione guidata è disponibile se si seleziona per l'installazione Mobile Device Management.

Nella finestra **Indirizzo per la connessione dei dispositivi mobili** specificare l'indirizzo esterno di Administration Server per la connessione dei dispositivi mobili che sono all'esterno della rete locale. È possibile specificare l'indirizzo IP o il DNS (Domain Name System) di Administration Server.

Passaggio 19. Decompressione e installazione dei file nel disco rigido

Al termine della configurazione dell'installazione dei componenti di Kaspersky Security Center, è possibile avviare l'installazione dei file sul disco rigido.

Se l'installazione richiede ulteriori programmi, verrà visualizzata una notifica nella pagina **Installazione prerequisiti**, prima dell'inizio dell'installazione di Kaspersky Security Center. I programmi richiesti verranno installati automaticamente facendo clic sul pulsante **Avanti**.

Nell'ultima pagina è possibile selezionare quale console avviare per l'utilizzo di Kaspersky Security Center:

- **Avvia Administration Console basata su MMC**
- **Avvia Kaspersky Security Center Web Console**

  Questa opzione è disponibile solo se si è scelto di installare Kaspersky Security Center Web Console in uno dei passaggi precedenti.

È inoltre possibile fare clic su **Fine** per chiudere la procedura guidata senza avviare l'utilizzo di Kaspersky Security Center. È possibile avviare l'utilizzo in qualsiasi momento.

Al primo avvio di Administration Console o di Kaspersky Security Center Web Console è possibile eseguire la configurazione iniziale dell'applicazione.

Installazione di Administration Server in modalità automatica

Administration Server può essere installato in modalità automatica, ovvero senza l'input interattivo delle impostazioni di installazione.

Per installare Administration Server in un dispositivo locale in modalità automatica:

1. Leggere il Contratto di licenza con l'utente finale. Utilizzare il comando di seguito solo se sono stati compresi e accettati i termini del Contratto di licenza con l'utente finale.

2. Leggere l'Informativa sulla privacy. Utilizzare il comando di seguito solo se si accetta che i dati vengano gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy.

3. Eseguire il comando

```
setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1
<parametri_installazione>"
```

dove `setup_parameters` è un elenco di parametri e dei valori corrispondenti separati da spazi (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). Il file setup.exe è posizionato nella cartella Server, appartenente al kit di distribuzione di Kaspersky Security Center.

I nomi e i possibili valori per i parametri che è possibile utilizzare durante l'installazione di Administration Server in modalità automatica sono elencati nella seguente tabella.

Parametri dell'installazione di Administration Server in modalità automatica

Nome del parametro	Descrizione del parametro	Valori disponibili
EULA	Accettazione dei termini del Contratto di licenza.	• 1 - Ho letto, compreso e accettato i termini del Contratto di licenza con l'utente finale. • Altri valori o nessun valore- Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita).
PRIVACYPOLICY	Accettazione dei termini dell'Informativa sulla privacy.	• 1 - Sono consapevole e accetto che i miei dati vengano gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy. Confermo di aver letto e compreso l'Informativa sulla privacy. • Altro valore o nessun valore- Non accetto i termini dell'Informativa sulla privacy (l'installazione non viene eseguita).
INSTALLATIONMODETYPE	Tipo di installazione di Administration Server.	• Standard – Installazione standard. • Custom – Installazione personalizzata.
INSTALLDIR	Percorso della cartella di installazione di Administration Server.	Valore stringa.
ADDLOCAL	Elenco dei componenti di Administration Server (separati da virgole) da installare.	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Elenco minimo di componenti sufficienti per la corretta installazione di Administration Server: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`.
NETRANGETYPE	Dimensioni della rete (numero di dispositivi della rete).	• NRT_1_100 – Da 1 a 100 dispositivi. • NRT_100_1000 – Da 101 a 1000 dispositivi. • NRT_GREATER_1000 – Oltre 1000 dispositivi.

Nome del parametro	Descrizione del parametro	Valori disponibili
SRV_ACCOUNT_TYPE	Modalità di specificazione di un account con cui Administration Server verrà eseguito come servizio.	• SrvAccountDefault – L'account viene creato automaticamente. • SrvAccountUser – L'account utente è specificato manualmente. In questo caso, è necessario specificare i valori per i parametri `SERVERACCOUNTNAME` e `SERVERACCOUNTPWD`.
SERVERACCOUNTNAME	Nome dell'account con cui Administration Server verrà eseguito come servizio. È necessario specificare un valore per il parametro se SRV_ACCOUNT_TYPE=SrvAccountUser.	Valore stringa.
SERVERACCOUNTPWD	Password dell'account che verrà utilizzato per avviare Administration Server come servizio. È necessario specificare un valore per il parametro se SRV_ACCOUNT_TYPE=SrvAccountUser.	Valore stringa.
SERVERCER	Dimensione della chiave per il certificato di Administration Server (in bit).	• 1 - La dimensione della chiave per il certificato di Administration Server è di 2048 bit. • Nessun valore - La dimensione della chiave per il certificato di Administration Server è di 1024 bit.
DBTYPE	Tipo di database che verrà utilizzato per archiviare il database di Administration Server. Questo parametro è obbligatorio.	• MySQL - Verrà utilizzato un database MySQL o MariaDB. In questo caso, è necessario specificare i valori per i parametri `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME` e `MYSQLACCOUNTPWD`. • MSSQL - Verrà utilizzato il database Microsoft SQL Server (SQL Express). In questo caso, è necessario specificare i valori per i parametri `MSSQLSERVERNAME`, `MSSQLDBNAME` e `MSSQLAUTHTYPE`. • POSTGRES: verrà utilizzato un database PostgreSQL o Postgres Pro. In questo caso, è necessario specificare i valori per i parametri `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` e `POSTGRESACCOUNTPWD`.
MYSQLSERVERNAME	Nome completo del server SQL. È necessario specificare un valore per il parametro se DBTYPE=MySQL.	Valore stringa.
MYSQLSERVERPORT	Numero di porta per la connessione al server SQL. È necessario specificare un valore per il parametro se DBTYPE=MySQL.	Valore numerico.
MYSQLDBNAME	Nome del database che verrà creato per archiviare i dati di Administration Server. È necessario specificare un valore per il parametro se DBTYPE=MySQL.	Valore stringa.
MYSQLACCOUNTNAME	Nome dell'account per la connessione al database. È necessario specificare un valore per il parametro se DBTYPE=MySQL.	Valore stringa.
MYSQLACCOUNTPWD	Password dell'account per la connessione al database. È necessario specificare un valore per il parametro se DBTYPE=MySQL.	Valore stringa.
MSSQLSERVERNAME	Nome completo del server SQL. È necessario specificare un valore per il parametro se DBTYPE=MSSQL.	Valore stringa.
MSSQLDBNAME	Nome del database. È necessario specificare un valore per il parametro se DBTYPE=MSSQL.	Valore stringa.

Nome del parametro	Descrizione del parametro	Valori disponibili
MSSQLAUTHTYPE	Tipo di autorizzazione durante la connessione al server SQL. È necessario specificare un valore per il parametro se DBTYPE=MSSQL.	• Windows – Modalità di Autenticazione di Microsoft Windows. • SQLServer – Modalità di Autenticazione SQL Server. In questo caso, è necessario specificare i valori per i parametri `MSSQLACCOUNTNAME` e `MSSQLACCOUNTPWD`.
MSSQLACCOUNTNAME	Nome dell'account per la connessione al server SQL. È necessario specificare un valore per il parametro se MSSQLAUTHTYPE=SQLServer.	Valore stringa.
MSSQLACCOUNTPWD	Password dell'account per la connessione al server SQL. È necessario specificare un valore per il parametro se MSSQLAUTHTYPE=SQLServer.	Valore stringa.
CREATE_SHARE_TYPE	Metodo per la specificazione della cartella condivisa.	• Create - Creare una nuova cartella condivisa. In questo caso, è necessario specificare i valori per i parametri `SHARELOCALPATH` e `SHAREFOLDERNAME`. • ChooseExisting - Selezionare una cartella esistente. In questo caso, è necessario specificare un valore per il parametro `EXISTSHAREFOLDERNAME`.
SHARELOCALPATH	Percorso completo di una cartella locale. È necessario specificare un valore per il parametro se CREATE_SHARE_TYPE=Create	Valore stringa.
SHAREFOLDERNAME	Nome di rete di una cartella condivisa. È necessario specificare un valore per il parametro se CREATE_SHARE_TYPE=Create.	Valore stringa.
EXISTSHAREFOLDERNAME	Percorso completo di una cartella condivisa esistente. È necessario specificare un valore per il parametro se CREATE_SHARE_TYPE=ChooseExisting.	Valore stringa.
SERVERPORT	Numero di porta per la connessione ad Administration Server.	Valore numerico.
SERVERSSLPORT	Numero di porta per la connessione criptata ad Administration Server tramite il protocollo SSL.	Valore numerico.
SERVERADDRESS	Indirizzo di Administration Server.	Valore stringa.
MOBILESERVERADDRESS	Indirizzo di Administration Server per la connessione dei dispositivi mobili.	Valore stringa.

Per una descrizione dettagliata dei parametri di installazione di Administration Server, fare riferimento alla sezione Installazione personalizzata.

Installazione di Administration Console nella workstation dell'amministratore

È possibile installare separatamente Administration Console nella workstation dell'amministratore e gestire Administration Server tramite la rete utilizzando tale console.

Per installare Administration Console nella workstation dell'amministratore:

1. Eseguire il file eseguibile setup.exe.

   Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da installare.

2. Nella finestra di selezione delle applicazioni, fare clic sul collegamento **Installa solo Kaspersky Security Center Administration Console** per eseguire l'Installazione guidata di Administration Console. Seguire le istruzioni della procedura guidata.

3. Selezionare una cartella di destinazione. Per impostazione predefinita, è selezionata la cartella <Unità>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Se tale cartella non esiste, verrà creata automaticamente durante l'installazione. È possibile modificare la cartella di destinazione utilizzando il pulsante **Sfoglia**.

4. Nell'ultima pagina dell'Installazione guidata, fare clic sul pulsante **Avvia** per avviare l'installazione di Administration Console.

Al termine della procedura guidata, Administration Console sarà installato nella workstation dell'amministratore.

Per installare Administration Console nella workstation dell'amministratore in modalità automatica:

1. Leggere il Contratto di licenza con l'utente finale. Utilizzare il comando di seguito solo se sono stati compresi e accettati i termini del Contratto di licenza con l'utente finale.

2. Nella cartella `Distrib\Console` del kit di distribuzione di Kaspersky Security Center eseguire il file setup.exe utilizzando il seguente comando:

   ```
   setup.exe /s /v"EULA=1"
   ```

   Se si desidera installare tutti i plug-in di gestione dalla cartella `Distrib\Console\Plugins` insieme ad Administration Console, eseguire il seguente comando:

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   Se si desidera specificare quali plug-in di gestione installare dalla cartella `Distrib\Console\Plugins` insieme ad Administration Console specificare i plug-in dopo "/p" e separarli con un punto e virgola:

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   dove `P1`, `P2`, `P3` sono nomi di plug-in che corrispondono ai nomi delle cartelle dei plug-in nella cartella `Distrib\Console\Plugins`. Ad esempio:

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

Administration Console e i plug-in di gestione (se presenti) verranno installati nella workstation dell'amministratore.

Dopo l'installazione di Administration Console, è necessario eseguire la connessione ad Administration Server. A tale scopo, eseguire Administration Console e, nella finestra visualizzata, specificare il nome o l'indirizzo IP del dispositivo in cui è installato Administration Server e le impostazioni dell'account utilizzato per la connessione. Una volta stabilita la connessione all'Administration Server, è possibile gestire il sistema di protezione anti-virus utilizzando Administration Console.

È possibile rimuovere Administration Console utilizzando gli strumenti standard di Microsoft Windows per l'aggiunta e la rimozione di applicazioni.

Modifiche apportate al sistema dopo l'installazione di Kaspersky Security Center

Icona Administration Console

In seguito all'installazione di Administration Console nel dispositivo, viene visualizzata la relativa icona, che consente di avviare Administration Console. Administration Console è disponibile nel menu **Start → Programmi → Kaspersky Security Center**.

Servizi Administration Server e Network Agent

Administration Server e Network Agent verranno installati nel dispositivo come servizi con le proprietà elencate di seguito. La tabella contiene anche gli attributi di altri servizi che si applicano nel dispositivo al termine dell'installazione di Administration Server.

Proprietà dei servizi di Kaspersky Security Center

Componente	Nome servizio	Nome servizio visualizzato	Account
Administration Server	kladminserver	Kaspersky Security Center Administration Server	Account dedicato o definito dall'utente senza privilegi nel formato KL-AK-* creato durante l'installazione
Network Agent	klnagent	Kaspersky Security Center Network Agent	Sistema locale
Server Web per l'accesso a Kaspersky Security Center Web Console e l'amministrazione della rete Intranet dell'organizzazione	klwebsrv	Server Web di Kaspersky	Account KlScSvc dedicato senza privilegi
Server proxy di attivazione	klactprx	Server proxy di attivazione Kaspersky	Account KlScSvc dedicato senza privilegi
Server proxy KSN	ksnproxy	Server proxy Kaspersky Security Network	Account KlScSvc dedicato senza privilegi

Se si installa Kaspersky Security Center nei nodi del cluster di failover Kaspersky Security Center, il servizio klfocsvc_klfoc diventa disponibile. I servizi klnagent_klfoc e klfocsvc_klfoc vengono eseguiti con l'account di sistema locale. Il servizio kladminserver_klfoc deve essere eseguito con l'account "ksc" e gli altri servizi devono essere eseguiti con l'account "rightless". Gli account "ksc" e "rightless" devono essere aggiunti nel gruppo KLAdmins con le autorizzazioni dell'amministratore locale. Per il corretto funzionamento di Kaspersky Security Center, è necessario utilizzare solo gli account "ksc" e "rightless" per l'esecuzione dei servizi. Non è consigliabile utilizzare altri account con gli stessi diritti. La tabella seguente contiene le proprietà dei servizi applicati al dispositivo dopo l'installazione di Administration Server nel cluster di failover Kaspersky Security Center.

Proprietà dei servizi di Kaspersky Security Center installati nel cluster di failover Kaspersky Security Center

Componente	Nome servizio	Nome servizio visualizzato	Account
Administration Server	kladminserver_klfoc	Kaspersky Security Center Administration Server	ksc
Network Agent	klnagent_klfoc	Kaspersky Security Center Network Agent	Sistema locale
Server Web per l'accesso a Kaspersky Security Center Web Console e l'amministrazione della rete Intranet dell'organizzazione	klwebsrv_klfoc	Server Web di Kaspersky	rightless
Server proxy di attivazione	klactprx_klfoc	Server proxy di attivazione Kaspersky	rightless

Server proxy KSN	ksnproxy_klfoc	Server proxy Kaspersky Security Network	rightless
Cluster di failover Kaspersky Security Center	klfocsvc_klfoc	Cluster di failover Kaspersky Security Center	Sistema locale

Servizi di Kaspersky Security Center Web Console

Se si installa Kaspersky Security Center Web Console nel dispositivo, vengono distribuiti i seguenti servizi (vedere la tabella di seguito):

Servizi di Kaspersky Security Center Web Console

Nome servizio visualizzato	Account
Kaspersky Security Center Service Web Console	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web Console	Servizio di rete
Kaspersky Security Center Product Plugins Server	NT Service/KSCWebConsolePlugin
Kaspersky Security Center Web Console Management Service	Sistema locale
Kaspersky Security Center Web Console Message Queue	NT Service/KSCWebConsoleMessageQueue

Versione del server Network Agent

La versione server di Network Agent verrà installata nel dispositivo insieme ad Administration Server. La versione server di Network Agent fa parte di Administration Server, viene installata e rimossa insieme ad Administration Server e può interagire solo con un Administration Server installato in locale. Non è necessario configurare la connessione di Network Agent ad Administration Server: la configurazione è implementata a livello di programmazione perché i componenti sono installati nello stesso dispositivo. La versione server di Network Agent è installata con le stesse proprietà della versione standard ed esegue le stesse funzioni di gestione delle applicazioni. Questa versione verrà gestita dal criterio del gruppo di amministrazione a cui appartiene il dispositivo client di Administration Server. Per la versione server di Network Agent, tutte le attività vengono create a partire dall'ambito di quelle fornite per Administration Server, ad eccezione dell'attività di modifica di Administration Server.

Network Agent non può essere installato separatamente in un dispositivo in cui è già installato Administration Server.

È possibile visualizzare le proprietà dei servizi di Administration Server e Network Agent, nonché monitorarne le operazioni utilizzando gli strumenti di gestione standard di Microsoft Windows: Gestione computer\Servizi. Le informazioni sull'attività del servizio Kaspersky Administration Server sono memorizzate nel registro di sistema di Microsoft Windows, in un ramo distinto del Registro eventi Kaspersky nel dispositivo in cui è installato Administration Server.

È consigliabile non avviare e arrestare manualmente i servizi e non apportare modifiche agli account del servizio nelle impostazioni del servizio. Se necessario, è possibile modificare l'account del servizio di Administration Server tramite l'utilità klsrvswch. È necessario avviare l'utilità klsrvswch nel dispositivo Administration Server con l'account con diritti di amministratore utilizzato per installare Administration Server.

Account utente e gruppi di sicurezza

Per impostazione predefinita, il programma di installazione di Administration Server crea i seguenti account:

- KL-AK-*: account del servizio di Administration Server
- KlScSvc: account per altri servizi del pool di Administration Server
- KlPxeUser: account per la distribuzione dei sistemi operativi

Se si selezionano altri account per il servizio di Administration Server e altri servizi durante l'esecuzione del programma di installazione, vengono utilizzati gli account specificati.

Nel dispositivo in cui è installato Administration Server vengono inoltre creati automaticamente gruppi di protezione locali denominati KLAdmins e KLOperators con i rispettivi set di diritti.

Non è consigliabile eseguire l'installazione di Administration Server in un controller di dominio. Se tuttavia si installa Administration Server nel controller di dominio, è necessario avviare il programma di installazione con i diritti di amministratore di dominio. In tal caso, il programma di installazione crea automaticamente gruppi di protezione dei domini denominati KLAdmins e KLOperators. Se si installa Administration Server in un dispositivo che non è controller di dominio, è necessario avviare il programma di installazione con i diritti di amministratore locali. In tal caso, il programma di installazione crea automaticamente gruppi di protezione locali denominati KLAdmins e KLOperators.

Durante la configurazione delle notifiche e-mail, potrebbe essere necessario creare un account nel server di posta per l'autenticazione ESMTP.

Disinstallazione dell'applicazione

È possibile rimuovere Kaspersky Security Center con gli strumenti standard di Microsoft Windows per l'aggiunta e la rimozione di applicazioni. La rimozione dell'applicazione richiede l'avvio di una procedura guidata che rimuove tutti i componenti dell'applicazione dal dispositivo (compresi i plug-in). La procedura guidata fa in modo che il browser predefinito apra una pagina Web con un sondaggio in cui è possibile specificare perché è stato scelto di interrompere l'utilizzo di Kaspersky Security Center. Se nel corso della procedura guidata non è stata selezionata la rimozione della cartella condivisa (KLSHARE), è possibile eliminarla manualmente dopo il completamento di tutte le attività correlate.

Dopo la rimozione dell'applicazione, alcuni file possono rimanere nella cartella temporanea del sistema.

Durante la Creazione guidata attività di rimozione delle applicazioni, verrà offerta la possibilità di memorizzare una copia di backup di Administration Server.

Dopo la rimozione dell'applicazione da Microsoft Windows 7 e Microsoft Windows 2008, è possibile che la Creazione guidata attività di rimozione delle applicazioni venga terminata prima del completamento. È possibile evitare il problema disabilitando la funzionalità Controllo dell'account utente nel sistema operativo e riavviando la rimozione dell'applicazione.

Informazioni sull'aggiornamento di Kaspersky Security Center

Questa sezione contiene informazioni su come aggiornare Kaspersky Security Center da una versione precedente. È possibile aggiornare Kaspersky Security Center in diversi modi, a seconda che Kaspersky Security Center sia stato installato in locale o nei nodi del cluster di failover Kaspersky Security Center.

Durante l'aggiornamento, l'utilizzo simultaneo del DBMS da parte di Administration Server e di un'altra applicazione non è consentito.

Se si esegue l'upgrade di Administration Server alla versione 15.1, non sarà possibile creare nuovi pacchetti di installazione di Network Agent versione 15 o precedente. Tuttavia, i pacchetti di installazione creati in precedenza saranno disponibili.

Quando si aggiorna Kaspersky Security Center da una versione precedente, tutti i plug-in installati delle applicazioni Kaspersky non vengono disinstallati. Viene eseguito l'aggiornamento automatico del plug-in di Administration Server e del plug-in di Network Agent (sia per Administration Console che per Kaspersky Security Center Web Console).

Upgrade di Kaspersky Security Center da una versione precedente

Il seguente argomento descrive i passaggi di preparazione consigliati per l'upgrade: Upgrade di Kaspersky Security Center e delle applicazioni di protezione gestite.

È possibile installare la versione 15.1 di Administration Server in un dispositivo in cui è installata una versione precedente di Administration Server (a partire dalla versione 11 (11.0.0.1131b)). Durante l'upgrade alla versione 15.1, tutti i dati e le impostazioni della versione precedente di Administration Server vengono mantenuti.

Se si verificano problemi durante l'installazione, è possibile ripristinare la versione precedente di Administration Server utilizzando la copia di backup dei dati di Administration Server data creata prima dell'aggiornamento.

Dopo aver installato nella rete almeno un Administration Server della nuova versione, è possibile eseguire l'upgrade degli altri Administration Server nella rete tramite l'attività di installazione remota che utilizza il pacchetto di installazione di Administration Server.

Se è stato distribuito il cluster di failover Kaspersky Security Center, è inoltre possibile aggiornare Kaspersky Security Center nei suoi nodi.

Per eseguire l'upgrade di una versione precedente di Administration Server alla versione 15.1:

1. Eseguire il file eseguibile ksc_15.1_<numero build>_full_<lingua>.exe per la versione 15.1 (è possibile scaricare il file dal sito Web di Kaspersky).

2. Nella finestra di selezione delle applicazioni fare clic sul collegamento **Installa Kaspersky Security Center** per avviare l'Installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

3. Leggere il Contratto di licenza e l'Informativa sulla privacy. Se si accettano tutte le condizioni del Contratto di licenza e dell'Informativa sulla privacy, selezionare le seguenti caselle di controllo nella sezione **Confermo di aver letto e compreso integralmente e di accettare quanto segue**:

   - **Termini e condizioni del presente Contratto di licenza con l'utente finale**
   - **Informativa sulla privacy in cui viene descritta la gestione dei dati**

   L'installazione dell'applicazione nel dispositivo continuerà dopo la selezione di entrambe le caselle di controllo. L'Installazione guidata richiede di creare un backup dei dati di Administration Server per la versione precedente.

   Kaspersky Security Center supporta il ripristino dei dati da una copia di backup creato con una versione precedente di Administration Server.

4. Se si desidera creare un backup dei dati di Administration Server, specificarlo nella finestra **Backup dei dati di Administration Server** visualizzata.

   L'utilità klbackup crea un backup. Questa utilità è inclusa nel kit di distribuzione ed è disponibile nella radice della cartella di installazione di Kaspersky Security Center.

5. Installare Administration Server versione 15.1 seguendo le istruzioni dell'Installazione guidata.

   Se viene visualizzato un messaggio che informa l'utente che il servizio Kaspersky Security Center Web Console è occupato, fare clic sul pulsante **Ignora** nella finestra della procedura guidata.

   > È consigliabile non interrompere l'Installazione guidata. Se si annulla l'upgrade durante l'installazione di Administration Server possono verificarsi errori nella versione aggiornata di Kaspersky Security Center.

6. Per i dispositivi in cui è installata la versione precedente di Network Agent, creare ed eseguire l'attività di installazione remota per la nuova versione di Network Agent.

   > Si consiglia di aggiornare Network Agent per Linux alla stessa versione di Kaspersky Security Center.

   Al termine dell'attività di installazione remota, viene eseguito l'upgrade della versione di Network Agent.

   Eseguire i seguenti comandi dalle risorse basate su Linux per rimuovere le dipendenze non più necessarie:

   - Per le risorse basate su Debian, eseguire uno dei seguenti comandi:
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - Per le risorse basate su RPM, eseguire uno dei seguenti comandi:
     - `dnf autoremove`
     - `yum autoremove`

Aggiornamento di Kaspersky Security Center nei nodi del cluster di failover Kaspersky Security Center

È possibile installare Administration Server versione 15.1 in ogni nodo del cluster di failover Kaspersky Security Center in cui è installata una versione precedente dell'Administration Server (a partire dalla versione 13.2). Durante l'upgrade alla versione 15.1, tutti i dati e le impostazioni della versione precedente di Administration Server vengono mantenuti.

Se in precedenza Kaspersky Security Center è stato installato nei dispositivi in locale, è inoltre possibile aggiornare Kaspersky Security Center in questi dispositivi.

Per aggiornare Kaspersky Security Center nei nodi del cluster di failover Kaspersky Security Center:

1. Eseguire le seguenti azioni sul nodo attivo del cluster:

   a. Eseguire il file eseguibile ksc_15.1_<numero build>_full_<lingua>.exe.

   Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da aggiornare. Fare clic sul collegamento **Installazione di Kaspersky Security Center Administration Server** per avviare l'Installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

   b. Leggere il Contratto di licenza e l'Informativa sulla privacy. Se si accettano tutte le condizioni del Contratto di licenza e dell'Informativa sulla privacy, selezionare le seguenti caselle di controllo nella sezione **Confermo di aver letto e compreso integralmente e di accettare quanto segue**:

   - **Termini e condizioni del presente Contratto di licenza con l'utente finale**
   - **Informativa sulla privacy in cui viene descritta la gestione dei dati**

   Selezionare entrambe le caselle di controllo per continuare l'installazione.

   Se il Contratto di licenza e l'Informativa sulla privacy non vengono accettati, fare clic sul pulsante **Annulla** per annullare l'aggiornamento.

2. Eseguire le stesse azioni sul nodo passivo del cluster di failover Kaspersky Security Center come sul nodo attivo.

3. Avviare il cluster.

A questo punto, risulta installata la versione più recente dell'Administration Server nei nodi del cluster di failover Kaspersky Security Center.

Aggiornamento di Kaspersky Security Center nei nodi del cluster di failover Microsoft

È possibile effettuare l'upgrade ad Administration Server versione 15.1 in ogni nodo del cluster di failover di Microsoft in cui è installata una versione precedente dell'Administration Server (a partire dalla versione 13.2). Durante l'upgrade alla versione 15.1, tutti i dati e le impostazioni della versione precedente di Administration Server vengono mantenuti.

Per aggiornare Kaspersky Security Center sui nodi del cluster di failover Microsoft, eseguire le seguenti azioni su qualsiasi nodo del cluster:

1. Eseguire il file eseguibile ksc_15.1_<numero build>_full_<lingua>.exe.

   Verrà visualizzata una finestra che richiede di selezionare le applicazioni Kaspersky da aggiornare. Fare clic sul collegamento **Installazione di Kaspersky Security Center Administration Server** per avviare l'Installazione guidata di Administration Server. Seguire le istruzioni della procedura guidata.

2. Leggere il Contratto di licenza e l'Informativa sulla privacy. Se si accettano tutte le condizioni del Contratto di licenza e dell'Informativa sulla privacy, selezionare le seguenti caselle di controllo nella sezione **Confermo di aver letto e compreso integralmente e di accettare quanto segue**:

   - **Termini e condizioni del presente Contratto di licenza con l'utente finale**
   - **Informativa sulla privacy in cui viene descritta la gestione dei dati**

   Selezionare entrambe le caselle di controllo per continuare l'installazione.

   Se il Contratto di licenza e l'Informativa sulla privacy non vengono accettati, fare clic sul pulsante **Annulla** per annullare l'aggiornamento.

3. Nella finestra **Tipo di installazione nel cluster**, selezionare **Cluster (installa su tutti i nodi del cluster)**.

   Successivamente, il programma di installazione configura e completa l'upgrade di Administration Server in tutti i nodi del cluster. Durante l'aggiornamento, non è possibile modificare le impostazioni di Administration Server.

A questo punto, risulta installata la versione più recente dell'Administration Server nei nodi del cluster di failover di Microsoft.

Configurazione iniziale di Kaspersky Security Center

Questa sezione descrive le operazioni che è necessario eseguire dopo l'installazione di Kaspersky Security Center per eseguire la configurazione iniziale.

Guida all'hardening

La Guida all'hardening è destinata ai professionisti che si occupano dell'installazione e dell'amministrazione di Kaspersky Security Center, nonché a quelli che forniscono assistenza tecnica alle organizzazioni che utilizzano Kaspersky Security Center.

Nella Guida all'hardening, sono descritti i suggerimenti e le caratteristiche della configurazione di Kaspersky Security Center e dei suoi componenti, intesi a ridurre i rischi di compromissione.

Prima della configurazione, creare una copia di backup di Kaspersky Security Center Administration Server utilizzando l'attività Backup dei dati di Administration Server o l'utilità klbackup e salvarla in una posizione sicura.

La Guida all'hardening include le seguenti informazioni:

- Selezione dell'architettura di Administration Server
- Configurazione di una connessione sicura ad Administration Server

- Configurazione degli account per l'accesso ad Administration Server
- Gestione della protezione di Administration Server e dei dispositivi client
- Configurazione della protezione per le applicazioni gestite
- Manutenzione di Administration Server
- Trasferimento di informazioni ad applicazioni di terzi

Prima di iniziare a utilizzare Administration Server, Kaspersky Security Center richiede di leggere la versione breve della Guida all'hardening.

Si noti che non è possibile utilizzare Administration Server finché non si conferma di aver letto la Guida all'hardening.

Per leggere la Guida all'hardening:

1. Aprire Administration Console o Kaspersky Security Center Web Console e accedere alla console. La console controlla se l'utente ha confermato di aver letto la versione corrente della Guida all'hardening.

   Se la Guida all'hardening non è ancora stata letta, si apre una finestra che ne mostra una versione breve.

2. Eseguire una delle seguenti operazioni:

   - Se si desidera visualizzare la versione breve della Guida all'hardening come documento di testo, fare clic sul collegamento **Apri in una nuova finestra**.
   - Se si desidera visualizzare la versione completa della Guida all'hardening, fare clic sul collegamento **Apri Guida all'hardening nella Guida in linea**.

3. Dopo aver letto la Guida all'hardening, selezionare la casella di controllo **Confermo di aver letto e compreso la Guida all'hardening**, quindi fare clic sul pulsante **Accetta**.

   A questo punto, è possibile utilizzare Administration Server.

Quando viene visualizzata una nuova versione della Guida all'hardening, Kaspersky Security Center richiederà di leggerla.

Avvio rapido guidato di Administration Server

Questa sezione fornisce informazioni su Avvio rapido guidato di Administration Server.

Informazioni sull'avvio rapido guidato

Questa sezione fornisce informazioni su Avvio rapido guidato di Administration Server.

L'Avvio rapido guidato di Administration Server consente di creare un numero minimo di attività e criteri necessari, regolare un numero minimo di impostazioni, scaricare e installare plug-in per applicazioni Kaspersky gestite e creare pacchetti di installazione di applicazioni Kaspersky gestite. Quando la procedura guidata è in esecuzione, è possibile apportare le seguenti modifiche all'applicazione:

- Scaricare e installare plug-in per applicazioni gestite. Al termine dell'Avvio rapido guidato, l'elenco dei plug-in di gestione installati viene visualizzato nella sezione **Avanzate** → **Dettagli dei plug-in di gestione applicazioni installati** della finestra delle proprietà di Administration Server.

- Creare pacchetti di installazione di applicazioni Kaspersky gestite. Al termine dell'Avvio rapido guidato, i pacchetti di installazione di Network Agent per Windows e delle applicazioni Kaspersky gestite vengono visualizzati nell'elenco **Administration Server** → **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.

- Aggiungere file chiave o immettere codici di attivazione che è possibile distribuire automaticamente ai dispositivi nei gruppi di amministrazione. Al termine dell'Avvio rapido guidato, le informazioni sulle chiavi di licenza vengono visualizzate nell'elenco **Administration Server** → **Licenze di Kaspersky** e nella sezione **Chiavi di licenza** della finestra delle proprietà di Administration Server.

- Configurare l'interazione con Kaspersky Security Network (KSN).

- Impostare l'invio di notifiche tramite e-mail per informare degli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni gestite (per il corretto invio delle notifiche, il servizio Messenger deve essere in esecuzione in Administration Server e in tutti i dispositivi dei destinatari). Al termine dell'Avvio rapido guidato, le impostazioni delle notifiche e-mail vengono visualizzate nella sezione **Notifica** della finestra delle proprietà di Administration Server.

- Configurare le impostazioni di aggiornamento e le impostazioni per la correzione delle vulnerabilità delle applicazioni installate nei dispositivi.

- Creare un criterio di protezione per workstation e server, nonché attività di scansione malware, attività di download degli aggiornamenti e attività di backup dei dati, per il livello superiore della gerarchia dei dispositivi gestiti. Al termine dell'Avvio rapido guidato, le attività create vengono visualizzate nell'elenco **Administration Server** → **Attività**, i criteri corrispondenti ai plug-in per le applicazioni gestite vengono visualizzati nell'elenco **Administration Server** → **Criteri**.

L'Avvio rapido guidato crea criteri per le applicazioni gestite, come Kaspersky Endpoint Security for Windows, a meno che tali criteri non siano già stati creati per il gruppo **Dispositivi gestiti**. L'Avvio rapido guidato crea attività se non esistono attività con gli stessi nomi per il gruppo **Dispositivi gestiti**.

In Administration Console, Kaspersky Security Center richiede automaticamente di eseguire l'Avvio rapido guidato dopo il primo avvio. È anche possibile avviare manualmente l'avvio rapido guidato in qualsiasi momento.

Avvio dell'Avvio rapido guidato di Administration Server

L'applicazione richiede automaticamente di eseguire l'Avvio rapido guidato dopo l'installazione di Administration Server, al momento della prima connessione. È anche possibile avviare manualmente l'avvio rapido guidato in qualsiasi momento.

Per avviare manualmente l'avvio rapido guidato:

1. Nella struttura della console selezionare il nodo **Administration Server**.

2. Nel menu di scelta rapida del nodo selezionare **Tutte le attività** → **Avvio rapido guidato di Administration Server**.

Verrà offerta la possibilità di eseguire la configurazione iniziale di Administration Server. Seguire le istruzioni della procedura guidata.

Se si avvia nuovamente l'Avvio rapido guidato, non è possibile creare nuovamente attività e criteri creati nell'esecuzione precedente della procedura guidata.

Passaggio 1. Configurazione di un server proxy

Specificare le impostazioni di accesso a Internet per Administration Server. È necessario configurare l'accesso a Internet per utilizzare Kaspersky Security Network e per scaricare gli aggiornamenti dei database anti-virus per Kaspersky Security Center e le applicazioni Kaspersky gestite.

Se si desidera utilizzare un server proxy durante la connessione a Internet, selezionare l'opzione **Usa server proxy**. Se questa opzione è selezionata, i campi sono disponibili per l'immissione delle impostazioni. Specificare le seguenti impostazioni per la connessione a un server proxy:

- **Indirizzo**

  Indirizzo del server proxy utilizzato per la connessione di Kaspersky Security Center a Internet.

- **Numero di porta**

  Numero della porta utilizzata per stabilire la connessione al proxy di Kaspersky Security Center.

- **Ignora il server proxy per gli indirizzi locali**

  Non verrà utilizzato alcun server proxy per la connessione ai dispositivi dalla rete locale.

- **Autenticazione server proxy**

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  Questo campo di immissione è disponibile se la casella di controllo **Usa server proxy** è selezionata.

- **Nome utente**

  Account utente con il quale è stata stabilita la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

- **Password**

  Password impostata dall'utente di cui è stato utilizzato l'account per stabilire la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

  Per visualizzare la password immessa, tenere premuto il pulsante **Mostra** per il tempo necessario.

È possibile configurare l'accesso a Internet in un secondo momento, separatamente dall'Avvio rapido guidato.

Passaggio 2. Selezione del metodo di attivazione dell'applicazione

Selezionare una delle seguenti opzioni di attivazione di Kaspersky Security Center:

- **Inserendo il codice di attivazione**

  Codice di attivazione è una sequenza univoca di 20 caratteri alfanumerici. Il codice di attivazione viene inserito per aggiungere una chiave che consente di attivare Kaspersky Security Center. Si riceve il codice di attivazione tramite l'indirizzo e-mail specificato dopo l'acquisto di Kaspersky Security Center.

  Per attivare l'applicazione utilizzando un codice di attivazione, è necessario l'accesso a Internet per stabilire la connessione con i server di attivazione Kaspersky.

  Se è stata selezionata questa opzione di attivazione, è possibile abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

  Se questa opzione è abilitata, la chiave di licenza verrà distribuita automaticamente ai dispositivi gestiti.

  Se questa opzione è disabilitata, è possibile distribuire la chiave di licenza ai dispositivi gestiti in un secondo momento, nel nodo **Licenze di Kaspersky** della struttura di Administration Console.

  Se l'attivazione non ha esito positivo per qualsiasi motivo dopo aver inserito il codice di attivazione, è possibile attivare l'applicazione specificando un file chiave.

- **Specificando un file chiave**

  File chiave: si tratta di un file con estensione key fornito all'utente da Kaspersky. Un file chiave consente di aggiungere una chiave per l'attivazione dell'applicazione.

  I metodi per ottenere il file chiave sono descritti nella sezione seguente: Informazioni sul file chiave.

  Per attivare l'applicazione utilizzando il file chiave, non è necessario connettersi ai server di attivazione di Kaspersky.

  Se è stata selezionata questa opzione di attivazione, è possibile abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

  Se questa opzione è abilitata, la chiave di licenza verrà distribuita automaticamente ai dispositivi gestiti.

  Se questa opzione è disabilitata, è possibile distribuire la chiave di licenza ai dispositivi gestiti in un secondo momento, nel nodo **Licenze di Kaspersky** della struttura di Administration Console.

- **Rimandando l'attivazione dell'applicazione**

  L'applicazione verrà eseguita con la funzionalità di base, senza Mobile Device Management e senza Vulnerability e patch management.

Se si sceglie di rimandare l'attivazione dell'applicazione, è possibile aggiungere successivamente una chiave di licenza in qualsiasi momento.

Passaggio 3. Selezione delle aree di protezione e dei sistemi operativi

Selezionare le aree di protezione e i sistemi operativi in uso nella rete. Quando si selezionano queste opzioni, si specificano i filtri per i plug-in di gestione delle applicazioni e i pacchetti di distribuzione nei server Kaspersky che è possibile scaricare per installarli nei dispositivi client nella rete. Selezionare le opzioni:

- **Aree**

  È possibile selezionare le seguenti aree di protezione:

  - **Workstation**. Selezionare questa opzione se si desidera proteggere le workstation nella rete. Per impostazione predefinita, l'opzione Workstation è selezionata.
  - **File server e archiviazione**. Selezionare questa opzione se si desidera proteggere i file server nella rete.
  - **Dispositivi mobili**. Selezionare questa opzione se si desidera proteggere i dispositivi mobili di proprietà dell'azienda o dei dipendenti aziendali. Se si seleziona questa opzione ma non è stata fornita una licenza con la funzionalità Mobile Device Management, viene visualizzato un messaggio che informa l'utente della necessità di fornire una licenza con la funzionalità Mobile Device Management. Se non viene fornita una licenza, non è possibile utilizzare la funzionalità per i dispositivi mobili.
  - **Virtualizzazione**. Selezionare questa opzione se si desidera proteggere le macchine virtuali nella rete.
  - **Kaspersky Anti-Spam**. Selezionare questa opzione se si desidera proteggere i server di posta aziendali dall'invio di spam, frodi e malware.

- **Sistemi operativi**

  È possibile selezionare le seguenti piattaforme:

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - Altro

  Per informazioni sui sistemi operativi supportati, fare riferimento a Requisiti hardware e software.

È possibile selezionare i pacchetti dell'applicazione Kaspersky nell'elenco dei pacchetti disponibili in un secondo momento, separatamente dall'Avvio rapido guidato. Per semplificare la ricerca dei pacchetti richiesti, è possibile filtrare l'elenco dei pacchetti disponibili in base ai seguenti criteri:

- Zona di protezione
- Tipo di software scaricato (pacchetto di distribuzione, utilità, plug-in o plug-in Web)

- Versione dell'applicazione Kaspersky
- Lingua di localizzazione dell'applicazione Kaspersky

Passaggio 4. Selezione dei plug-in per le applicazioni gestite

Selezionare i plug-in per le applicazioni gestite da installare. Viene visualizzato un elenco dei plug-in che si trovano nei server Kaspersky. L'elenco viene filtrato in base alle opzioni selezionate nel passaggio precedente della procedura guidata. Per impostazione predefinita, un elenco completo include i plug-in di tutte le lingue. Per visualizzare solo il plug-in di una lingua specifica, selezionare la lingua dall'elenco a discesa **Mostra lingua di localizzazione di Administration Console oppure**. L'elenco dei plug-in include le seguenti colonne:

- **Nome applicazione**

  I plug-in sono selezionati in base alle aree di protezione e alle piattaforme, selezionati nel passaggio precedente.

- **Versione applicazione**

  L'elenco include i plug-in di tutte le versioni che si trovano nei server Kaspersky. Per impostazione predefinita, sono selezionati i plug-in delle versioni più recenti.

- **Lingua localizzazione**

  Per impostazione predefinita, la lingua di localizzazione di un plug-in è determinata dalla lingua di Kaspersky Security Center selezionata al momento dell'installazione. È possibile specificare altre lingue nell'elenco a discesa **Mostra lingua di localizzazione di Administration Console oppure**.

Dopo avere selezionato i plug-in, la relativa installazione viene avviata automaticamente in una finestra separata. Per installare alcuni plug-in è necessario accettare le condizioni del Contratto di licenza con l'utente finale. Leggere il testo del Contratto di licenza con l'utente finale, selezionare l'opzione **Accetto i termini del Contratto di licenza** e fare clic sul pulsante **Installa**. Se non si accettano le condizioni del Contratto di licenza con l'utente finale, il plug-in non viene installato.

Al termine dell'installazione, chiudere la finestra di installazione.

È inoltre possibile selezionare i plug-in di gestione in un secondo momento, separatamente dall'Avvio rapido guidato.

Passaggio 5. Download dei pacchetti di distribuzione e creazione dei pacchetti di installazione

Kaspersky Endpoint Security for Windows include uno strumento di criptaggio per le informazioni archiviate nei dispositivi client. Per scaricare un pacchetto di distribuzione di Kaspersky Endpoint Security for Windows valido per le esigenze aziendali, consultare le normative del paese in cui si trovano i dispositivi client dell'organizzazione.

Nella finestra **Tipo di criptaggio** selezionare uno dei seguenti tipi di criptaggio:

- Crittografia avanzata (AES256). Questo tipo di criptaggio utilizza una lunghezza della chiave di 256 bit.
- Crittografia Lite (AES56). Questo tipo di criptaggio utilizza una lunghezza della chiave di 56 bit.

La finestra **Tipo di criptaggio** viene visualizzata solo se è stato selezionato **Workstation** come ambito della protezione e **Microsoft Windows** come piattaforma.

Dopo aver selezionato un tipo di criptaggio, viene visualizzato un elenco dei pacchetti di distribuzione di entrambi i tipi di criptaggio. Nell'elenco viene selezionato un pacchetto di distribuzione con il tipo di criptaggio selezionato. La lingua del pacchetto di distribuzione corrisponde alla lingua di Kaspersky Security Center. Se non esiste un pacchetto di distribuzione di Kaspersky Endpoint Security for Windows per la lingua di Kaspersky Security Center, viene selezionato il pacchetto di distribuzione in inglese.

Nell'elenco è possibile selezionare le lingue del pacchetto di distribuzione tramite l'elenco a discesa **Mostra lingua di localizzazione di Administration Console oppure**.

Le distribuzioni delle applicazioni gestite potrebbero richiedere l'installazione di una versione minima specifica di Kaspersky Security Center.

Nell'elenco è possibile selezionare pacchetti di distribuzione di qualsiasi tipo di criptaggio, diversi da quelli selezionati nella finestra **Tipo di criptaggio**. Dopo aver selezionato un pacchetto di distribuzione per Kaspersky Endpoint Security for Windows, viene avviato il download dei pacchetti di distribuzione, corrispondenti ai componenti e alle piattaforme. È possibile monitorare l'avanzamento del download nella colonna **Stato del download**. Al termine dell'Avvio rapido guidato, i pacchetti di installazione di Network Agent per Windows e delle applicazioni Kaspersky gestite vengono visualizzati nell'elenco **Administration Server → Avanzate → Installazione remota → Pacchetti di installazione**.

Per terminare il download di alcuni pacchetti di distribuzione è necessario accettare il Contratto di licenza con l'utente finale. Quando si fa clic sul pulsante **Accetta**, viene visualizzato il testo del Contratto di licenza con l'utente finale. Per procedere al passaggio successivo della procedura guidata, è necessario accettare i termini e le condizioni del Contratto di licenza con l'utente finale e i termini e le condizioni dell'Informativa sulla privacy di Kaspersky. Selezionare le opzioni relative al Contratto di licenza con l'utente finale e all'Informativa sulla privacy di Kaspersky, quindi fare clic sul pulsante **Accetta tutto**. Se non si accettano i termini e le condizioni, il download del pacchetto viene annullato.

Dopo aver accettato i termini e le condizioni del Contratto di licenza con l'utente finale e i termini e le condizioni dell'Informativa sulla privacy di Kaspersky, il download dei pacchetti di distribuzione prosegue. Al termine del download, viene visualizzato lo stato **Pacchetto di installazione creato**. Successivamente è possibile utilizzare i pacchetti di installazione per distribuire le applicazioni Kaspersky nei dispositivi client.

È possibile creare i pacchetti di installazione manualmente in un secondo momento, separatamente dall'Avvio rapido guidato. Passare a **Administration Server → Avanzate → Installazione remota → Pacchetti di installazione** nella struttura di Administration Console.

Passaggio 6. Configurazione dell'utilizzo di Kaspersky Security Network

È possibile ottenere l'accesso ali database di reputazione di Kaspersky Security Network per garantire una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliorare l'efficacia di alcuni componenti della protezione e ridurre il rischio di falsi positivi.

Leggere l'Informativa KSN, visualizzata nella finestra. Specificare le impostazioni per la trasmissione delle informazioni sulle operazioni di Kaspersky Security Center alla Knowledge Base di Kaspersky Security Network. Selezionare una delle seguenti opzioni:

- **Accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center e le applicazioni gestite installate nei dispositivi client trasferiranno automaticamente i dettagli sull'esecuzione a Kaspersky Security Network. La partecipazione a Kaspersky Security Network garantisce aggiornamenti più rapidi dei database contenenti le informazioni sui virus e sulle altre minacce, assicurando una risposta più rapida alle minacce per la sicurezza emergenti.

- **Non accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center e le applicazioni gestite non forniranno informazioni a Kaspersky Security Network.

  Se si seleziona questa opzione, l'utilizzo di Kaspersky Security Network sarà disabilitato.

Se è stato scaricato il plug-in di Kaspersky Endpoint Security for Windows, si visualizzeranno entrambe le informative KSN, sia l'Informativa KSN per Kaspersky Security Center sia l'informativa KSN per Kaspersky Endpoint Security for Windows. Le informative KSN per altre applicazioni Kaspersky gestite i cui plug-in sono stati scaricati verranno visualizzate in finestre separate e sarà necessario accettare (o non accettare) ciascuna informativa separatamente.

È inoltre possibile configurare l'accesso di Administration Server a Kaspersky Security Network (KSN) in un secondo momento nella finestra delle proprietà di Administration Server di Administration Console.

Passaggio 7. Configurazione delle notifiche e-mail

Configurare l'invio di notifiche relative agli eventi registrati durante l'esecuzione delle applicazioni Kaspersky nei dispositivi gestiti. Queste impostazioni vengono utilizzate come impostazioni predefinite per Administration Server.

Per configurare l'invio di notifiche relative agli eventi che si verificano nelle applicazioni Kaspersky, utilizzare le seguenti impostazioni:

- **Destinatari (indirizzi e-mail)**

  Gli indirizzi e-mail degli utenti a cui l'applicazione invierà le notifiche. È possibile immettere uno o più indirizzi; se si immette più di un indirizzo, separarli con un punto e virgola.

- **Server SMTP**

  L'indirizzo o gli indirizzi dei server di posta dell'organizzazione.

  Se si immette più di un indirizzo, separarli con un punto e virgola. È possibile utilizzare i seguenti valori:

  - Indirizzo IPv4 o IPv6
  - Nome di rete Windows (nome NetBIOS) del dispositivo
  - Nome DNS del server SMTP

- Porta server SMTP

  Numero di porta di comunicazione del server SMTP. Se si utilizzano più server SMTP, la connessione a questi viene stabilita tramite la porta di comunicazione specificata. Il numero di porta predefinito è 25.

- Usa autenticazione ESMTP

  Abilita il supporto dell'autenticazione ESMTP. Quando la casella di controllo è selezionata, nei campi **Nome utente** e **Password** è possibile specificare le impostazioni per l'autenticazione ESMTP. Per impostazione predefinita, questa casella di controllo è deselezionata.

- Impostazioni

  Specificare le seguenti impostazioni:

  - **Oggetto** (oggetto di un messaggio e-mail)
  - **Indirizzo e-mail del mittente**
  - **Impostazioni TLS per server SMTP**

  È possibile specificare le impostazioni TLS per il server SMTP:

  È possibile disabilitare l'utilizzo di TLS, utilizzare TLS se il server SMTP supporta questo protocollo oppure forzare solo l'utilizzo di TLS. Se si sceglie di utilizzare solo TLS, specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. Inoltre, se si sceglie di utilizzare solo TLS, è possibile specificare un certificato per l'autenticazione client nel server SMTP.

  - Cercare un file di certificato del server SMTP:

  È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Administration Server. Kaspersky Security Center verifica se anche il certificato di un server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center non può connettersi a un server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

  - Cercare un file di certificato del client:

  È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. È necessario specificare il certificato e la relativa chiave privata utilizzando uno dei seguenti tipi di certificato:

  - Certificato X-509:

  Specificare il file con il certificato e un file con la chiave privata. Questi file possono essere caricati in qualsiasi ordine. Una volta caricati entrambi i file, specificare la password per il decriptaggio della chiave privata. La password può avere un valore vuoto se la chiave privata non è criptata.

  - Contenitore pkcs12:

  È necessario caricare un singolo file che contenga il certificato e la relativa chiave privata. Quando il file viene caricato, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

È possibile verificare le nuove impostazioni di notifica e-mail facendo clic sul pulsante **Invia messaggio di test**.

È possibile configurare le notifiche degli eventi anche in un secondo momento, separatamente rispetto all'Avvio rapido guidato.

Passaggio 8. Configurazione della gestione degli aggiornamenti

Configurare le impostazioni per la gestione degli aggiornamenti delle applicazioni installate nei dispositivi client.

È possibile configurare queste impostazioni solo se è stata fornita una chiave di licenza con l'opzione Vulnerability e patch management.

Nel gruppo di impostazioni **Cerca e installa gli aggiornamenti** è possibile selezionare una modalità di ricerca e installazione degli aggiornamenti di Kaspersky Security Center:

- **Cerca gli aggiornamenti richiesti**

  L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente, se non ne è presente una.

  Questa opzione è selezionata per impostazione predefinita.

- **Cerca e installa gli aggiornamenti richiesti**

  Se non sono già esistenti, le attività *Trova vulnerabilità e aggiornamenti richiesti* e *Installa aggiornamenti richiesti e correggi vulnerabilità* vengono create automaticamente.

Nel gruppo di impostazioni **Windows Server Update Services** è possibile selezionare la sorgente di sincronizzazione degli aggiornamenti:

- **Utilizzare le sorgenti degli aggiornamenti definite nel criterio di dominio**

  I dispositivi client scaricheranno gli aggiornamenti Windows Update in base alle impostazioni del criterio di dominio. Se non è già esistente, il criterio di Network Agent viene creato automaticamente.

- **Usa Administration Server come server WSUS**

  I dispositivi client scaricheranno gli aggiornamenti Windows Update da Administration Server. Se non sono già esistenti, l'attività *Esegui sincronizzazione di Windows Update* e il criterio di Network Agent vengono creati automaticamente.

È possibile creare le attività *Trova vulnerabilità e aggiornamenti richiesti* e *Installa gli aggiornamenti richiesti e correggi vulnerabilità* separatamente dall'Avvio rapido guidato. Per utilizzare Administration Server come server WSUS, creare l'attività *Esegui sincronizzazione di Windows Update* e selezionare l'opzione **Usa Administration Server come server WSUS** nel criterio di Network Agent.

Passaggio 9. Creazione di una configurazione della protezione iniziale

La finestra **Configura protezione iniziale** visualizza un elenco dei criteri e delle attività creati automaticamente. Vengono creati i seguenti criteri e attività:

- Criterio per Kaspersky Security Center Network Agent
- Criteri per le applicazioni Kaspersky gestite i cui plug-in di gestione sono stati installati in precedenza
- Attività Manutenzione di Administration Server
- Attività Backup dei dati di Administration Server
- Attività Scarica aggiornamenti nell'archivio dell'Administration Server
- Attività Trova vulnerabilità e aggiornamenti richiesti
- Attività Installa aggiornamento

Attendere il completamento della creazione di criteri e attività prima di procedere al passaggio successivo della procedura guidata.

Se è stato scaricato e installato il plug-in per Kaspersky Endpoint Security for Windows 10 Service Pack 1 e versioni successive fino alla 11.0.1, durante la creazione di criteri e attività viene visualizzata una finestra per la configurazione iniziale dell'area attendibile di Kaspersky Endpoint Security for Windows. L'applicazione richiederà di aggiungere i vendor verificati da Kaspersky nell'area attendibile, in modo da escludere le relative applicazioni dalle scansioni per impedire che vengano bloccate accidentalmente. È possibile creare subito esclusioni consigliate o creare un elenco di esclusioni in un secondo momento selezionando i seguenti elementi nella struttura della console: **Criteri** → menu Proprietà di Kaspersky Endpoint Security → **Protezione Minacce Avanzata** → **Area attendibile** → **Impostazioni** → **Aggiungi**. L'elenco delle esclusioni dalla scansione è disponibile per la modifica in qualsiasi momento durante l'utilizzo dell'applicazione.

> Le operazioni sull'area attendibile vengono eseguite tramite gli strumenti integrati in Kaspersky Endpoint Security for Windows. Per istruzioni dettagliate sull'esecuzione delle operazioni e una descrizione delle funzionalità di criptaggio, consultare la Guida in linea di Kaspersky Endpoint Security for Windows.

Per completare la configurazione iniziale dell'area attendibile e tornare alla procedura guidata, fare clic su **OK**.

Fare clic su **Avanti**. Questo pulsante diventa disponibile dopo che tutti i criteri e le attività necessari sono stati creati.

È inoltre possibile creare le attività e i criteri richiesti in un secondo momento, separatamente dall'Avvio rapido guidato.

Passaggio 10. Connessione dei dispositivi mobili

Se è stato abilitato l'ambito della protezione **Dispositivi mobili** nelle impostazioni della procedura guidata, specificare le impostazioni per la connessione dei dispositivi mobili aziendali dell'organizzazione gestita. Se non è stato abilitato l'ambito della protezione **Dispositivi mobili**, questo passaggio viene ignorato.

A questo punto della procedura guidata, effettuare le seguenti operazioni:

- Configurare le porte per la connessione dei dispositivi mobili
- Configurare l'autenticazione di Administration Server
- Creare o gestire i certificati
- Configurare l'emissione, l'aggiornamento automatico e il criptaggio dei certificati di tipo generico
- Creare una regola di spostamento per i dispositivi mobili

Per configurare le porte per la connessione dei dispositivi mobili:

1. Fare clic sul pulsante **Configura** a destra del campo **Connessione dispositivo mobile**.
2. Nell'elenco a discesa selezionare **Configura le porte**.
   Verrà visualizzata la finestra delle proprietà di Administration Server, con la sezione **Porte aggiuntive**.

3. Nella sezione **Porte aggiuntive** è possibile specificare le impostazioni di connessione dei dispositivi mobili:

- **Porta SSL per il server proxy di attivazione**

  Numero di una porta SSL per la connessione di Kaspersky Endpoint Security for Windows ai server di attivazione di Kaspersky.

  Il numero di porta predefinito è 17000.

- **Apri porta per i dispositivi mobili**

  Verrà aperta una porta per la connessione dei dispositivi mobili al server di licensing. È possibile definire il numero della porta e altre impostazioni nei campi sottostanti.

  Per impostazione predefinita, questa opzione è abilitata.

- **Porta per la sincronizzazione del dispositivo mobile**

  Numero della porta utilizzata dai dispositivi mobili per la connessione ad Administration Server e lo scambio dei dati. Il numero di porta predefinito è 13292.

  È possibile assegnare una porta diversa se la porta 13292 viene utilizzata per altri scopi.

- **Porta per l'attivazione del dispositivo mobile**

  Porta per la connessione di Kaspersky Endpoint Security for Android ai server di attivazione di Kaspersky.

  Il numero di porta predefinito è 17100.

- **Porta aperta per i dispositivi di protezione UEFI e i dispositivi KasperskyOS**

  I dispositivi di protezione UEFI possono connettersi all'Administration Server.

- **Porta per i dispositivi di protezione UEFI e i dispositivi KasperskyOS**

  È possibile modificare il numero di porta se l'opzione **Porta aperta per i dispositivi di protezione UEFI e i dispositivi KasperskyOS** è abilitata. Il numero di porta predefinito è 13294.

- **Apri la porta per Prometheus**

  La porta per le richieste di pull di Prometheus. Il numero di porta predefinito è 13296.

4. Fare clic su **OK** per salvare le modifiche e tornare all'Avvio rapido guidato.

È necessario configurare l'autenticazione di Administration Server per i dispositivi mobili e l'autenticazione dei dispositivi mobili per l'Administration Server. Se si desidera, è possibile configurare l'autenticazione in un secondo momento, separatamente rispetto all'Avvio rapido guidato.

Per configurare l'autenticazione di Administration Server per dispositivi mobili:

1. Fare clic sul pulsante **Configura** a destra del campo **Connessione dispositivo mobile**.

2. Nell'elenco a discesa selezionare **Configura l'autenticazione**.

   Verrà visualizzata la finestra delle proprietà di Administration Server, con la sezione **Certificati**.

3. Selezionare l'opzione di autenticazione per i dispositivi mobili nel gruppo di impostazioni **Autenticazione Administration Server da parte dei dispositivi mobili** e selezionare l'opzione di autenticazione per i dispositivi di protezione UEFI nel gruppo di impostazioni **Autenticazione Administration Server da parte dei dispositivi di protezione UEFI**.

   Quando Administration Server esegue lo scambio dei dati con i dispositivi client, l'autenticazione avviene tramite l'utilizzo di un certificato.

   Per impostazione predefinita, viene utilizzato il certificato creato durante l'installazione di Administration Server. Se si desidera, è possibile aggiungere un nuovo certificato.

Per aggiungere un nuovo certificato (opzione facoltativa):

1. Selezionare **Altro certificato**.

   Viene visualizzato il pulsante **Sfoglia**.

2. Fare clic sul pulsante **Sfoglia**.

3. Nella finestra visualizzata specificare le impostazioni del certificato:

   - Tipo di certificato

     Nell'elenco a discesa è possibile selezionare un tipo di certificato:

     - **Certificato X.509**. Se questa opzione è selezionata, è necessario specificare la chiave privata di un certificato e un certificato aperto:
       - **Chiave privata (.prk, .pem)**. In questo campo fare clic sul pulsante **Sfoglia** per specificare la chiave privata di un certificato nel formato PKCS #8 (*.prk).
       - **Chiave pubblica (.cer)**. In questo campo fare clic sul pulsante **Sfoglia** per specificare una chiave pubblica nel formato PEM (*.cer).
     - **Contenitore PKCS #12**. Se si seleziona questa opzione è possibile specificare un file di certificato nel formato P12 o PFX facendo clic sul pulsante **Sfoglia** e compilando il campo **File di certificato**.

   - Ora di attivazione:

     - Immediatamente

       Dopo aver fatto clic su **OK** il certificato corrente verrà sostituito immediatamente con il nuovo.

       I dispositivi mobili connessi in precedenza non saranno in grado di connettersi ad Administration Server.

     - Al termine di questo periodo (giorni)

       Se si seleziona questa opzione, verrà generato un certificato di riserva. Il certificato corrente verrà sostituito con il nuovo dopo il numero di giorni specificato. La data effettiva del certificato di riserva viene visualizzata nella sezione **Certificati**.

       È consigliabile pianificare preventivamente la riemissione. Il certificato di riserva deve essere scaricato nei dispositivi mobili prima della scadenza del periodo specificato. In seguito alla sostituzione del certificato corrente con il nuovo, i dispositivi mobili connessi in precedenza che non dispongono del certificato di riserva non saranno in grado di connettersi ad Administration Server.

4. Fare clic sul pulsante **Proprietà** per visualizzare le impostazioni del certificato di Administration Server selezionato.

Per riemettere un certificato emesso tramite Administration Server:

1. Selezionare **Certificato emesso tramite Administration Server**.
2. Fare clic sul pulsante **Riemetti**.
3. Nella finestra visualizzata specificare le seguenti impostazioni:

   - Indirizzo di connessione:

     - Usa l'indirizzo di connessione precedente

L'indirizzo di Administration Server a cui si connettono i dispositivi mobili non viene modificato.

Questa opzione è selezionata per impostazione predefinita.

- **Modifica l'indirizzo di connessione in**

  Se si desidera che i dispositivi mobili si connettano a un indirizzo diverso, specificare l'indirizzo attinente in questo campo.

  Se l'indirizzo per la connessione del dispositivo mobile è stato modificato, è necessario rilasciare un nuovo certificato. Il certificato precedente diventa non valido in tutti i dispositivi mobili connessi. I dispositivi connessi in precedenza non saranno in grado di connettersi ad Administration Server e diventeranno quindi non gestiti.

- Ora di attivazione:

  - **Immediatamente**

    Dopo aver fatto clic su **OK** il certificato corrente verrà sostituito immediatamente con il nuovo.

    I dispositivi mobili connessi in precedenza non saranno in grado di connettersi ad Administration Server.

  - **Al termine di questo periodo (giorni)**

    Se si seleziona questa opzione, verrà generato un certificato di riserva. Il certificato corrente verrà sostituito con il nuovo dopo il numero di giorni specificato. La data effettiva del certificato di riserva viene visualizzata nella sezione **Certificati**.

    È consigliabile pianificare preventivamente la riemissione. Il certificato di riserva deve essere scaricato nei dispositivi mobili prima della scadenza del periodo specificato. In seguito alla sostituzione del certificato corrente con il nuovo, i dispositivi mobili connessi in precedenza che non dispongono del certificato di riserva non saranno in grado di connettersi ad Administration Server.

4. Fare clic su **OK** per salvare le modifiche e tornare alla finestra **Certificati**.

5. Fare clic su **OK** per salvare le modifiche e tornare all'Avvio rapido guidato.

Per configurare l'emissione, l'aggiornamento automatico e il criptaggio dei certificati di tipo generico per l'identificazione dei dispositivi mobili da parte di Administration Server:

1. Fare clic sul pulsante **Configura** a destra del campo **Autenticazione dispositivo mobile**.

   Viene visualizzata la finestra **Regole di emissione certificati**, che visualizza la sezione **Emissione di certificati mobili**.

2. Se necessario, specificare le seguenti impostazioni nella sezione **Impostazioni di emissione**:

   - **Durata del certificato (giorni)**

     Durata del certificato in giorni. La durata predefinita di un certificato è di 365 giorni. Alla scadenza di questo periodo, il dispositivo mobile non sarà in grado di connettersi ad Administration Server.

   - **Origine certificato**

     Selezionare l'origine dei certificati di tipo generico per i dispositivi mobili: i certificati vengono emessi da Administration Server o specificati manualmente.

     Se è stata configurata l'integrazione con infrastruttura a chiave pubblica (PKI) nella sezione **Integrazione con PKI** è possibile modificare i modelli di certificato. In questo caso, sono disponibili i seguenti campi di selezione del modello:

   - **Modello predefinito**

     Utilizzare un certificato emesso da un'origine di certificati esterna (Centro di certificazione) in base al modello predefinito.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Altro modello**

     Selezionare un modello utilizzato per emettere i certificati. È possibile selezionare i modelli di certificato nel dominio. Il pulsante **Aggiorna elenco** consente di aggiornare l'elenco dei modelli di certificato.

3. Se necessario, specificare le seguenti impostazioni per l'emissione automatica dei certificati nella sezione **Impostazioni degli aggiornamenti automatici**:

   - **Rinnova quando la scadenza del certificato è prevista tra (giorni)**

     Il numero di giorni rimanenti prima della scadenza del certificato corrente durante i quali Administration Server deve emettere un nuovo certificato. Se ad esempio il valore del campo è 4, Administration Server emette un nuovo certificato quattro giorni prima della scadenza del certificato corrente. Il valore predefinito è 7.

   - **Riemetti automaticamente il certificato se possibile**

     Selezionare questa opzione per riemettere automaticamente un certificato per il numero di giorni specificato nel campo **Rinnova quando la scadenza del certificato è prevista tra (giorni)**. Se un certificato è stato definito manualmente, non può essere rinnovato automaticamente e l'opzione abilitata non funzionerà.

     Per impostazione predefinita, questa opzione è disabilitata.

   I certificati vengono riemessi automaticamente da un'autorità di certificazione.

4. Se necessario, nella sezione delle impostazioni **Protezione tramite password** specificare le impostazioni per il decriptaggio dei certificati durante l'installazione.

   Selezionare l'opzione **Richiedi la password durante l'installazione del certificato** per richiedere all'utente la password durante l'installazione del certificato in un dispositivo mobile. La password viene utilizzata solo una volta, durante l'installazione del certificato nel dispositivo mobile.

   La password verrà automaticamente generata e inviata da Administration Server all'indirizzo e-mail specificato. È possibile specificare l'indirizzo e-mail dell'utente o il proprio indirizzo e-mail, se si desidera utilizzare un altro metodo per inviare la password all'utente.

   È possibile utilizzare il dispositivo di scorrimento per specificare il numero di caratteri contenuti nella password per il decriptaggio del certificato.

   L'opzione per la richiesta della password è ad esempio necessaria per la protezione di un certificato condiviso in un pacchetto di installazione indipendente di Kaspersky Endpoint Security for Android. La protezione tramite password impedisce a un utente malintenzionato di ottenere l'accesso al certificato condiviso tramite il furto del pacchetto di installazione indipendente dal Server Web di Kaspersky Security Center.

   Se questa opzione è deselezionata, il certificato viene decriptato automaticamente durante l'installazione e all'utente non viene richiesta alcuna password. Per impostazione predefinita, questa opzione è disabilitata.

5. Fare clic su **OK** per salvare le modifiche e tornare alla finestra Avvio rapido guidato.

   Fare clic sul pulsante **Annulla** per tornare all'Avvio rapido guidato senza salvare le modifiche.

Per abilitare la funzione di spostamento dei dispositivi mobili in un gruppo di amministrazione selezionato,

Nel campo **Spostamento automatico dei dispositivi mobili** selezionare l'opzione **Crea una regola di spostamento per i dispositivi mobili**.

Se l'opzione **Crea una regola di spostamento per i dispositivi mobili** è selezionata, l'applicazione crea automaticamente una regola di spostamento che sposta i dispositivi iOS e Android nel gruppo **Dispositivi gestiti**:

- Con sistemi operativi Android in cui sono installati Kaspersky Endpoint Security for Android e un certificato mobile
- Con sistemi operativi iOS in cui è installato il profilo MDM iOS con un certificato condiviso

Se una regola esiste già, l'applicazione non la crea nuovamente.

Per impostazione predefinita, questa opzione è disabilitata.

Kaspersky non supporta più Kaspersky Safe Browser.

Passaggio 11. Download degli aggiornamenti

Gli aggiornamenti per i database anti-virus per Kaspersky Security Center e le applicazioni Kaspersky gestite vengono scaricati automaticamente. Gli aggiornamenti vengono scaricati dai server Kaspersky.

Per scaricare gli aggiornamenti separatamente dall'Avvio rapido guidato, creare e configurare l'attività *Scarica gli aggiornamenti nell'archivio dell'Administration Server*.

Passaggio 12. Device discovery

La finestra **Polling della rete** visualizza le informazioni sullo stato del polling della rete eseguito da Administration Server.

È possibile visualizzare i dispositivi della rete rilevati da Administration Server e ottenere assistenza sull'utilizzo della finestra **Device discovery** facendo clic sui collegamenti nella parte inferiore della finestra.

È possibile eseguire il polling della rete in un secondo momento, separatamente dall'Avvio rapido guidato. Utilizzare Administration Console per configurare il polling dei domini di Windows, Active Directory, degli intervalli IP e delle reti IPv6.

Passaggio 13. Chiusura dell'Avvio rapido guidato

Nella finestra di completamento dell'Avvio rapido guidato selezionare l'opzione **Esegui l'installazione remota guidata** se si desidera avviare l'installazione automatica delle applicazioni anti-virus e/o di Network Agent nei dispositivi della rete.

Per completare la procedura guidata, fare clic sul pulsante **Fine**.

Configurazione della connessione di Administration Console ad Administration Server

Administration Console è connessa ad Administration Server tramite la porta SSL TCP 13291. La stessa porta può essere utilizzata dagli oggetti di automazione klakaut.

La porta TCP 14000 può essere utilizzata per connettere Administration Console, punti di distribuzione, Administration Server secondari e oggetti di automazione klakaut, nonché per ricevere i dati dai dispositivi client.

In genere, la porta SSL TCP 13000 può essere utilizzata solo da Network Agent, un Administration Server secondario e dall'Administration Server primario nella rete DMZ. In alcuni casi può essere necessario connettere Administration Console tramite la porta SSL 13000:

- Se è probabile che venga utilizzata una singola porta SSL sia per Administration Console che per altre attività (ricezione dei dati dai dispositivi client, connessione di punti di distribuzione, connessione di Administration Server secondari).
- Se un oggetto di automazione klakaut non è connesso ad Administration Server direttamente, bensì tramite un punto di distribuzione nella rete perimetrale.

Per consentire la connessione di Administration Console tramite la porta 13000:

1. Aprire il Registro di sistema del dispositivo in cui è installato Administration Server (ad esempio, in locale, utilizzando il comando regedit dal menu **Start** → **Esegui**).
2. Passare al seguente hive:
   - Per i sistemi a 32 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Per i sistemi a 64 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Per la chiave LP_ConsoleMustUsePort13291 (DWORD) impostare il valore 00000000.

   Il valore predefinito specificato per questa chiave è 1.
4. Riavviare il servizio Administration Server.

A questo punto, sarà possibile connettere Administration Console ad Administration Server tramite la porta 13000.

Configurazione delle impostazioni di accesso a Internet per Administration Server

È necessario configurare l'accesso a Internet per utilizzare Kaspersky Security Network e per scaricare gli aggiornamenti dei database anti-virus per Kaspersky Security Center e le applicazioni Kaspersky gestite.

Per specificare le impostazioni di accesso a Internet per Administration Server:

1. Nella struttura della console selezionare il nodo **Administration Server %s**.
2. Dal menu di scelta rapida dell'Administration Server selezionare **Proprietà**.

3. Nella finestra delle proprietà di Administration Server, passare a **Avanzate** → **Configurazione dell'accesso a Internet**.

4. Se si desidera utilizzare un server proxy durante la connessione a Internet, selezionare l'opzione **Usa server proxy**. Se questa opzione è selezionata, i campi sono disponibili per l'immissione delle impostazioni. Specificare le seguenti impostazioni per la connessione a un server proxy:

   - **Indirizzo**

     Indirizzo del server proxy utilizzato per la connessione di Kaspersky Security Center a Internet.

   - **Numero di porta**

     Numero della porta utilizzata per stabilire la connessione al proxy di Kaspersky Security Center.

   - **Ignora il server proxy per gli indirizzi locali**

     Non verrà utilizzato alcun server proxy per la connessione ai dispositivi dalla rete locale.

   - **Autenticazione server proxy**

     Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

     Questo campo di immissione è disponibile se la casella di controllo **Usa server proxy** è selezionata.

   - **Nome utente**

     Account utente con il quale è stata stabilita la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

   - **Password**

     Password impostata dall'utente di cui è stato utilizzato l'account per stabilire la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

     Per visualizzare la password immessa, tenere premuto il pulsante **Mostra** per il tempo necessario.

È inoltre possibile configurare l'accesso a Internet utilizzando l'Avvio rapido guidato.

Connessione dei dispositivi fuori sede

Questa sezione descrive come connettere i dispositivi fuori sede (cioè i dispositivi gestiti che si trovano all'esterno della rete principale) ad Administration Server.

Scenario: Connessione dei dispositivi fuori sede tramite un gateway di connessione

Questo scenario descrive come connettere i dispositivi gestiti che si trovano all'esterno della rete principale ad Administration Server.

Prerequisiti

Lo scenario prevede i seguenti prerequisiti:

- Una rete perimetrale deve essere organizzata nella rete dell'organizzazione.
- Kaspersky Security Center Administration Server deve essere distribuito nella rete aziendale.

Passaggi

Questo scenario procede per fasi:

1. **Selezione di un dispositivo client nella rete perimetrale**

   Questo dispositivo verrà utilizzato come gateway di connessione. Il dispositivo selezionato deve soddisfare i requisiti per i gateway di connessione.

2. **Installazione di Network Agent nel ruolo di gateway di connessione**

   È consigliabile utilizzare un'installazione locale per installare Network Agent nel dispositivo selezionato.

   Per impostazione predefinita, il file di installazione si trova in: \\<nome server>\KLSHARE\PkgInst\NetAgent_<numero versione>

   Nella finestra **Gateway di connessione** dell'Installazione guidata di Network Agent selezionare **Utilizzare Network Agent come gateway di connessione nella rete perimetrale**. Questa modalità attiva contemporaneamente il ruolo del gateway di connessione e indica a Network Agent di attendere le connessioni da Administration Server anziché stabilire connessioni ad Administration Server.

   In alternativa, è possibile installare Network Agent in un dispositivo Linux e configurare Network Agent in modo che funga da gateway di connessione, ma è necessario prestare attenzione all'elenco delle limitazioni di Network Agent in esecuzione nei dispositivi Linux.

3. **Autorizzazione delle connessioni nei firewall sul gateway di connessione**

   Per assicurarsi che Administration Server sia effettivamente in grado di connettersi al gateway di connessione nella rete perimetrale, consentire le connessioni alla porta TCP 13000 in tutti i firewall tra Administration Server e il gateway di connessione.

   Se il gateway di connessione non dispone di un indirizzo IP reale in Internet ma si trova invece dietro una configurazione NAT (Network Address Translation), configurare una regola per inoltrare le connessioni tramite NAT.

4. **Creazione di un gruppo di amministrazione per i dispositivi esterni**

   Creare un nuovo gruppo nel gruppo **Dispositivi gestiti**. Questo nuovo gruppo conterrà dispositivi gestiti esterni.

5. **Connessione del gateway di connessione ad Administration Server**

Il gateway di connessione configurato è in attesa di una connessione da Administration Server. Tuttavia, Administration Server non elenca il dispositivo con il gateway di connessione tra i dispositivi gestiti. Questo è dovuto al fatto che il gateway di connessione non ha tentato di stabilire una connessione ad Administration Server. È pertanto necessaria una procedura speciale per garantire che Administration Server avvii una connessione al gateway di connessione.

Procedere come segue:

1. Aggiungere il gateway di connessione come punto di distribuzione.
2. Spostare il gateway di connessione dal gruppo **Dispositivi non assegnati** al gruppo creato per i dispositivi esterni.

Il gateway di connessione è stato connesso e configurato.

6 **Connessione dei dispositivi desktop esterni ad Administration Server**

Solitamente i dispositivi desktop esterni non vengono spostati all'interno del perimetro. Pertanto è necessario configurarli per eseguire la connessione ad Administration Server tramite il gateway durante l'installazione di Network Agent.

7 **Configurazione degli aggiornamenti per i computer dispositivi esterni**

Se gli aggiornamenti delle applicazioni di protezione sono configurati per il download da Administration Server, i dispositivi esterni scaricano gli aggiornamenti tramite il gateway di connessione. Questo comporta due svantaggi:

- Si tratta di traffico non necessario che occupa la larghezza di banda del canale di comunicazione Internet aziendale.
- Questo non è necessariamente il modo più rapido per ottenere aggiornamenti. È molto probabile che per i dispositivi esterni sarebbe più economico e veloce ricevere gli aggiornamenti dai server di aggiornamento Kaspersky.

Procedere come segue:

1. Spostare tutti i dispositivi esterni nel gruppo di amministrazione separato creato in precedenza.
2. Escludere il gruppo con i dispositivi esterni dall'attività di aggiornamento.
3. Creare un'attività di aggiornamento separata per il gruppo con i dispositivi esterni.

8 **Connessione dei laptop mobili ad Administration Server**

I laptop mobili a volte sono all'interno della rete e altre volte all'esterno della rete. Per una gestione efficace, è necessario che questi si connettano ad Administration Server in modo diverso a seconda della posizione. Per un utilizzo efficiente del traffico, è inoltre necessario che ricevano gli aggiornamenti da origini diverse a seconda della posizione.

È necessario configurare le regole per gli utenti fuori sede: profili di connessione e descrizioni dei percorsi di rete. Ciascuna regola definisce l'istanza di Administration Server a cui i laptop mobili devono connettersi a seconda della posizione e l'istanza di Administration Server da cui devono ricevere gli aggiornamenti.

Scenario: connessione di dispositivi fuori sede tramite un Administration Server secondario in DMZ

Se si desidera connettere i dispositivi gestiti che si trovano all'esterno della rete principale ad Administration Server, è possibile utilizzare un Administration Server secondario situato nella rete perimetrale (DMZ).

Prerequisiti

Prima di iniziare, verificare di avere:

- Una rete perimetrale deve essere organizzata nella rete dell'organizzazione.
- Kaspersky Security Center Administration Server è distribuito nella rete interna dell'organizzazione.

Passaggi

Questo scenario procede per fasi:

1. **Selezione di un dispositivo client nella rete perimetrale**

   Nella DMZ, selezionare un dispositivo client che verrà utilizzato come Administration Server secondario.

2. **Installazione di Kaspersky Security Center Administration Server**

   Installare Kaspersky Security Center Administration Server in questo dispositivo client.

3. **Creazione di una gerarchia di Administration Server**

   Se si posiziona un Administration Server secondario in DMZ, l'Administration Server secondario deve ricevere una connessione dall'Administration Server primario. A tale scopo, aggiungere un nuovo Administration Server come secondario in modo che l'Administration Server primario si connetta all'Administration Server secondario tramite la porta 13000. Quando si combinano due Administration Server in una gerarchia, verificare che la porta 13291 sia accessibile in entrambi gli Administration Server. Administration Console si connette a un Administration Server tramite la porta 13291.

4. **Connessione dei dispositivi gestiti fuori sede all'Administration Server secondario**

   È possibile connettere i dispositivi fuori sede ad Administration Server in DMZ nello stesso modo in cui viene stabilita la connessione tra Administration Server e i dispositivi gestiti che si trovano nella rete principale. I dispositivi gestiti fuori sede avviano la connessione tramite la porta 13000.

Informazioni sulla connessione dei dispositivi fuori sede

Alcuni dispositivi gestiti si trovano sempre all'esterno della rete principale (ad esempio dispositivi nelle filiali dell'azienda; chioschi, bancomat e terminali installati in vari punti vendita; dispositivi negli uffici domestici dei dipendenti). Alcuni dispositivi si spostano di tanto in tanto al di fuori del perimetro (ad esempio i laptop degli utenti che visitano le filiali regionali o l'ufficio di un cliente).

È comunque necessario monitorare e gestire la protezione dei dispositivi fuori sede: ricevere informazioni effettive sul relativo stato della protezione e mantenere aggiornate le applicazioni di protezione in essi installate. Questa prassi è necessaria perché se ad esempio uno di questi dispositivi viene compromesso mentre è all'esterno della rete principale, potrebbe diventare una piattaforma per la propagazione delle minacce non appena si connette alla rete principale. Per connettere i dispositivi fuori sede ad Administration Server è possibile utilizzare due metodi:

- Gateway di connessione nella rete perimetrale

  Visualizzare lo schema del traffico dati: Administration Server nella LAN, dispositivi gestiti in Internet, gateway di connessione in uso

- Administration Server nella rete perimetrale

  Visualizzare lo schema del traffico dati: Administration Server nella rete perimetrale, dispositivi gestiti in Internet

Un gateway di connessione nella rete perimetrale

Un metodo consigliato per connettere i dispositivi fuori sede ad Administration Server è quello di organizzare una rete perimetrale nella rete dell'organizzazione e di installare un gateway di connessione nella rete perimetrale. I dispositivi esterni si connetteranno al gateway di connessione e Administration Server all'interno della rete avvierà una connessione ai dispositivi tramite il gateway di connessione.

Rispetto all'altro metodo, questo è più sicuro:

- Non è necessario aprire l'accesso ad Administration Server dall'esterno della rete.
- Un gateway di connessione compromesso non rappresenta un rischio elevato per la sicurezza dei dispositivi di rete. Un gateway di connessione in realtà non gestisce nulla autonomamente e non stabilisce alcuna connessione.

Inoltre, un gateway di connessione non richiede molte risorse hardware.

Tuttavia, questo metodo ha un processo di configurazione più complicato:

- Per fare in modo che un dispositivo funga da gateway di connessione nella rete perimetrale, è necessario installare Network Agent e connetterlo ad Administration Server in un modo specifico.
- Non sarà possibile utilizzare lo stesso indirizzo per la connessione ad Administration Server per tutte le situazioni. Dall'esterno del perimetro sarà necessario utilizzare non solo un indirizzo diverso (indirizzo del gateway di connessione), ma anche una modalità di connessione diversa: tramite un gateway di connessione.
- È inoltre necessario definire impostazioni di connessione diverse per i laptop in posizioni diverse.

Per aggiungere un gateway di connessione a una rete configurata in precedenza:

1. Installare Network Agent in modalità gateway di connessione.
2. Reinstallare Network Agent nei dispositivi che si desidera connettere al gateway di connessione appena aggiunto.

Administration Server nella rete perimetrale

Un altro metodo consiste nell'installare un singolo Administration Server nella rete perimetrale.

Questa configurazione è meno sicura rispetto all'altro metodo. Per gestire laptop esterni in questo caso, Administration Server deve accettare connessioni da qualsiasi indirizzo in Internet. Gestirà comunque tutti i dispositivi nella rete interna, ma dalla rete perimetrale. Pertanto, un server compromesso potrebbe causare un'ingente quantità di danni, nonostante la bassa probabilità che tale evento si verifichi.

Il rischio si riduce notevolmente se Administration Server nella rete perimetrale non gestisce i dispositivi nella rete interna. Tale configurazione può essere utilizzata ad esempio da un fornitore di servizi per gestire i dispositivi dei clienti.

Potrebbe essere opportuno utilizzare questo metodo nei seguenti casi:

- Se si ha familiarità con l'installazione e la configurazione di Administration Server e non si desidera eseguire un'altra procedura per installare e configurare un gateway di connessione.
- Se è necessario gestire più dispositivi. La capacità massima di Administration Server è di 100.000 dispositivi, mentre un gateway di connessione può supportare fino a 10.000 dispositivi.

Questa soluzione presenta anche possibili difficoltà:

- Administration Server richiede più risorse hardware e un altro database.
- Le informazioni sui dispositivi verranno archiviate in due database non correlati (per Administration Server all'interno della rete e un altro nella rete perimetrale), il che complica il monitoraggio.
- Per gestire tutti i dispositivi, Administration Server deve trovarsi in una gerarchia, il che complica non solo il monitoraggio ma anche la gestione. Un'istanza dell'Administration Server secondario impone limitazioni alle possibili strutture dei gruppi di amministrazione. È necessario decidere come e quali attività e criteri distribuire a un'istanza dell'Administration Server secondario.
- La configurazione di dispositivi esterni per l'utilizzo di Administration Server nella rete perimetrale dall'esterno e per l'utilizzo dell'Administration Server primario dall'interno non è più semplice della configurazione per l'utilizzo di una connessione condizionale tramite un gateway.
- Elevati rischi per la sicurezza. Un'istanza di Administration Server compromessa semplifica la compromissione dei laptop gestiti. In tal caso, gli hacker devono solo attendere che uno dei laptop torni nella rete aziendale in modo da poter proseguire l'attacco nella LAN.

Connessione dei dispositivi desktop esterni ad Administration Server

I dispositivi desktop che si trovano sempre all'esterno della rete principale (ad esempio dispositivi nelle filiali dell'azienda; chioschi, bancomat e terminali installati in vari punti vendita; dispositivi negli uffici domestici dei dipendenti) non possono essere collegati direttamente ad Administration Server. Devono essere collegati ad Administration Server tramite un gateway di connessione installato nella rete perimetrale. Questa configurazione viene eseguita durante l'installazione di Network Agent in tali dispositivi.

Per connettere dispositivi desktop esterni ad Administration Server:

1. Creare un nuovo pacchetto di installazione per Network Agent.
2. Aprire le proprietà del pacchetto di installazione creato e passare alla sezione **Avanzate**, quindi selezionare l'opzione **Esegui la connessione ad Administration Server utilizzando un gateway di connessione**.

   L'impostazione **Esegui la connessione ad Administration Server utilizzando un gateway di connessione** non è compatibile con l'impostazione **Utilizzare Network Agent come gateway di connessione nella rete perimetrale**. Non è possibile abilitare entrambe queste impostazioni contemporaneamente.

3. In **Indirizzo gateway connessione** specificare l'indirizzo pubblico del gateway di connessione.

   Se il gateway di connessione si trova dietro una configurazione NAT (Network Address Translation) e non dispone di un proprio indirizzo pubblico, configurare una regola del gateway NAT per inoltrare le connessioni dall'indirizzo pubblico all'indirizzo interno del gateway di connessione.

4. Creare un pacchetto di installazione indipendente basato sul pacchetto di installazione creato.

5. Distribuire il pacchetto di installazione indipendente ai dispositivi di destinazione in formato elettronico o tramite un'unità rimovibile.

6. Installare Network Agent dal pacchetto indipendente.

I dispositivi desktop esterni sono connessi ad Administration Server.

Informazioni sui profili di connessione per gli utenti fuori sede

Gli utenti fuori sede con computer portatili (di seguito denominati anche "dispositivi") possono aver bisogno di modificare il metodo di connessione a un Administration Server o passare da un Administration Server all'altro a seconda della posizione corrente del dispositivo nella rete aziendale.

I profili di connessione sono supportati solo per i dispositivi che eseguono Windows e macOS.

Utilizzo di differenti indirizzi di un singolo Administration Server

I dispositivi con Network Agent installato possono connettersi all'Administration Server dalla rete Intranet dell'organizzazione o da Internet. Questa situazione può richiedere l'utilizzo da parte di Network Agent di differenti indirizzi per la connessione ad Administration Server: l'indirizzo esterno dell'Administration Server per la connessione Internet e l'indirizzo interno dell'Administration Server per la connessione dalla rete interna.

A tale scopo, è necessario aggiungere un profilo (per la connessione ad Administration Server da Internet) al criterio di Network Agent. Aggiungere il profilo nelle proprietà del criterio (sezione **Connettività**, sottosezione **Profili connessione**). Nella finestra di creazione del profilo è necessario disabilitare l'opzione **Usa per ricevere solo aggiornamenti** e selezionare l'opzione **Sincronizza le impostazioni di connessione con le impostazioni di Administration Server specificate nel profilo**. Se si utilizza un gateway di connessione per accedere ad Administration Server (ad esempio, in una configurazione di Kaspersky Security Center come quella descritta in Accesso a Internet: Network Agent come gateway nella rete perimetrale), è necessario specificare l'indirizzo del gateway di connessione nel campo corrispondente del profilo di connessione.

Passaggio da un Administration Server all'altro a seconda della rete corrente

Se l'organizzazione ha più sedi con diversi Administration Server e alcuni dispositivi con Network Agent installato si spostano tra di esse, è necessario che Network Agent si connetta all'Administration Server della rete locale nella sede in cui si trova attualmente il dispositivo.

In questo caso, è necessario creare un profilo per la connessione ad Administration Server nelle proprietà del criterio di Network Agent per ciascuna delle sedi, tranne che per la sede principale in cui si trova l'Administration Server principale originale. È necessario specificare gli indirizzi di Administration Server nei profili di connessione e abilitare o disabilitare l'opzione **Usa per ricevere solo aggiornamenti**:

- Selezionare l'opzione se è necessario sincronizzare Network Agent con l'Administration Server principale e utilizzare il server locale solo per scaricare gli aggiornamenti.

- Disabilitare questa opzione se è necessario che Network Agent sia completamente gestito dall'Administration Server locale.

Sarà quindi necessario impostare le condizioni per il passaggio ai nuovi profili creati: almeno una condizione per ciascuna delle sedi, tranne che per la sede principale. Lo scopo di ogni condizione consiste nel rilevamento degli elementi che sono specifici per l'ambiente di rete di una sede. Se una condizione è vera, il profilo corrispondente viene attivato. Se nessuna delle condizioni è vera, Network Agent passa all'Administration Server principale.

Creazione di un profilo di connessione per gli utenti fuori sede

Un profilo di connessione di Administration Server è disponibile solo nei dispositivi che eseguono Windows e macOS.

Per creare un profilo per la connessione di Network Agent ad Administration Server per gli utenti fuori sede:

1. Nella struttura della console selezionare il gruppo di amministrazione che contiene i dispositivi client in cui è necessario creare un profilo per la connessione di Network Agent ad Administration Server.
2. Eseguire una delle seguenti operazioni:
   - Se si desidera creare un profilo di connessione per tutti i dispositivi del gruppo, selezionare un criterio di Network Agent nell'area di lavoro del gruppo, nella scheda **Criteri**. Aprire la finestra delle proprietà del criterio selezionato.
   - Se si desidera creare un profilo di connessione per un dispositivo in un gruppo, selezionare il dispositivo nell'area di lavoro del gruppo, nella scheda **Dispositivi**, ed eseguire le seguenti azioni:
     a. Aprire la finestra delle proprietà del dispositivo selezionato.
     b. Nella sezione **Applicazioni** della finestra delle proprietà del dispositivo selezionare Network Agent.
     c. Aprire la finestra delle proprietà del Network Agent.
3. Nella finestra delle proprietà, nella sezione **Connettività** selezionare la sottosezione **Profili connessione**.
4. Nel gruppo di impostazioni **Profili connessione di Administration Server** fare clic sul pulsante **Aggiungi**.

   Per impostazione predefinita, l'elenco dei profili di connessione contiene i profili <Modalità offline> e <Administration Server principale>. I profili non possono essere modificati o rimossi.

   Il profilo <Modalità offline> non specifica alcun server per la connessione. Di conseguenza, quando viene eseguito il passaggio a questo profilo, Network Agent non tenta di connettersi ad alcun Administration Server, mentre le applicazioni installate nei dispositivi client sono eseguite con i criteri di lavoro fuori sede. Il profilo <Modalità offline> può essere utilizzato se i dispositivi sono disconnessi dalla rete.

   Il profilo <Administration Server principale> specifica la connessione per l'Administration Server che è stato selezionato durante l'installazione di Network Agent. Il profilo <Administration Server principale> viene applicato quando un dispositivo si riconnette all'Administration Server principale dopo l'esecuzione in una rete esterna per un determinato periodo.

5. Nella finestra **Nuovo profilo** visualizzata configurare il profilo di connessione:

- Nome profilo

  Nel campo di immissione è possibile visualizzare o modificare il nome del profilo di connessione.

- Administration Server

  Indirizzo di Administration Server a cui il dispositivo client deve connettersi durante l'attivazione del profilo.

- Porta

  Il numero di porta utilizzato per la connessione.

- Porta SSL

  Il numero della porta per la connessione tramite il protocollo SSL.

- Usa SSL

  Se questa opzione è abilitata, la connessione viene stabilita tramite una porta sicura utilizzando il protocollo SSL.

  Per impostazione predefinita, questa opzione è abilitata. È consigliabile non disabilitare questa opzione in modo che la connessione rimanga protetta.

- Fare clic sul collegamento **Configura la connessione tramite server proxy** per configurare la connessione tramite un server proxy: Se si desidera utilizzare un server proxy durante la connessione a Internet, selezionare l'opzione **Usa server proxy**. Se questa opzione è selezionata, i campi sono disponibili per l'immissione delle impostazioni. Specificare le seguenti impostazioni per la connessione a un server proxy:

  - Indirizzo server proxy

    Indirizzo del server proxy utilizzato per la connessione di Kaspersky Security Center a Internet.

  - Numero di porta

    Numero della porta utilizzata per stabilire la connessione al proxy di Kaspersky Security Center.

  - Autenticazione server proxy

    Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

    Questo campo di immissione è disponibile se la casella di controllo **Usa server proxy** è selezionata.

  - Nome utente (questo campo è disponibile se l'opzione **Autenticazione server proxy** è selezionata)

Account utente con il quale è stata stabilita la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

- **Password** (questo campo è disponibile se l'opzione **Autenticazione server proxy**)

  Password impostata dall'utente di cui è stato utilizzato l'account per stabilire la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

  Per visualizzare la password immessa, tenere premuto il pulsante **Mostra** per il tempo necessario.

- **Impostazioni gateway di connessione**

  Indirizzo del gateway attraverso cui i dispositivi client si connettono ad Administration Server.

- **Abilita la modalità fuori sede**

  Se questa opzione è abilitata, in caso di utilizzo di questo profilo per la connessione, le applicazioni installate nel dispositivo client utilizzeranno i profili criterio per i dispositivi in modalità fuori sede, nonché i criteri fuori sede. Se non è definito alcun criterio fuori sede per l'applicazione, verrà utilizzato il criterio attivo.

  Se questa opzione è disabilitata, le applicazioni utilizzeranno i criteri attivi.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa per ricevere solo aggiornamenti**

  Se questa opzione è abilitata, il profilo verrà utilizzato solo per il download degli aggiornamenti da parte delle applicazioni installate nel dispositivo client. Per le altre operazioni verrà stabilita la connessione ad Administration Server con le impostazioni di connessione iniziali definite durante l'installazione di Network Agent.

  Per impostazione predefinita, questa opzione è abilitata.

- **Sincronizza le impostazioni di connessione con le impostazioni di Administration Server specificate nel profilo**

  Se questa opzione è abilitata, Network Agent si connette ad Administration Server utilizzando le impostazioni specificate nelle proprietà del profilo.

  Se questa opzione è disabilitata, Network Agent si connette ad Administration Server utilizzando le impostazioni originali specificate durante l'installazione.

  Questa opzione è disponibile se l'opzione **Usa per ricevere solo aggiornamenti** è disabilitata.

  Per impostazione predefinita, questa opzione è disabilitata.

6. Selezionare l'opzione **Abilita la modalità fuori sede quando Administration Server non è disponibile** per consentire alle applicazioni installate in un dispositivo client di utilizzare i profili criterio per i dispositivi in modalità fuori sede, nonché i criteri fuori sede, per qualsiasi tentativo di connessione se Administration Server non è disponibile. Se non è definito alcun criterio fuori sede per l'applicazione, verrà utilizzato il criterio attivo.

Verrà creato un profilo per la connessione di Network Agent ad Administration Server per gli utenti mobili. Quando Network Agent si connette ad Administration Server con questo profilo, le applicazioni installate in un dispositivo client utilizzeranno i criteri per i dispositivi in modalità fuori sede o i criteri fuori sede.

Informazioni sul passaggio di Network Agent ad altri Administration Server

Le impostazioni iniziali della connessione di Network Agent ad Administration Server vengono definite durante l'installazione di Network Agent. Per passare da Network Agent ad altri Administration Server, è possibile utilizzare le regole per il passaggio. Questa funzionalità è supportata solo per i Network Agent installati nei dispositivi che eseguono Windows o macOS.

Le regole per il passaggio possono essere attivate al momento della modifica dei seguenti parametri di rete:

- Indirizzo gateway predefinito.
- Indirizzo IP del server DHCP (Dynamic Host Configuration Protocol).
- Suffisso DNS della subnet.
- Indirizzo IP del server DNS di rete.
- Accessibilità del dominio Windows. Questo parametro è disponibile solo per i dispositivi in cui viene eseguito Windows.
- Indirizzo e maschera della subnet.
- Indirizzo IP del server WINS di rete. Questo parametro è disponibile solo per i dispositivi in cui viene eseguito Windows.
- Nome DNS o NetBIOS del dispositivo client.
- Accessibilità indirizzo di connessione SSL.

Se sono state create regole per il passaggio del Network Agent ad altri Administration Server, Network Agent risponde alle modifiche dei parametri di rete nel modo seguente:

- Se le impostazioni di rete sono conformi a una delle regole create, Network Agent si connette all'Administration Server specificato in questa regola. Le applicazioni installate nei dispositivi client passano ai criteri fuori sede, a condizione che tale comportamento sia abilitato da una regola.
- Se non è applicabile alcuna regola, Network Agent ripristina le impostazioni predefinite della connessione all'Administration Server specificato durante l'installazione. Per le applicazioni installate nei dispositivi client vengono ripristinati i criteri attivi.
- Se l'Administration Server non è accessibile, Network Agent utilizzerà i criteri fuori sede.

Network Agent passa al criterio fuori sede solo se l'opzione **Abilita la modalità fuori sede quando Administration Server non è disponibile** è abilitata nelle impostazioni del criterio di Network Agent.

Le impostazioni della connessione di Network Agent all'Administration Server vengono salvate in un profilo. Nel profilo di connessione è possibile creare regole per il passaggio dei dispositivi client ai criteri fuori sede, nonché configurare il profilo in modo da utilizzarlo solo per il download degli aggiornamenti.

Creazione di una regola per il passaggio di Network Agent in base al percorso di rete

Il passaggio di Network Agent in base al percorso di rete è disponibile solo nei dispositivi che eseguono Windows e macOS.

Per creare una regola per il passaggio di Network Agent da un Administration Server all'altro in caso di modifiche delle impostazioni di rete:

1. Nella struttura della console selezionare il gruppo di amministrazione che contiene i dispositivi per cui è necessario creare una regola per il passaggio di Network Agent in base alla descrizione del percorso di rete.
2. Eseguire una delle seguenti operazioni:
   - Se si desidera creare una regola per tutti i dispositivi del gruppo, passare all'area di lavoro del gruppo e selezionare un criterio di Network Agent nella scheda **Criteri**. Aprire la finestra delle proprietà del criterio selezionato.
   - Se si desidera creare una regola per un dispositivo selezionato da un gruppo, passare all'area di lavoro del gruppo, selezionare il dispositivo nella scheda **Dispositivi** ed eseguire le seguenti azioni:
     a. Aprire la finestra delle proprietà del dispositivo selezionato.
     b. Nella sezione **Applicazioni** della finestra delle proprietà del dispositivo selezionare Network Agent.
     c. Aprire la finestra delle proprietà del Network Agent.
3. Nella finestra **Proprietà** visualizzata, nella sezione **Connettività**, selezionare la sottosezione **Profili connessione**.
4. Nella sezione **Impostazioni percorso di rete** fare clic sul pulsante **Aggiungi**.
5. Nella finestra **Nuova descrizione** visualizzata configurare la descrizione del percorso di rete e la regola per il passaggio. Specificare le seguenti impostazioni della descrizione del percorso di rete:
   - Nome della descrizione del percorso di rete

     Il nome della descrizione del percorso di rete non può essere superiore a 255 caratteri, né contenere simboli speciali come ("*<>?\/:|).
   - Usa profilo connessione

     Nell'elenco a discesa è possibile specificare il profilo di connessione utilizzato da Network Agent per connettersi ad Administration Server. Questo profilo verrà utilizzato quando sono soddisfatte le condizioni della descrizione del percorso di rete. Il profilo di connessione contiene le impostazioni per la connessione di Network Agent all'Administration Server e definisce in quali casi i dispositivi client devono passare ai criteri fuori sede. Il profilo viene utilizzato solo per scaricare gli aggiornamenti.

6. Nella sezione **Cambia condizioni** fare clic sul pulsante **Aggiungi** per creare un elenco di condizioni della descrizione del percorso di rete.

   Le condizioni in una regola vengono combinate utilizzando l'operatore logico AND. Per attivare una regola di passaggio in base alla descrizione del percorso di rete, devono essere soddisfatte tutte le condizioni della regola.

7. Nell'elenco a discesa selezionare il valore corrispondente alla modifica delle caratteristiche della rete a cui il dispositivo client è connesso:

   - **Indirizzo gateway di connessione predefinito** – L'indirizzo del gateway principale della rete è stato modificato.
   - **Indirizzo server DHCP** – L'indirizzo IP del server DHCP della rete è stato modificato.
   - **Dominio DNS** – Il suffisso DNS della subnet è stato modificato.
   - **Indirizzo server DNS** – L'indirizzo IP del server DNS della rete è stato modificato.
   - **Accessibilità dominio Windows (solo Windows)** – Modifica dello stato del dominio Windows a cui il dispositivo client è connesso. Utilizzare questa impostazione solo per i dispositivi che eseguono Windows.
   - **Subnet** – Modifica dell'indirizzo e della subnet mask.
   - **Indirizzo server WINS (solo Windows)** – L'indirizzo IP del server WINS della rete è stato modificato. Utilizzare questa impostazione solo per i dispositivi che eseguono Windows.
   - **Risolvibilità del nome**—Il nome DNS o NetBIOS del dispositivo client è cambiato.
   - **Accessibilità indirizzo di connessione SSL**: il dispositivo client può o non può (a seconda dell'opzione selezionata) stabilire una connessione SSL con un server specificato (nome: porta). Per ogni server è inoltre possibile specificare un certificato SSL. In questo caso, Network Agent verifica il certificato del server oltre a controllare la capacità di una connessione SSL. Se il certificato non corrisponde, la connessione non va a buon fine. La frequenza di connessione è di una volta al minuto.

8. Nella finestra visualizzata specificare la condizione per il passaggio di Network Agent a un altro Administration Server. Il nome della finestra dipende dal valore selezionato durante il passaggio precedente. Specificare le seguenti impostazioni della condizione di passaggio:

   - **Valore**

     In questo campo è possibile aggiungere uno o più valori per la condizione creata.

   - **Corrisponde ad almeno un valore dell'elenco**

     Se questa opzione è selezionata, la condizione sarà soddisfatta indipendentemente dal valore specificato nell'elenco **Valore**.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Non corrisponde ad alcun valore dell'elenco**

     Se questa opzione è selezionata, la condizione viene soddisfatta se il relativo valore non è contenuto nell'elenco **Valore**.

9. Nella finestra **Nuova descrizione** selezionare l'opzione **Descrizione abilitata** per abilitare l'utilizzo della nuova descrizione del percorso di rete.

Verrà creata una nuova regola di passaggio in base alla descrizione del percorso di rete. Quando le condizioni della regola sono soddisfatte, Network Agent utilizza il profilo di connessione specificato nella regola per connettersi ad Administration Server.

Viene cercata una corrispondenza del layout di rete nelle descrizioni del percorso di rete, in base all'ordine in cui le regole sono visualizzate nell'elenco. Se una rete corrisponde a più descrizioni, viene utilizzata la prima. È possibile modificare l'ordine delle regole nell'elenco utilizzando i pulsanti **Su** (↑) e **Giù** (↓).

Notifiche degli eventi

In questa sezione viene descritto come selezionare un metodo per l'invio delle notifiche all'amministratore sugli eventi che si verificano nei dispositivi client e come configurare le impostazioni di notifica degli eventi.

Viene inoltre descritto come testare la distribuzione delle notifiche degli eventi tramite il virus di prova Eicar.

Configurazione delle notifiche degli eventi

Kaspersky Security Center consente di selezionare un metodo per la notifica all'amministratore degli eventi che si verificano nei dispositivi client e di configurare la notifica:

- E-mail. Quando si verifica un evento, l'applicazione invia una notifica agli indirizzi e-mail specificati. È possibile modificare il testo della notifica.
- SMS. Quando si verifica un evento, l'applicazione invia una notifica ai numeri di telefono specificati. È possibile configurare le notifiche SMS per l'invio tramite il gateway di posta.
- File eseguibile. Quando si verifica un evento in un dispositivo, il file eseguibile viene avviato nella workstation dell'amministratore. Utilizzando il file eseguibile, l'amministratore può ricevere i parametri di qualsiasi evento che si è verificato.

Per configurare le notifiche degli eventi che si verificano nei dispositivi client:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Fare clic sul collegamento **Configura notifiche ed esportazione eventi** e selezionare il valore **Configura notifiche** nell'elenco a discesa.

   Verrà visualizzata la finestra **Proprietà: Eventi**.

4. Nella sezione **Notifica** selezionare un metodo di notifica (via e-mail, SMS o attraverso un file eseguibile) e definire le impostazioni di notifica:

   - **E-mail**

La scheda **E-mail** consente di configurare le notifiche degli eventi tramite e-mail.

Nel campo **Destinatari (indirizzi e-mail)** specificare gli indirizzi e-mail a cui l'applicazione invierà le notifiche. È possibile specificare più indirizzi in questo campo, separandoli con punto e virgola.

Nel campo **Server SMTP** specificare gli indirizzi dei server di posta, separandoli con punto e virgola. È possibile utilizzare i seguenti valori:

- Indirizzo IPv4 o IPv6
- Nome di rete Windows (nome NetBIOS) del dispositivo
- Nome DNS del server SMTP

Nel campo **Porta server SMTP** specificare il numero di una porta di comunicazione del server SMTP. Il numero di porta predefinito è 25.

Se si abilita l'opzione **Usa ricerca DNS MX**, è possibile utilizzare più record MX degli indirizzi IP per lo stesso nome DNS del server SMTP. Lo stesso nome DNS può avere diversi record MX con valori di priorità differenti di ricezione dei messaggi e-mail. Administration Server tenta di inviare notifiche e-mail al server SMTP in ordine crescente di priorità dei record MX. Per impostazione predefinita, questa opzione è disabilitata.

Se si abilita l'opzione **Usa ricerca DNS MX** e non si abilita l'utilizzo delle impostazioni TLS, è consigliabile utilizzare le impostazioni DNSSEC nel dispositivo server come misura di protezione aggiuntiva per l'invio di notifiche e-mail.

Fare clic sul collegamento **Impostazioni** per definire impostazioni di notifica aggiuntive:

- Nome dell'oggetto (nome dell'oggetto di un messaggio e-mail)
- Indirizzo e-mail del mittente
- Impostazioni di autenticazione ESMTP

È necessario specificare un account per l'autenticazione in un server SMTP se l'opzione di autenticazione ESMTP è abilitata per il server SMTP.

- Impostazioni TLS per il server SMTP:
  - **Non utilizzare TLS**

    È possibile selezionare questa opzione se si desidera disabilitare il criptaggio dei messaggi e-mail.
  - **Usa TLS se supportato dal server SMTP**

    È possibile selezionare questa opzione se si desidera utilizzare una connessione TLS in un server SMTP. Se il server SMTP non supporta TLS, Administration Server si connette al server SMTP senza utilizzare TLS.
  - **Usa sempre TLS, controlla la validità del certificato del server**

    È possibile selezionare questa opzione se si desidera utilizzare le impostazioni di autenticazione TLS. Se il server SMTP non supporta TLS, Administration Server non può connettersi al server SMTP.

È consigliabile utilizzare questa opzione per una protezione più efficace della connessione con un server SMTP. Se si seleziona questa opzione, è possibile configurare le impostazioni di autenticazione per una connessione TLS.

Se si sceglie il valore **Usa sempre TLS, controlla la validità del certificato del server**, è possibile specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. È inoltre possibile specificare un certificato per l'autenticazione del client nel server SMTP.

È possibile specificare le impostazioni TLS per un server SMTP:

- Cercare un file di certificato del server SMTP:

È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Administration Server. Kaspersky Security Center verifica se anche il certificato di un server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center non può connettersi a un server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

- Cercare un file di certificato del client:

È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. È necessario specificare il certificato e la relativa chiave privata utilizzando uno dei seguenti tipi di certificato:

- Certificato X-509:

È necessario specificare un file con il certificato e un file con la chiave privata. Entrambi i file non dipendono l'uno dall'altro e l'ordine di caricamento dei file non è significativo. Quando entrambi i file vengono caricati, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

- Contenitore pkcs12:

È necessario caricare un singolo file che contenga il certificato e la relativa chiave privata. Quando il file viene caricato, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

Il campo **Messaggio di notifica** contiene testo standard con informazioni sull'evento inviate dall'applicazione quando si verifica un evento. Il testo include parametri sostitutivi, ad esempio il nome dell'evento, il nome del dispositivo e il nome di dominio. È possibile modificare il testo del messaggio aggiungendo altri parametri sostitutivi con dettagli più pertinenti dell'evento. L'elenco dei parametri sostitutivi è disponibile facendo clic sul pulsante a destra del campo.

Se il testo di notifica contiene un segno percentuale (%), è necessario digitarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

Fare clic sul collegamento **Configura un limite numerico per le notifiche** per specificare il numero massimo di notifiche che l'applicazione può inviare durante l'intervallo di tempo specificato.

Fare clic sul pulsante **Invia messaggio di test** per verificare se le notifiche sono state configurate correttamente. L'applicazione dovrebbe inviare una notifica di prova agli indirizzi e-mail specificati.

- SMS

La scheda **SMS** consente di configurare la trasmissione delle notifiche SMS di diversi eventi a un cellulare. I messaggi SMS vengono inviati tramite un gateway di posta.

Nel campo **Destinatari (indirizzi e-mail)** specificare gli indirizzi e-mail a cui l'applicazione invierà le notifiche. È possibile specificare più indirizzi in questo campo, separandoli con punto e virgola. Le notifiche verranno inviate ai numeri di telefono associati agli indirizzi e-mail specificati.

Nel campo **Server SMTP** specificare gli indirizzi dei server di posta, separandoli con punto e virgola. È possibile utilizzare i seguenti valori:

- Indirizzo IPv4 o IPv6
- Nome di rete Windows (nome NetBIOS) del dispositivo
- Nome DNS del server SMTP

Nel campo **Porta server SMTP** specificare il numero di una porta di comunicazione del server SMTP. Il numero di porta predefinito è 25.

Fare clic sul collegamento **Impostazioni** per definire impostazioni di notifica aggiuntive:

- Nome dell'oggetto (nome dell'oggetto di un messaggio e-mail)
- Indirizzo e-mail del mittente
- Impostazioni di autenticazione ESMTP

Se necessario, è possibile specificare un account per l'autenticazione in un server SMTP se l'opzione di autenticazione ESMTP è abilitata per il server SMTP.

- Impostazioni TLS per un server SMTP

È possibile disabilitare l'utilizzo di TLS, utilizzare TLS se il server SMTP supporta questo protocollo oppure forzare solo l'utilizzo di TLS. Se si sceglie di utilizzare solo TLS, è possibile specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. Inoltre, se si sceglie di utilizzare solo TLS, è possibile specificare un certificato per l'autenticazione client nel server SMTP.

- Cercare un file di certificato del server SMTP

È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Kaspersky Security Center. Kaspersky Security Center verifica se anche il certificato del server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center non può connettersi al server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

È necessario caricare un singolo file che contenga il certificato e la relativa chiave privata. Quando il file viene caricato, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata. Il campo **Messaggio di notifica** contiene testo standard con informazioni sull'evento che l'applicazione invia quando si verifica un evento. Il testo include parametri sostitutivi, ad esempio il nome dell'evento, il nome del dispositivo e il nome di dominio. È possibile modificare il testo del messaggio aggiungendo altri parametri sostitutivi con dettagli più pertinenti dell'evento. L'elenco dei parametri sostitutivi è disponibile facendo clic sul pulsante a destra del campo.

Se il testo di notifica contiene un segno percentuale (%), è necessario digitarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

Fare clic sul collegamento **Configura un limite numerico per le notifiche** per specificare il numero massimo di notifiche che l'applicazione può inviare nell'intervallo di tempo specificato.

Fare clic sul pulsante **Invia messaggio di prova** per verificare se le notifiche sono state configurate correttamente. L'applicazione dovrebbe inviare una notifica di prova al destinatario specificato.

- File eseguibile da avviare

Se è selezionato questo metodo di notifica, nel campo di immissione è possibile specificare l'applicazione che verrà avviata quando si verifica un evento.

Il collegamento **Configurare un limite numerico per la notifica** consente di specificare il numero massimo di notifiche che l'applicazione può inviare nell'intervallo di tempo specificato.

Il pulsante **Invia messaggio di prova** consente di verificare se le notifiche sono state configurate correttamente: l'applicazione invia una notifica di prova all'indirizzo e-mail specificato.

5. Nel campo **Messaggio di notifica** immettere il testo che l'applicazione invierà quando si verifica un evento.

   È possibile utilizzare l'elenco a discesa a destra del campo di testo per aggiungere impostazioni di sostituzione con dettagli sull'evento (ad esempio la descrizione dell'evento o l'ora in cui si è verificato).

   Se il testo di notifica contiene una percentuale (%), è necessario specificarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

6. Fare clic sul pulsante **Invia messaggio di test** per verificare se la notifica è stata configurata correttamente.

   L'applicazione invia una notifica test all'utente specificato.

7. Fare clic su **OK** per salvare le modifiche.

Le impostazioni di notifica modificate verranno applicate a tutti gli eventi che si verificano nei dispositivi client.

È possibile sostituire le impostazioni di notifica per determinati eventi nella sezione **Configurazione eventi** delle impostazioni di Administration Server, delle impostazioni di un criterio o delle impostazioni di un'applicazione.

Testing delle notifiche

Per verificare l'invio delle notifiche degli eventi, l'applicazione utilizza la notifica di rilevamento del "virus" di prova EICAR nei dispositivi client.

Per verificare l'invio delle notifiche degli eventi:

1. Arrestare l'attività di protezione del file system in tempo reale in un dispositivo client e copiare il "virus" di prova EICAR nel dispositivo client. Abilitare nuovamente la protezione in tempo reale del file system.

2. Eseguire un'attività di scansione per dispositivi client in un gruppo di amministrazione o per dispositivi specifici, compreso uno con il "virus" EICAR.

   Se l'attività di scansione è configurata correttamente, il virus di prova verrà rilevato. Se le notifiche sono configurate correttamente, si riceverà una notifica del rilevamento di un virus.

   Nell'area di lavoro del nodo **Administration Server**, nella scheda **Eventi**, la selezione **Eventi recenti** visualizza un record di rilevamento di un "virus".

Il "virus" di prova EICAR non contiene codice che può danneggiare il dispositivo. Tuttavia, la maggior parte delle applicazioni di protezione identifica il file come virus. È possibile scaricare il "virus" di prova dal sito Web ufficiale di EICAR.

Notifiche degli eventi visualizzate dall'esecuzione di un file eseguibile

Kaspersky Security Center consente di inviare all'amministratore notifiche degli eventi nei dispositivi client visualizzate dall'esecuzione di un file eseguibile. Il file eseguibile deve contenere un altro file eseguibile con segnaposto dell'evento da inviare all'amministratore (vedere la tabella seguente).

Segnaposto per la descrizione di un evento

Segnaposto	Descrizione del segnaposto
%SEVERITY%	Livello di criticità di un evento. Valori possibili: • **Informazioni** • **Avviso** • **Errore** • **Critico**
%COMPUTER%	Nome del dispositivo in cui si è verificato l'evento. La lunghezza massima del nome del dispositivo è di 256 caratteri.
%DOMAIN%	Nome di dominio del dispositivo in cui si è verificato l'evento
%EVENT%	Nome del tipo di evento. La lunghezza massima del nome del tipo di evento è 50 caratteri.
%DESCR%	Descrizione dell'evento. La lunghezza massima della descrizione è di 1000 caratteri.
%RISE_TIME%	Ora di creazione dell'evento.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nome dell'attività. La lunghezza massima del nome dell'attività è di 100 caratteri.
%KL_PRODUCT%	Nome applicazione.
%KL_VERSION%	Numero di versione dell'applicazione.
%KLCSAK_EVENT_SEVERITY_NUM%	Numero del livello di criticità dell'evento. Valori possibili: • 1—**Informazioni** • 2—**Avviso** • 3—**Errore** • 4—**Critico**
%HOST_IP%	Indirizzo IP del dispositivo in cui si è verificato l'evento.
%HOST_CONN_IP%	Indirizzo IP della connessione del dispositivo in cui si è verificato l'evento.

Esempio:
Le notifiche degli eventi sono inviate tramite un file eseguibile (come script1.bat) all'interno del quale viene avviato un altro file eseguibile (come script2.bat) con il segnaposto %COMPUTER%. Quando si verifica un evento, il file script1.bat viene eseguito nel dispositivo dell'amministratore, eseguendo a sua volta il file script2.bat con il segnaposto %COMPUTER%. L'amministratore riceverà il nome del dispositivo in cui si è verificato l'evento.

Criptaggio delle comunicazioni con TLS

Per correggere le vulnerabilità nella rete aziendale dell'organizzazione, è possibile abilitare il criptaggio del traffico tramite il protocollo TLS. È possibile abilitare i protocolli di criptaggio TLS e i pacchetti di criptaggio supportati in Administration Server e iOS MDM Server. Kaspersky Security Center supporta le versioni del protocollo TLS 1.0, 1.1, 1.2 e 1.3. È possibile selezionare il protocollo e i pacchetti di criptaggio richiesti.

Kaspersky Security Center utilizza certificati autofirmati. Non sono necessarie configurazioni aggiuntive dei dispositivi iOS. È inoltre possibile utilizzare i propri certificati. Gli specialisti di Kaspersky consigliano di utilizzare i certificati rilasciati da autorità di certificazione attendibili.

Administration Server

Per configurare i protocolli e i pacchetti di criptaggio consentiti in Administration Server:

1. Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

2. Utilizzare il contrassegno SrvUseStrictSslSettings per configurare i protocolli e i pacchetti di criptaggio consentiti in Administration Server. Immettere il seguente comando:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valore> -t d
   ```

   Specificare il parametro <valore> del contrassegno SrvUseStrictSslSettings:

   - `4`: Sono abilitati solo i protocolli TLS 1.2 e TLS 1.3. Sono abilitate anche le suite di criptaggio con TLS_RSA_WITH_AES_256_GCM_SHA384 (queste suite di criptaggio sono necessarie per la retrocompatibilità con le versioni precedenti di Kaspersky Security Center). Questo è il valore predefinito.

     Suite di criptaggio supportate per il protocollo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (suite di criptaggio con TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

     Suite di criptaggio supportate per il protocollo TLS 1.3:

     - TLS_AES_256_GCM_SHA384
     - TLS_CHACHA20_POLY1305_SHA256
     - TLS_AES_128_GCM_SHA256
     - TLS_AES_128_CCM_SHA256

   - `5`: Sono abilitati solo i protocolli TLS 1.2 e TLS 1.3. Per i protocolli TLS 1.2 e TLS 1.3, sono supportati i pacchetti di criptaggio specifici elencati di seguito.

     Suite di criptaggio supportate per il protocollo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

Suite di criptaggio supportate per il protocollo TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256

Non è consigliabile utilizzare 0, 1, 2 o 3 come valore del parametro del contrassegno SrvUseStrictSslSettings. Questi valori dei parametri corrispondono a versioni non sicure del protocollo TLS (i protocolli TLS 1.0 e TLS 1.1) e a suite di criptaggio non sicure e vengono utilizzati solo per la compatibilità con le versioni precedenti di Kaspersky Security Center.

3. Riavviare i seguenti servizi Kaspersky Security Center 15.1:
   - Administration Server
   - Server Web
   - Proxy di attivazione

Il criptaggio del traffico utilizzando il protocollo TLS è abilitato.

È possibile utilizzare i contrassegni KLTR_TLS12_ENABLED e KLTR_TLS13_ENABLED per abilitare rispettivamente il supporto dei protocolli TLS 1.2 e TLS 1.3. Questi contrassegni sono abilitati per impostazione predefinita.

Per abilitare o disabilitare il supporto dei protocolli TLS 1.2 e TLS 1.3:

1. Eseguire l'utilità klscflag.

   Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

2. Immettere uno dei seguenti comandi nel prompt dei comandi di Windows, utilizzando i diritti di amministratore:
   - Utilizzare questo comando per abilitare o disabilitare il supporto del protocollo TLS 1.2:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS12_ENABLED -v <valore> -t d
     ```

   - Utilizzare questo comando per abilitare o disabilitare il supporto del protocollo TLS 1.3:

     ```
     klscflag -fset -pv ".core/.independent" -s Transport -n KLTR_TLS13_ENABLED -v <valore> -t d
     ```

   Specificare il parametro < `valore` > del contrassegno:

   - `1`: Per abilitare il supporto del protocollo TLS.
   - `0`: Per disabilitare il supporto del protocollo TLS.

Server per dispositivi mobili MDM iOS

La connessione tra i dispositivi iOS e il Server per dispositivi mobili MDM iOS è criptata per impostazione predefinita.

Per configurare i protocolli e i pacchetti di criptaggio consentiti in Server per dispositivi mobili MDM iOS:

1. Aprire il Registro di sistema del dispositivo client in cui è installato il server per dispositivi mobili MDM iOS (ad esempio, in locale, utilizzando il comando regedit dal menu **Start** → **Esegui**).
2. Passare al seguente hive:
   - Per i sistemi a 32 bit:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - Per i sistemi a 64 bit:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. Creare una chiave con il nome `StrictSslSettings`.
4. Specificare `DWORD` come tipo di chiave.
5. Impostare il valore della chiave:
   - `2`: i protocolli TLS 1.0, TLS 1.1 e TLS 1.2 sono abilitati.
   - `3`: solo il protocollo TLS 1.2 è abilitato (valore predefinito).
6. Riavviare il servizio Server per dispositivi mobili MDM iOS di Kaspersky Security Center.

Configurazione dell'interfaccia

È possibile configurare l'interfaccia di Kaspersky Security Center:

- Mostrare e nascondere oggetti nella struttura della console, nell'area di lavoro e nelle finestre delle proprietà degli oggetti (cartelle, sezioni) a seconda delle funzionalità utilizzate.
- Mostrare e nascondere elementi della finestra principale (ad esempio la struttura della console o menu standard come **Azioni** e **Visualizza**).

Per configurare l'interfaccia di Kaspersky Security Center in base al set di funzionalità utilizzate al momento:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Nella barra del menu della finestra principale dell'applicazione selezionare **Visualizza** → **Configura interfaccia**.

3. Nella finestra **Configura interfaccia** visualizzata configurare la visualizzazione degli elementi di interfaccia utilizzando le seguenti caselle di controllo:

- Visualizza Gestione vulnerabilità e patch

  Se questa opzione è abilitata, nella cartella **Installazione remota** viene visualizzata la sottocartella **Distribuisci immagini dei dispositivi**, mentre nella cartella **Archivi** viene visualizzata la sottocartella **Hardware**.

  Questa opzione è disabilitata per impostazione predefinita se l'Avvio rapido guidato non è stato terminato. Questa opzione è abilitata per impostazione predefinita al termine dell'Avvio rapido guidato.

  Se questa opzione è disabilitata, le voci di menu **Crea sessioni RDP** e **Condivisione desktop Windows** non saranno disponibili anche se si dispone di una licenza di gestione dei sistemi.

- Visualizza Criptaggio e protezione dei dati

  Se questa opzione è abilitata, la struttura della console visualizza la cartella **Criptaggio e protezione dei dati**.

  Per impostazione predefinita, questa opzione è abilitata.

- Visualizza impostazioni di controllo degli endpoint

  Se questa opzione è abilitata, vengono visualizzate le seguenti sottosezioni nella sezione **Controlli di Sicurezza** della finestra delle proprietà del criterio di Kaspersky Endpoint Security for Windows:

  - **Controllo Applicazioni**
  - **Controllo Dispositivi**
  - **Controllo Web**
  - **Controllo adattivo delle anomalie**

  Se questa opzione è disabilitata, queste sottosezioni non vengono visualizzate nella sezione **Controlli di Sicurezza**.

  Per impostazione predefinita, questa opzione è abilitata.

- Visualizza Mobile Device Management

  Se questa opzione è abilitata, è disponibile la funzionalità **Mobile Device Management**. Dopo il riavvio dell'applicazione, nella struttura della console viene visualizzata la cartella **Dispositivi mobili**.

  Per impostazione predefinita, questa opzione è abilitata.

- Visualizza Administration Server secondari

Se la casella di controllo è selezionata, nella struttura della console vengono visualizzati i nodi degli Administration Server secondari e virtuali inclusi nei gruppi di amministrazione. Le funzionalità correlate agli Administration Server secondari e virtuali (ad esempio la creazione di attività di installazione remota delle applicazioni negli Administration Server secondari) sono disponibili.

Per impostazione predefinita, questa casella di controllo è deselezionata.

- Visualizza le sezioni delle impostazioni di protezione

  Se questa opzione è abilitata, viene visualizzata la sezione **Protezione** nella finestra delle proprietà di Administration Server, dei gruppi di amministrazione e di altri oggetti. Questa opzione consente di concedere a utenti e gruppi di utenti autorizzazioni personalizzate per l'utilizzo degli oggetti.

  Per impostazione predefinita, questa opzione è disabilitata.

4. Fare clic su **OK**.

Per applicare alcune modifiche, è necessario chiudere la finestra principale dell'applicazione e quindi aprirla nuovamente.

Per configurare la visualizzazione di elementi nella finestra principale dell'applicazione:

1. Nella barra dei menu della finestra principale dell'applicazione selezionare **Visualizza** → **Configura**.
2. Nella finestra **Configura visualizzazione** visualizzata configurare la visualizzazione degli elementi della finestra principale utilizzando le caselle di controllo.
3. Fare clic su **OK**.

Individuazione dei dispositivi nella rete

Questa sezione descrive le operazioni che è necessario eseguire dopo l'installazione di Kaspersky Security Center.

Scenario: Individuazione dei dispositivi nella rete

È necessario eseguire la device discovery prima dell'installazione delle applicazioni di protezione. Administration Server riceve informazioni sui dispositivi rilevati e consente di gestire i dispositivi tramite criteri. Sono necessari polling periodici della rete per aggiornare l'elenco dei dispositivi disponibili nella rete.

Prima di avviare il polling di rete, verificare che il protocollo SMB sia abilitato. In caso contrario, Kaspersky Security Center non può rilevare i dispositivi nella rete sottoposta a polling. Per abilitare il protocollo SMB, seguire le istruzioni per il proprio sistema operativo.

Il rilevamento dei dispositivi in rete comprende i seguenti fasi:

1. **Individuazione dei dispositivi**

L'Avvio rapido guidato fornisce supporto tramite la device discovery e aiuta a individuare i dispositivi della rete quali computer, tablet e cellulari. È inoltre possibile eseguire manualmente la device discovery.

2. **Configurazione dei polling pianificati**

   Decidere quali tipi di polling si desidera utilizzare periodicamente. Abilitare i tipi desiderati e configurare la pianificazione dei polling. È possibile fare riferimento ai suggerimenti per la frequenza dei polling della rete.

3. **Configurazione delle regole per l'aggiunta dei dispositivi individuati nei gruppi di amministrazione (facoltativa)**

   Se vengono visualizzati nuovi dispositivi nella rete, questi vengono individuati durante il polling periodico e vengono automaticamente inclusi nel gruppo **Dispositivi non assegnati**. È possibile impostare regole di spostamento dei dispositivi per automatizzare l'allocazione dei dispositivi al gruppo **Dispositivi gestiti**. È inoltre possibile configurare le regole di conservazione.

   Se si ignora il passaggio 3, i nuovi dispositivi rilevati vengono assegnati al gruppo **Dispositivi non assegnati**. Se si desidera, è possibile spostare questi dispositivi nel gruppo **Dispositivi gestiti** manualmente. Se si spostano manualmente i dispositivi nel gruppo **Dispositivi gestiti**, è possibile analizzare le informazioni su ciascun dispositivo, decidere se spostarlo in un gruppo di amministrazione e, in tal caso, in quale gruppo.

Risultati

Il completamento dello scenario dà i seguenti risultati:

- Kaspersky Security Center Administration Server rileva i dispositivi nella rete e fornisce informazioni in merito.
- Le operazioni di polling future vengono impostate ed eseguite in base alla pianificazione specificata.
- I nuovi dispositivi individuati vengono organizzati in base alle regole configurate. (In alternativa, se non è configurata alcuna regola, i dispositivi rimangono nel gruppo **Dispositivi non assegnati**).

Dispositivi non assegnati

Questa sezione contiene informazioni sulla gestione dei dispositivi di una rete aziendale non inclusi in un gruppo di amministrazione.

Device discovery

In questa sezione vengono descritti i tipi di device discovery disponibili in Kaspersky Security Center e vengono fornite informazioni sull'utilizzo di ogni tipo.

L'Administration Server riceve le informazioni sulla struttura della rete e sui dispositivi al suo interno tramite il polling periodico. Le informazioni vengono registrate nel database di Administration Server. Administration Server può utilizzare i seguenti tipi di polling:

- **Polling della rete Windows**. L'Administration Server può eseguire due tipi di polling della rete Windows: rapido e completo. Durante un polling rapido Administration Server recupera informazioni solo dall'elenco dei nomi di dispositivi NetBIOS in tutti i domini di rete e i gruppi di lavoro. Durante un polling completo vengono richieste più informazioni da ogni dispositivo client: nome del sistema operativo, indirizzo IP, nome DNS e nome NetBIOS. Per impostazione predefinita sono abilitati sia il polling rapido che quello completo. Il polling della rete Windows può non essere in grado di individuare i dispositivi, ad esempio se le porte UDP 137, UDP 138, TCP 139 sono chiuse nel router o dal firewall.

- **Polling Active Directory**. L'Administration Server recupera le informazioni sulla struttura delle unità Active Directory e sui nomi DNS dei dispositivi dai gruppi Active Directory. Per impostazione predefinita, questo tipo di polling è abilitato. È consigliabile utilizzare il polling di Active Directory se si utilizza Active Directory. In caso contrario, l'Administration Server non individua i dispositivi. Se si utilizza Active Directory ma alcuni dei dispositivi della rete non sono elencati come membri, tali dispositivi non possono essere individuati dal polling di Active Directory.

- **Polling intervallo IP**. Administration Server esegue il polling dell'intervallo IP specificati utilizzando pacchetti ICMP o il protocollo NBNS e compila un set completo di dati sui dispositivi all'interno degli intervalli IP. Per impostazione predefinita, questo tipo di polling è disabilitato. Non è consigliabile utilizzare questo tipo di polling se si utilizza il polling di rete Windows e/o il polling di Active Directory.

- **Polling Zeroconf**. Un punto di distribuzione che esegue il polling della rete IPv6 utilizzando le reti zero-configuration (definite anche *Zeroconf*). Per impostazione predefinita, questo tipo di polling è disabilitato. È possibile utilizzare il polling Zeroconf se il punto di distribuzione esegue Linux.

Se sono installate e attivate le regole di spostamento dei dispositivi, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi gestiti**. Se non sono state abilitate regole di spostamento, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi non assegnati**.

È possibile modificare le impostazioni di device discovery per ciascun tipo. È ad esempio possibile modificare la pianificazione del polling o impostare l'esecuzione del polling dell'intera foresta di domini o solo di un dominio specifico.

Prima di avviare il polling di rete, verificare che il protocollo SMB sia abilitato. In caso contrario, Kaspersky Security Center non può rilevare i dispositivi nella rete sottoposta a polling. Per abilitare il protocollo SMB, seguire le istruzioni per il proprio sistema operativo.

Polling della rete Windows

Informazioni sul polling della rete Windows

Durante un polling rapido Administration Server recupera informazioni solo dall'elenco dei nomi di dispositivi NetBIOS in tutti i domini di rete e i gruppi di lavoro. Durante un polling completo sono richieste le seguenti informazioni da ogni dispositivo client:

- Nome del sistema operativo

- Indirizzo IP

- Nome DNS
- Nome NetBIOS

Sia il polling rapido che quello completo richiedono le seguenti operazioni:

- Le porte UDP 137/138, TCP 139, UDP 445, TCP 445 devono essere disponibili nella rete.
- Il protocollo SMB è abilitato.
- È necessario utilizzare il servizio Microsoft Computer Browser e il computer del browser primario deve essere abilitato in Administration Server.
- È necessario utilizzare il servizio Microsoft Computer Browser e il computer del browser primario deve essere abilitato nei dispositivi client:
  - In almeno un dispositivo, se il numero di dispositivi della rete non è superiore a 32.
  - In almeno un dispositivo ogni 32 dispositivi della rete.

Il polling completo può essere eseguito solo se il polling rapido è stato eseguito almeno una volta.

Visualizzazione e modifica delle impostazioni per il polling della rete Windows

Per modificare le impostazioni per il polling della rete Windows:

1. Nella struttura della console selezionare la sottocartella **Domini** nella cartella **Device discovery**.

   È possibile passare dalla cartella **Dispositivi non assegnati** alla cartella **Device discovery** facendo clic sul pulsante **Esegui il polling**.

   Nell'area di lavoro della sottocartella **Domini** viene visualizzato l'elenco dei dispositivi.

2. Fare clic su **Esegui il polling**.

   Verrà visualizzata la finestra delle proprietà del dominio. Se si desidera, modificare le impostazioni del polling della rete Windows:

   - Abilita il polling della rete Windows

     Questa opzione è selezionata per impostazione predefinita. Se non si desidera eseguire il polling della rete Windows (ad esempio, se si ritiene che il polling di Active Directory sia sufficiente), è possibile deselezionare questa opzione.

   - Imposta pianificazione di polling rapido

Il periodo predefinito è di 15 minuti.

Durante un polling rapido Administration Server recupera informazioni solo dall'elenco dei nomi di dispositivi NetBIOS in tutti i domini di rete e i gruppi di lavoro.

I dati ricevuti al successivo polling sostituiscono completamente i dati precedenti.

Sono disponibili le opzioni di pianificazione di polling seguenti:

- **Ogni N giorni**

  Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

  Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N minuti**

  Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

  Per impostazione predefinita, il polling viene eseguito ogni 5 minuti, a partire dall'ora di sistema corrente.

- **In base ai giorni della settimana**

  Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, il polling viene eseguito ogni venerdì alle 18:00:00.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è 18:00:00.

- **Esegui attività non effettuate**

  Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

  Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

  Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

  Per impostazione predefinita, questa opzione è abilitata.

- **Imposta pianificazione di polling completo**

Il periodo predefinito è un'ora. I dati ricevuti al successivo polling sostituiscono completamente i dati precedenti.

Sono disponibili le opzioni di pianificazione di polling seguenti:

- **Ogni N giorni**

  Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

  Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N minuti**

  Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

  Per impostazione predefinita, il polling viene eseguito ogni 5 minuti, a partire dall'ora di sistema corrente.

- **In base ai giorni della settimana**

  Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, il polling viene eseguito ogni venerdì alle 18:00:00.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è 18:00:00.

- **Esegui attività non effettuate**

  Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

  Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

  Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

  Per impostazione predefinita, questa opzione è abilitata.

Se si desidera eseguire immediatamente il polling fare clic su **Esegui il polling**. Verranno avviati entrambi i tipi di polling.

Nell'Administration Server virtuale è possibile visualizzare e modificare le impostazioni del polling della rete Windows nella finestra delle proprietà del punto di distribuzione, nella sezione **Device discovery**.

Polling Active Directory

Utilizzare il polling di Active Directory se si utilizza Active Directory; in caso contrario, è consigliabile utilizzare altri tipi di polling. Se si utilizza Active Directory ma alcuni dei dispositivi della rete non sono elencati come membri, tali dispositivi non possono essere individuati dal polling di Active Directory.

I risultati del polling di Active Directory vengono archiviati nell'Administration Server per 30 giorni, indipendentemente dai risultati dei polling successivi.

Prima di avviare il polling di rete, verificare che il protocollo SMB sia abilitato. In caso contrario, Kaspersky Security Center non può rilevare i dispositivi nella rete sottoposta a polling. Per abilitare il protocollo SMB, seguire le istruzioni per il proprio sistema operativo.

Visualizzazione e modifica delle impostazioni per il polling di Active Directory

Per visualizzare e modificare le impostazioni per il polling dei gruppi di Active Directory:

1. Nella struttura della console selezionare la sottocartella **Active Directory** nella cartella **Device discovery**.

   In alternativa, è possibile passare dalla cartella **Dispositivi non assegnati** alla cartella **Device discovery** facendo clic sul pulsante **Esegui il polling**.

2. Fare clic su **Configura polling**.

   Verrà visualizzata la finestra delle proprietà di Active Directory. Se si desidera, modificare le impostazioni del polling dei gruppi di Active Directory:

   - Abilita polling di Active Directory

     Questa opzione è selezionata per impostazione predefinita. Tuttavia, se non si utilizza Active Directory, il polling non recupera alcun risultato. In questo caso, è possibile deselezionare l'opzione.

   - Imposta pianificazione di polling

Il periodo predefinito è un'ora.

Sono disponibili le opzioni di pianificazione di polling seguenti:

- **Ogni N giorni**

  Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

  Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N minuti**

  Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

  Per impostazione predefinita, il polling viene eseguito ogni 5 minuti, a partire dall'ora di sistema corrente.

- **In base ai giorni della settimana**

  Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, il polling viene eseguito ogni venerdì alle 18:00:00.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è 18:00:00.

- **Esegui attività non effettuate**

  Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

  Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

  Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

  Per impostazione predefinita, questa opzione è abilitata.

- **Avanzate**

È possibile selezionare i domini per i quali Active Directory eseguirà il polling:

- Dominio di Active Directory a cui appartiene Kaspersky Security Center.
- Foresta di dominio a cui appartiene Kaspersky Security Center.
- Elenco di domini Active Directory specificato.

  Se si seleziona questa opzione è possibile aggiungere domini all'ambito di polling:

  - Fare clic sul pulsante **Aggiungi**.
  - Nei campi corrispondenti specificare l'indirizzo del controller di dominio, il nome e la password dell'account per l'accesso.
  - Fare clic su **OK** per salvare le modifiche.

  È possibile selezionare l'indirizzo del controller di dominio nell'elenco e fare clic sui pulsanti **Modifica** o **Rimuovi** per modificarlo o rimuoverlo.
- Fare clic su **OK** per salvare le modifiche.

Se si desidera eseguire immediatamente il polling fare clic sul pulsante **Esegui il polling**.

Nell'Administration Server virtuale è possibile visualizzare e modificare le impostazioni del polling dei gruppi di Active Directory nella finestra delle proprietà del punto di distribuzione, nella sezione **Device discovery**.

Polling intervallo IP

Administration Server esegue il polling degli intervalli IP specificati utilizzando pacchetti ICMP o il protocollo NBNS e compila un set completo di dati sui dispositivi all'interno degli intervalli IP. Per impostazione predefinita, questo tipo di polling è disabilitato.

Per tutti gli host basati su Linux all'interno di un controller di dominio Microsoft Active Directory o Samba, specificare il `netbios name` e i parametri del `workgroup` nel file `/etc/samba/smb.conf`. In caso contrario, i risultati del polling potrebbero contenere contenitori host duplicati.

Prima di avviare il polling di rete, verificare che il protocollo SMB sia abilitato. In caso contrario, Kaspersky Security Center non può rilevare i dispositivi nella rete sottoposta a polling. Per abilitare il protocollo SMB, seguire le istruzioni per il proprio sistema operativo.

Visualizzazione e modifica delle impostazioni per il polling degli intervalli IP

Per visualizzare e modificare le impostazioni per il polling dei gruppi di intervalli IP:

1. Nella struttura della console selezionare la sottocartella **Intervalli IP** nella cartella **Device discovery**.

   È possibile passare dalla cartella **Dispositivi non assegnati** alla cartella **Device discovery** facendo clic su **Esegui il polling**.

2. Se si desidera, nella sottocartella **Intervalli IP** fare clic su **Aggiungi subnet** per aggiungere un intervallo IP per il polling, quindi fare clic su **OK**.

3. Fare clic su **Configura polling**.

   Verrà visualizzata la finestra delle proprietà degli intervalli IP. Se si desidera, è possibile modificare le impostazioni del polling dell'intervallo IP:

   - **Abilita polling intervalli IP**

     Questa opzione non è selezionata per impostazione predefinita. Non è consigliabile utilizzare questo tipo di polling se si utilizza il polling di rete Windows e/o il polling di Active Directory.

   - **Imposta pianificazione di polling**

Il periodo predefinito è di 420 minuti. I dati ricevuti al successivo polling sostituiscono completamente i dati precedenti.

Sono disponibili le opzioni di pianificazione di polling seguenti:

- **Ogni N giorni**

  Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

  Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

- **Ogni N minuti**

  Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

  Per impostazione predefinita, il polling viene eseguito ogni 5 minuti, a partire dall'ora di sistema corrente.

- **In base ai giorni della settimana**

  Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, il polling viene eseguito ogni venerdì alle 18:00:00.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è 18:00:00.

- **Esegui attività non effettuate**

  Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

  Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

  Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

  Per impostazione predefinita, questa opzione è abilitata.

Se si desidera eseguire immediatamente il polling fare clic su **Esegui il polling**. Questo pulsante è disponibile solo se è stato selezionato **Abilita polling intervalli IP**.

Nell'Administration Server virtuale è possibile visualizzare e modificare le impostazioni del polling dell'intervallo IP nella finestra delle proprietà del punto di distribuzione, nella sezione **Device discovery**. I dispositivi client individuati durante il polling dell'intervallo IP sono visualizzati nella cartella **Domini** dell'Administration Server virtuale.

Polling zeroconf

Questo tipo di polling è supportato solo per i punti di distribuzione basati su Linux.

Un punto di distribuzione può eseguire il polling delle reti che hanno dispositivi con indirizzi IPv6. In questo caso, gli intervalli IP non vengono specificati e il punto di distribuzione esegue il polling dell'intera rete utilizzando le reti zero-configuration (definite anche *Zeroconf*). Per iniziare a utilizzare Zeroconf è necessario installare l'utilità avahi-browse nel punto di distribuzione.

Per abilitare il polling Zeroconf:

1. Nella struttura della console selezionare la sottocartella **Intervalli IP** nella cartella **Device discovery**.

   È possibile passare dalla cartella **Dispositivi non assegnati** alla cartella **Device discovery** facendo clic su **Esegui il polling**.

2. Fare clic su **Configura polling**.

3. Nella finestra delle proprietà degli intervalli IP visualizzata selezionare **Abilita il polling con la tecnologia Zeroconf**.

Successivamente, il punto di distribuzione inizia a eseguire il polling della rete. In questo caso gli intervalli IP specificati vengono ignorati.

Utilizzo di domini Windows. Visualizzazione e modifica delle impostazioni del dominio

Per modificare le impostazioni del dominio:

1. Nella struttura della console selezionare la sottocartella **Domini** nella cartella **Device discovery**.

2. Selezionare un dominio e aprire la relativa finestra delle proprietà in uno dei seguenti modi:

   - Selezionando **Proprietà** nel menu di scelta rapida del dominio.

   - Facendo clic sul collegamento **Mostra proprietà gruppo**.

   Verrà visualizzata la finestra **Proprietà: <Nome dominio>**, in cui è possibile configurare il dominio selezionato.

Configurazione delle regole di conservazione per i dispositivi non assegnati

Al termine del polling della rete Windows, i dispositivi trovati vengono inseriti nei sottogruppi del gruppo di amministrazione Dispositivi non assegnati. Questo gruppo di amministrazione è disponibile in **Avanzate** → **Device discovery** → **Domini**. La cartella **Domini** è il gruppo padre. Contiene gruppi figlio denominati in base ai domini e ai gruppi di lavoro corrispondenti rilevati durante il polling della rete. Il gruppo padre può anche contenere il gruppo di amministrazione dei dispositivi mobili. È possibile configurare le regole di conservazione dei dispositivi non assegnati per il gruppo padre e ognuno dei gruppi figlio. Le regole di conservazione non dipendono dalle impostazioni del polling della rete e operano anche se il polling della rete è disabilitato.

Per configurare le regole di conservazione per i dispositivi non assegnati:

1. Nella struttura della console, nella cartella **Device discovery**, eseguire una delle seguenti operazioni:

   - Per configurare le impostazioni del gruppo padre, fare clic con il pulsante destro del mouse sulla sottocartella **Domini**, quindi selezionare **Proprietà**.

     Verrà visualizzata la finestra delle proprietà dal gruppo padre.

   - Per configurare le impostazioni di un gruppo figlio, fare clic con il pulsante destro del mouse sul relativo nome, quindi selezionare **Proprietà**.

     Verrà visualizzata la finestra delle proprietà del gruppo figlio.

2. Nella sezione **Dispositivi** specificare le seguenti impostazioni:

   - **Rimuovi il dispositivo dal gruppo se è inattivo da più di (giorni)**

     Se questa opzione è abilitata, è possibile specificare l'intervallo di tempo al termine del quale il dispositivo viene rimosso automaticamente dal gruppo. Per impostazione predefinita, questa opzione viene distribuita anche ai gruppi figlio. L'intervallo di tempo predefinito è 7 giorni.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Eredita da gruppo padre**

     Se questa opzione è abilitata, il periodo di conservazione per i dispositivi del gruppo corrente viene ereditato dal gruppo padre e non può essere modificato.

     Questa opzione è disponibile solo per i gruppi figlio.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Forza ereditarietà nei gruppi figlio**

     I valori delle impostazioni vengono distribuiti ai gruppi figlio, ma nelle proprietà dei gruppi figlio tali impostazioni sono bloccate.

     Per impostazione predefinita, questa opzione è disabilitata.

Le modifiche verranno salvate e applicate.

Utilizzo degli intervalli IP

È possibile personalizzare gli intervalli IP esistenti e crearne di nuovi.

Creazione di un intervallo IP

Per creare un intervallo IP:

1. Nella struttura della console selezionare la sottocartella **Intervalli IP** nella cartella **Device discovery**.
2. Nel menu di scelta rapida della cartella selezionare **Nuovo** → **Intervallo IP**.
3. Nella finestra **Nuovo intervallo IP** visualizzata configurare il nuovo intervallo IP.

Il nuovo intervallo IP viene visualizzato nella cartella **Intervalli IP**.

Visualizzazione e modifica delle impostazioni degli intervalli IP

Per modificare le impostazioni degli intervalli IP:

1. Nella struttura della console, nella cartella **Device discovery** selezionare la sottocartella **Intervalli IP**.
2. Selezionare un intervallo IP, quindi aprire la relativa finestra delle proprietà in uno dei seguenti modi:
   - Selezionando **Proprietà** nel menu di scelta rapida dell'intervallo IP.
   - Facendo clic sul collegamento **Mostra proprietà gruppo**.

Verrà visualizzata la finestra **Proprietà: <Nome intervallo IP>**, in cui è possibile configurare le proprietà dell'intervallo IP selezionato.

Utilizzo di gruppi Active Directory. Visualizzazione e modifica delle impostazioni dei gruppi

Per modificare le impostazioni per il gruppo Active Directory:

1. Nella struttura della console selezionare la sottocartella **Active Directory** nella cartella **Device discovery**.
2. Selezionare un gruppo Active Directory, quindi aprire la relativa finestra delle proprietà in uno dei seguenti modi:
   - Selezionando **Proprietà** nel menu di scelta rapida dell'intervallo IP.
   - Facendo clic sul collegamento **Mostra proprietà gruppo**.

Verrà visualizzata la finestra **Proprietà: <Nome gruppo Active Directory>**, in cui è possibile configurare il gruppo Active Directory selezionato.

Creazione di regole per lo spostamento automatico dei dispositivi nei gruppi di amministrazione

È possibile configurare lo spostamento automatico dei dispositivi nei gruppi di amministrazione dopo che vengono individuati durante il polling di una rete aziendale.

Per configurare le regole per spostare automaticamente i dispositivi nei gruppi di amministrazione:

1. Nella struttura della console selezionare la cartella **Dispositivi non assegnati**.
2. Nell'area di lavoro di questa cartella fare clic su **Configura regole**.

   Verrà visualizzata la finestra **Proprietà: Dispositivi non assegnati**. Nella sezione **Sposta dispositivi** configurare le regole per lo spostamento automatico dei dispositivi nei gruppi di amministrazione.

La prima regola applicabile nell'elenco (dall'alto verso il basso dell'elenco) verrà applicata a un dispositivo.

Utilizzo della modalità dinamica VDI nei dispositivi client

Un'infrastruttura virtuale può essere distribuita in una rete aziendale utilizzando macchine virtuali temporanee. Kaspersky Security Center è in grado di rilevare le macchine virtuali temporanee aggiungendo le relative informazioni al database di Administration Server. Dopo che un utente ha finito di utilizzare una macchina virtuale temporanea, quest'ultima viene rimossa dall'infrastruttura virtuale. Tuttavia, è possibile che un record relativo alla macchina virtuale rimossa venga salvato nel database di Administration Server. Anche le macchine virtuali non esistenti possono essere visualizzate in Administration Console.

Per evitare che le informazioni relative alle macchine virtuali non esistenti vengano salvate, Kaspersky Security Center supporta la modalità dinamica per Virtual Desktop Infrastructure (VDI). L'amministratore può abilitare il supporto della modalità dinamica per VDI nelle proprietà del pacchetto di installazione di Network Agent da installare nella macchina virtuale temporanea.

Quando una macchina virtuale temporanea viene disabilitata, Network Agent notifica ad Administration Server che la macchina è stata disabilitata. Se la macchina virtuale è stata disabilitata correttamente, viene rimossa dall'elenco dei dispositivi connessi ad Administration Server. Se durante la disabilitazione della macchina virtuale si verificano errori e Network Agent non invia una notifica relativa alla macchina virtuale disabilitata ad Administration Server, verrà utilizzato uno scenario di backup. In questo scenario, una macchina virtuale viene rimossa dall'elenco dei dispositivi connessi ad Administration Server dopo tre tentativi non riusciti di sincronizzazione con Administration Server.

Abilitazione della modalità dinamica VDI nelle proprietà di un pacchetto di installazione per Network Agent

Per abilitare la modalità dinamica VDI:

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Pacchetti di installazione**.
2. Nel menu di scelta rapida del pacchetto di installazione di Network Agent selezionare **Proprietà**.

   Verrà visualizzata la finestra **Proprietà: Kaspersky Security Center Network Agent**.

3. Nella finestra **Proprietà: Kaspersky Security Center Network Agent** selezionare la sezione **Avanzate**.
4. Nella sezione **Avanzate** selezionare l'opzione **Abilita modalità dinamica per VDI**.

Il dispositivo in cui deve essere installato Network Agent verrà incluso in VDI.

Ricerca dei dispositivi appartenenti a VDI

Per individuare i dispositivi non assegnati inclusi in VDI:

1. Selezionare **Cerca** dal menu di scelta rapida della cartella **Dispositivi non assegnati**.

   Per visualizzare un elenco di tutti i dispositivi che fanno parte di Virtual Desktop Infrastructure, selezionare **Cerca** nel menu di scelta rapida della cartella **Administration Server**.
2. Nella finestra **Cerca**, nella scheda **Macchine virtuali**, selezionare **Sì** nel gruppo di impostazioni **Parte di Virtual Desktop Infrastructure**.
3. Fare clic sul pulsante **Trova**.

Viene visualizzato l'elenco dei dispositivi non assegnati che fanno parte di Virtual Desktop Infrastructure.

Spostamento dei dispositivi da VDI a un gruppo di amministrazione

Per spostare i dispositivi inclusi in VDI in un gruppo di amministrazione:

1. Nell'area di lavoro della cartella **Dispositivi non assegnati** fare clic sul pulsante **Configura regole**.

   Verrà visualizzata la finestra delle proprietà della cartella **Dispositivi non assegnati**.
2. Nella finestra delle proprietà della cartella **Dispositivi non assegnati**, nella sezione **Sposta dispositivi**, fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Nuova regola**.
3. Nella finestra **Nuova regola** selezionare la sezione **Macchine virtuali**.
4. Nell'elenco a discesa **Questa è una macchina virtuale** selezionare **Sì**.

Verrà creata una regola per il riposizionamento dei dispositivi in un gruppo di amministrazione.

Inventario dei dispositivi

L'elenco dell'hardware (**Archivi** → **Hardware**) utilizzato per eseguire l'inventario dei dispositivi viene popolato in due modi: automatico e manuale. Dopo ogni polling di rete, tutti i dispositivi rilevati vengono aggiunti automaticamente all'elenco; tuttavia è anche possibile aggiungere manualmente i dispositivi se non si desidera eseguire il polling della rete. È possibile aggiungere manualmente altri dispositivi all'elenco, ad esempio, router, stampanti o hardware di dispositivi.

Nelle proprietà di un dispositivo è possibile visualizzare e modificare informazioni dettagliate sul dispositivo.

L'elenco dell'hardware può contenere i seguenti tipi di dispositivi:

- Computer
- Dispositivi mobili
- Dispositivi di rete
- Dispositivi virtuali
- Componenti OEM
- Periferiche per computer
- Dispositivi connessi
- Telefoni VoIP
- Archivi di rete

L'amministratore può assegnare l'attributo *Aziendale* ai dispositivi rilevati. Questo attributo può essere assegnato manualmente nelle proprietà di un dispositivo o l'amministratore può specificare criteri per l'assegnazione automatica dell'attributo. In questo caso, l'attributo *Aziendale* viene assegnato in base al tipo di dispositivo.

Kaspersky Security Center consente l'eliminazione dei dispositivi. A tale scopo, selezionare l'opzione **Dispositivo eliminato** nelle proprietà di un dispositivo. Il dispositivo non verrà visualizzato nell'elenco dei dispositivi.

Un amministratore può gestire l'elenco dei PLC (Programmable Logic Controller) nella cartella **Hardware**. Informazioni dettagliate sulla gestione dell'elenco PLC sono disponibili nel *manuale dell'utente di Kaspersky Industrial CyberSecurity for Nodes*.

Aggiunta di informazioni sui nuovi dispositivi

Per aggiungere informazioni sui nuovi dispositivi nella rete:

1. Nella cartella **Archivi** della struttura della console selezionare la sottocartella **Hardware**.
2. Nell'area di lavoro della cartella **Hardware** fare clic sul pulsante **Aggiungi dispositivo** per aprire la finestra **Nuovo dispositivo**.

   Verrà visualizzata la finestra **Nuovo dispositivo**.
3. Nella finestra **Nuovo dispositivo** selezionare nell'elenco a discesa **Tipo** il tipo di dispositivo da aggiungere.
4. Fare clic su **OK**.

   Verrà visualizzata la finestra delle proprietà del dispositivo, nella sezione **Generale**.

5. Nella sezione **Generale** compilare i campi di immissione con i dati sul dispositivo. Nella sezione **Generale** sono elencate le seguenti impostazioni:

   - **Dispositivo aziendale**. Selezionare la casella di controllo se si desidera assegnare l'attributo *Aziendale* al dispositivo. Utilizzando questo attributo è possibile eseguire la ricerca di dispositivi nella cartella **Hardware**.

   - **Dispositivo eliminato**. Selezionare la casella di controllo se non si desidera che il dispositivo venga visualizzato nell'elenco dei dispositivi nella cartella **Hardware**.

6. Fare clic su **Applica**.

Il nuovo dispositivo verrà visualizzato nell'area di lavoro della cartella **Hardware**.

Configurazione dei criteri utilizzati per definire i dispositivi aziendali

Per configurare i criteri di rilevamento dei dispositivi aziendali:

1. Nella cartella **Archivi** della struttura della console selezionare la sottocartella **Hardware**.

2. Nell'area di lavoro della cartella **Hardware** fare clic sul pulsante **Azioni aggiuntive** e selezionare **Configura regola per i dispositivi aziendali** nell'elenco a discesa.

   Verrà visualizzata la finestra delle proprietà dell'hardware.

3. Nella finestra delle proprietà dell'hardware, nella sezione **Dispositivi aziendali**, selezionare un metodo per l'assegnazione dell'attributo *Aziendale* al dispositivo:

   - **Imposta manualmente l'attributo Dispositivo aziendale per il dispositivo**. L'attributo *Hardware aziendale* viene assegnato al dispositivo manualmente nella finestra delle proprietà del dispositivo, nella sezione **Generale**.

   - **Imposta automaticamente l'attributo Dispositivo aziendale per il dispositivo**. Nel gruppo di impostazioni **Per tipo di dispositivo** specificare tipi di dispositivi a cui l'applicazione assegnerà automaticamente l'attributo *Aziendale*.

     Questa opzione interessa solo i dispositivi che sono stati aggiunti tramite il polling della rete. Per i dispositivi aggiunti manualmente, impostare manualmente l'attributo *Aziendale*.

4. Fare clic su **OK**.

I criteri di rilevamento per i dispositivi aziendali sono configurati.

Configurazione dei campi personalizzati

Per configurare i campi personalizzati dei dispositivi:

1. Nella cartella **Archivi** della struttura della console selezionare la sottocartella **Hardware**.
2. Nell'area di lavoro della cartella **Hardware** fare clic sul pulsante **Azioni aggiuntive** e selezionare **Configura campi di dati personalizzati** nell'elenco a discesa.

   Verrà visualizzata la finestra delle proprietà dell'hardware.
3. Nella finestra delle proprietà dell'hardware selezionare la sezione **Campi personalizzati** e fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Aggiungi campo**.
4. Nella finestra **Aggiungi campo** specificare il nome del campo personalizzato che verrà visualizzato nelle proprietà dell'hardware.

   È possibile creare più campi personalizzati con nomi univoci.
5. Fare clic su **OK**.

I campi personalizzati che sono stati aggiunti sono visualizzati nella sezione **Campi personalizzati** delle proprietà dell'hardware. È possibile utilizzare i campi personalizzati per fornire informazioni specifiche sui dispositivi. Potrebbe ad esempio trattarsi del numero di ordine interno per l'acquisto di un componente hardware.

Licensing

In questa sezione vengono fornite informazioni sulle condizioni generali relative al licensing di Kaspersky Security Center 15.1.

Eventi di superamento del limite di licenze

Kaspersky Security Center consente di ottenere informazioni sugli eventi che si verificano in caso di superamento dei limiti di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client.

Il livello di importanza degli eventi quando avviene il superamento di un limite di licenze è definito in base alle regole seguenti:

- Se le unità attualmente in uso coperte da una singola licenza costituiscono tra il 90% e il 100% del numero totale di unità coperte dalla licenza, l'evento è pubblicato con il livello di importanza **Informazioni**.
- Se le unità attualmente in uso coperte da una singola licenza costituiscono tra il 100% e il 110% del numero totale di unità coperte dalla licenza, l'evento è pubblicato con il livello di importanza **Avviso**.
- Se il numero di unità attualmente in uso coperte da una singola licenza è superiore al 110% del numero totale di unità coperte dalla licenza, l'evento è pubblicato con il livello di importanza **Evento critico**.

Informazioni sulle licenze

Questa sezione contiene informazioni sul licensing delle applicazioni Kaspersky gestite tramite Kaspersky Security Center.

Informazioni sulla licenza

Una *licenza* concede per un determinato periodo di tempo il diritto di utilizzare Kaspersky Security Center, in conformità con i termini del Contratto di licenza (Contratto di licenza con l'utente finale).

L'ambito dei servizi forniti e il periodo di validità per l'utilizzo dell'applicazione dipendono dalla licenza utilizzata per attivare l'applicazione.

Sono disponibili i seguenti tipi di licenza:

- *Di prova*

  Una licenza gratuita che consente di valutare l'applicazione. Una licenza di prova ha in genere un periodo limitato.

  Alla scadenza di una licenza di prova, tutte le funzionalità di Kaspersky Security Center vengono disabilitate. Per continuare a utilizzare l'applicazione, è necessario acquistare una licenza commerciale.

  È possibile utilizzare l'applicazione con una licenza di prova per un solo periodo di prova.

- *Commerciale*

  Una licenza a pagamento.

  Alla scadenza di una licenza commerciale, le funzionalità chiave dell'applicazione vengono disattivate. Per continuare a utilizzare Kaspersky Security Center, è necessario rinnovare la licenza commerciale. Dopo la scadenza di una licenza commerciale, non è possibile continuare a utilizzare l'applicazione ed è necessario rimuoverla dal dispositivo.

  È consigliabile rinnovare la licenza prima della scadenza per assicurare la protezione costante da tutti i tipi di minacce.

Informazioni sul Contratto di licenza con l'utente finale

Il *Contratto di licenza con l'utente finale* (Contratto di licenza o EULA) è un accordo vincolante tra l'utente e AO Kaspersky Lab, in cui sono definite le condizioni di utilizzo dell'applicazione.

Leggere attentamente il Contratto di licenza prima di iniziare a utilizzare l'applicazione.

Kaspersky Security Center e i relativi componenti, ad esempio Network Agent, hanno Contratti di licenza con l'utente finale distinti.

È possibile visualizzare le condizioni del Contratto di licenza con l'utente finale per Kaspersky Security Center utilizzando i seguenti metodi:

- Durante l'installazione di Kaspersky Security Center.
- Leggendo il documento license.txt incluso nel kit di distribuzione di Kaspersky Security Center.
- Leggendo il documento license. txt nella cartella di installazione di Kaspersky Security Center.
- Scaricando il file license.txt dal sito Web di Kaspersky.

È possibile visualizzare i termini del Contratto di licenza con l'utente finale per Network Agent per Windows, Network Agent per Mac e Network Agent per Linux utilizzando i seguenti metodi:

- Durante il download del pacchetto di distribuzione di Network Agent dai server Web di Kaspersky.
- Durante l'installazione di Network Agent per Windows, Network Agent per Mac o Network Agent per Linux.
- Leggendo il documento license.txt incluso nel pacchetto di distribuzione di Network Agent per Windows, Network Agent per Mac o Network Agent per Linux.
- Leggendo il documento license.txt nella cartella di installazione di Network Agent per Windows, Network Agent per Mac o Network Agent per Linux.
- Scaricando il file license.txt dal sito Web di Kaspersky.

Le condizioni del Contratto di licenza con l'utente finale si considerano accettate quando l'utente conferma l'accettazione del Contratto di licenza con l'utente finale durante l'installazione dell'applicazione. Se non si accettano le condizioni del Contratto di licenza, annullare l'installazione dell'applicazione e rinunciare all'utilizzo dell'applicazione.

Informazioni sul certificato di licenza

Un *certificato di licenza* è un documento ricevuto insieme a un file chiave o a un codice di attivazione.

Un certificato di licenza contiene le seguenti informazioni sulla licenza fornita:

- ID licenza o numero di ordine
- Informazioni sull'utente a cui è stata concessa la licenza
- Informazioni sull'applicazione che può essere attivata con la licenza fornita
- Limite del numero di unità di licensing (ad esempio dispositivi in cui può essere utilizzata l'applicazione con la licenza fornita)
- Data di inizio del periodo di validità della licenza
- Data di scadenza della licenza o periodo licenza
- Tipo di licenza

Informazioni sulla chiave di licenza

Una *chiave di licenza* è una sequenza di bit che è possibile applicare per attivare e quindi utilizzare l'applicazione in conformità alle condizioni del Contratto di licenza con l'utente finale. Le chiavi di licenza sono generate dagli specialisti di Kaspersky.

È possibile aggiungere una chiave di licenza all'applicazione utilizzando uno dei seguenti metodi: applicando un *file chiave* o inserendo un *codice di attivazione*. La chiave di licenza viene visualizzata nell'interfaccia dell'applicazione come sequenza alfanumerica univoca dopo essere stata aggiunta all'applicazione.

La chiave di licenza può essere bloccata da Kaspersky in caso di violazione delle condizioni del Contratto di licenza con l'utente finale. Se la chiave di licenza è stata bloccata, è necessario aggiungerne un'altra se si desidera utilizzare l'applicazione.

Una chiave di licenza può essere attiva o aggiuntiva (o di riserva).

Una *chiave di licenza attiva* è una chiave di licenza attualmente utilizzata dall'applicazione. È possibile aggiungere una chiave di licenza attiva per una licenza di prova o commerciale. L'applicazione non può avere più di una chiave di licenza attiva.

Una *chiave di licenza aggiuntiva (o di riserva)* è una chiave di licenza che concede all'utente il diritto di utilizzare l'applicazione, pur non essendo attualmente in uso. La chiave di licenza di riserva diventa automaticamente attiva alla scadenza della licenza associata alla chiave di licenza attiva corrente. Una chiave di licenza di riserva può essere aggiunta solo se è stata già aggiunta una chiave di licenza attiva.

Una chiave di licenza per una licenza di prova può essere aggiunta come chiave di licenza attiva. Non è possibile aggiungere come chiave di licenza di riserva una chiave di licenza per una licenza di prova.

Informazioni sul file chiave

Un *file chiave* è un file con estensione key fornito all'utente da Kaspersky. I file chiave sono progettati per attivare l'applicazione attraverso l'aggiunta di una chiave di licenza.

Il file chiave viene ricevuto all'indirizzo e-mail specificato al momento dell'acquisto di Kaspersky Security Center o dell'ordine della versione di prova di Kaspersky Security Center.

Non è necessario connettersi ai server di attivazione di Kaspersky per attivare l'applicazione con un file chiave.

È possibile ripristinare un file chiave eliminato accidentalmente. Un file chiave potrebbe ad esempio essere necessario per eseguire la registrazione a Kaspersky CompanyAccount.

Per ripristinare il file chiave, eseguire una delle seguenti azioni:

- Contattare il venditore della licenza.
- Ricevere un file chiave tramite il sito Web di Kaspersky utilizzando il codice di attivazione disponibile.
- Esportare un file della chiave di licenza da un altro Administration Server.

Informazioni sull'abbonamento

L'*abbonamento a Kaspersky Security Center* è un ordine per l'utilizzo dell'applicazione con le impostazioni selezionate (data di scadenza dell'abbonamento, numero di dispositivi protetti). È possibile registrare l'abbonamento a Kaspersky Security Center presso il provider di servizi (ad esempio il provider Internet). L'abbonamento può essere rinnovato manualmente o in modalità automatica; è possibile anche annullarlo.

Un abbonamento può essere limitato (ad esempio un anno) o illimitato (senza data di scadenza). Per continuare a utilizzare Kaspersky Security Center dopo la scadenza di un abbonamento limitato, è necessario rinnovarlo. L'abbonamento illimitato viene rinnovato automaticamente se il pagamento al provider di servizi è stato effettuato anticipatamente entro i termini.

Quando un abbonamento limitato scade, è possibile usufruire di un periodo di tolleranza per il rinnovo durante il quale l'applicazione continua a funzionare. La disponibilità e la durata del periodo di tolleranza sono definite dal provider di servizi.

Per utilizzare Kaspersky Security Center con abbonamento, è necessario applicare il codice di attivazione ricevuto dal provider di servizi.

È possibile applicare un codice di attivazione diverso per Kaspersky Security Center solo dopo la scadenza dell'abbonamento scade o in seguito all'annullamento.

A seconda del provider di servizi, il set di azioni possibili per la gestione dell'abbonamento può variare. Il provider di servizi potrebbe non fornire alcun periodo di tolleranza per il rinnovo dell'abbonamento, pertanto l'applicazione perde le funzionalità.

I codici di attivazione acquistati con l'abbonamento non possono essere utilizzati per attivare versioni precedenti di Kaspersky Security Center.

Quando si utilizza l'applicazione con abbonamento, Kaspersky Security Center tenta automaticamente di accedere al server di attivazione a intervalli di tempo specificati fino alla scadenza dell'abbonamento. Ciò garantisce che le informazioni sull'abbonamento siano sincronizzate con il server di attivazione. Se non è possibile accedere al server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. È possibile rinnovare l'abbonamento nel sito Web del provider di servizi.

È possibile aggiornare manualmente le informazioni sull'abbonamento, senza attendere che Kaspersky Security Center acceda al server di attivazione. Ad esempio, potrebbe essere utile quando si modificano le impostazioni dell'abbonamento.

Per aggiornare manualmente le informazioni sull'abbonamento:

1. Nella struttura della console selezionare la cartella **Licenze di Kaspersky**.
2. Fare clic su **Azioni aggiuntive** e, nell'elenco a discesa, selezionare **Sincronizza le impostazioni dell'abbonamento con il server di gestione delle licenze**.

Le informazioni sull'abbonamento vengono aggiornate nel server di attivazione.

Informazioni sul codice di attivazione

Codice di attivazione è una sequenza univoca di 20 caratteri alfanumerici. Il codice di attivazione viene inserito per aggiungere una chiave di licenza che consente di attivare Kaspersky Security Center. Il codice di attivazione viene ricevuto all'indirizzo e-mail specificato, in seguito all'acquisto di Kaspersky Security Center o all'ordine della versione di prova di Kaspersky Security Center.

Per attivare l'applicazione utilizzando un codice di attivazione, è necessario l'accesso a Internet per stabilire la connessione con i server di attivazione Kaspersky. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici.

Se l'applicazione è stata attivata con un codice di attivazione, l'applicazione in alcuni casi invia richieste ricorrenti ai server di attivazione di Kaspersky per verificare lo stato corrente della chiave di licenza. È necessario concedere all'applicazione l'accesso a Internet per consentire l'invio delle richieste.

Se è stato smarrito il codice di attivazione dopo l'installazione dell'applicazione, contattare il partner Kaspersky da cui è stata acquistata la licenza.

Non è possibile utilizzare file chiave per l'attivazione di applicazioni gestite; sono accettati solo i codici di attivazione.

Revoca del consenso a un Contratto di licenza con l'utente finale

Se si decide di interrompere la protezione dei dispositivi client, è possibile disinstallare le applicazioni Kaspersky gestite e revocare il Contratto di licenza con l'utente finale (EULA) per tali applicazioni.

Per revocare un EULA per le applicazioni Kaspersky gestite:

1. Nella struttura della console selezionare **Administration Server** → **Avanzate** →**Contratti di licenza con l'utente finale accettati**.

   Verrà visualizzato un elenco degli EULA accettati al momento della creazione dei pacchetti di installazione, dell'installazione immediata degli aggiornamenti o della distribuzione di Kaspersky Security for Mobile.

2. Nell'elenco selezionare il Contratto di licenza con l'utente finale che si desidera revocare.

   È possibile visualizzare le seguenti proprietà degli EULA:

   - Data di accettazione dell'EULA.
   - Nome dell'utente che ha accettato l'EULA.
   - Collegamento ai termini dell'EULA.
   - Elenco degli oggetti collegati al Contratto di licenza con l'utente finale: nomi dei pacchetti di installazione, nomi degli aggiornamenti immediati, nomi delle app mobili.

3. Fare clic sul pulsante **Revoca EULA**.

   Nella finestra visualizzata l'utente viene informato della necessità di disinstallare l'applicazione Kaspersky corrispondente all'EULA.

4. Fare clic sul pulsante per confermare la revoca.

   Kaspersky Security Center verifica se i pacchetti di installazione (corrispondenti all'applicazione Kaspersky gestita per cui si desidera revocare il Contratto di licenza con l'utente finale) sono stati eliminati.

   È possibile revocare il Contratto di licenza con l'utente finale solo per un'applicazione Kaspersky gestita i cui pacchetti di installazione vengono eliminati.

L'EULA è revocato. Non viene visualizzato nell'elenco dei Contratti di licenza con l'utente finale nella sezione **Administration Server → Avanzate → Contratti di licenza con l'utente finale accettati**. Non è possibile proteggere i dispositivi client utilizzando un'applicazione Kaspersky il cui EULA è stato revocato.

Informazioni sulla trasmissione dei dati

Dati trasferiti a terze parti

Quando si utilizza la funzionalità del Software Mobile Device Management, allo scopo di inviare in modo tempestivo i comandi ai dispositivi che eseguono il sistema operativo Android tramite il meccanismo delle notifiche push, viene utilizzato il servizio Google Firebase Cloud Messaging. Se l'Utente ha configurato l'utilizzo del servizio Google Firebase Cloud Messaging, l'Utente accetta di fornire le seguenti informazioni al servizio Google Firebase Cloud Messaging in modalità automatica: ID di installazione delle applicazioni Kaspersky Endpoint Security for Android a cui devono essere inviate le notifiche push.

Per bloccare lo scambio di informazioni con il servizio Google Firebase Cloud Messaging, l'Utente deve ripristinare i valori predefiniti delle impostazioni di utilizzo del servizio Google Firebase Cloud Messaging.

Quando si utilizza la funzionalità del Software Mobile Device Management, allo scopo di inviare in modo tempestivo i comandi ai dispositivi che eseguono il sistema operativo iOS tramite il meccanismo delle notifiche push, viene utilizzato il servizio Apple Push Notification Service (APNs). Se l'Utente ha installato un certificato APNs in un server per dispositivi mobili MDM iOS, ha creato un profilo MDM iOS con una raccolta di impostazioni per la connessione dei dispositivi mobili iOS al Software e ha installato questo profilo nei dispositivi mobili, l'Utente accetta di fornire le seguenti informazioni ad APNs in modalità automatica:

- Token - token push del dispositivo. Il server utilizza questo token quando invia notifiche push al dispositivo.
- PushMagic - stringa che deve essere inclusa nella notifica push. Il valore della stringa viene generato dal dispositivo.

Dati elaborati in locale

Kaspersky Security Center è progettato per l'esecuzione centralizzata delle attività di base di amministrazione e manutenzione nella rete di un'organizzazione. Kaspersky Security Center consente all'amministratore di accedere a informazioni dettagliate sul livello di protezione della rete dell'organizzazione; Kaspersky Security Center consente all'amministratore di configurare tutti i componenti della protezione in base alle applicazioni Kaspersky. Kaspersky Security Center esegue le seguenti funzioni principali:

- Rilevamento dei dispositivi e dei relativi utenti nella rete dell'organizzazione
- Creazione di una gerarchia di gruppi di amministrazione per la gestione dei dispositivi

- Installazione delle applicazioni Kaspersky nei dispositivi
- Gestione delle impostazioni e delle attività delle applicazioni installate
- Gestione degli aggiornamenti per Kaspersky e applicazioni di terze parti e rilevamento e correzione delle vulnerabilità
- Attivazione delle applicazioni Kaspersky nei dispositivi
- Gestione degli account utente
- Visualizzazione delle informazioni sul funzionamento delle applicazioni Kaspersky nei dispositivi
- Visualizzazione dei rapporti

Per eseguire le funzioni principali, Kaspersky Security Center può ricevere, archiviare ed elaborare le seguenti informazioni:

- Informazioni sui dispositivi nella rete dell'organizzazione ricevute tramite la scansione del dominio Windows, Active Directory o Samba o tramite la scansione degli intervalli IP. Administration Server ottiene i dati in modo indipendente o riceve i dati dal Network Agent che funge da punto di distribuzione.
- Informazioni da Active Directory e Samba su unità organizzative, domini, utenti e gruppi. Administration Server ottiene i dati in modo indipendente o riceve i dati dal Network Agent che funge da punto di distribuzione.
- Dettagli dei dispositivi gestiti. Network Agent trasferisce i dati elencati di seguito dal dispositivo ad Administration Server. L'utente inserisce il nome visualizzato e la descrizione del dispositivo nell'interfaccia di Administration Console o nell'interfaccia di Kaspersky Security Center Web Console:
  - Specifiche tecniche del dispositivo gestito e relativi componenti richiesti per l'identificazione del dispositivo: nome visualizzato e descrizione del dispositivo, tipo e nome del dominio Windows, nome del dispositivo nell'ambiente Windows, dominio DNS e nome DNS, indirizzo IPv4, indirizzo IPv6, numero di serie, posizione di rete, indirizzo MAC, tipo di sistema operativo, informazioni che indicano se il dispositivo è una macchina virtuale o meno e il tipo di hypervisor e informazioni che indicano se il dispositivo è una macchina virtuale dinamica nell'ambito di VDI.
  - Altre specifiche dei dispositivi gestiti e dei relativi componenti richieste per il controllo dei dispositivi gestiti e per le decisioni sull'applicabilità di patch e aggiornamenti specifici: stato di Windows Update Agent (WUA), architettura del sistema operativo, vendor del sistema operativo, numero di build del sistema operativo, ID di rilascio del sistema operativo, cartella della posizione del sistema operativo, tipo di macchina virtuale (se il dispositivo è una macchina virtuale); il nome dell'Administration Server virtuale che gestisce il dispositivo; i dati del dispositivo cloud (regione cloud, VPC, zona di disponibilità cloud, sottorete cloud, zona di collocazione cloud).
  - Dettagli delle azioni sui dispositivi gestiti: data e ora dell'ultimo aggiornamento, ora in cui il dispositivo è stato visibile per l'ultima volta nella rete, stato di attesa del riavvio e ora in cui il dispositivo è stato acceso.
  - Dettagli degli account utente del dispositivo e delle relative sessioni di lavoro.
- Dati ricevuti eseguendo la diagnostica remota in un dispositivo gestito: file di traccia, informazioni di sistema, dettagli delle applicazioni Kaspersky installate nel dispositivo, file di dump, registri eventi, risultati dell'esecuzione degli script di diagnostica ricevuti dall'Assistenza tecnica Kaspersky.
- Statistiche di funzionamento dei punti di distribuzione se il dispositivo è un punto di distribuzione. Network Agent trasferisce i dati dal dispositivo ad Administration Server.

- Impostazioni del punto di distribuzione immesse dall'Utente in Administration Console o Kaspersky Security Center Web Console.

- Dati necessari per la connessione dei dispositivi mobili ad Administration Server: certificato, porta per la connessione mobile, indirizzo di connessione di Administration Server. L'Utente immette i dati in Administration Console o in Kaspersky Security Center Web Console.

- Dettagli dei dispositivi mobili trasferiti tramite il protocollo MDM iOS. I dati elencati di seguito vengono trasferiti dal dispositivo mobile ad Administration Server:

    - Specifiche tecniche del dispositivo mobile e dei relativi componenti richiesti per l'identificazione del dispositivo: nome del dispositivo, modello, nome e numero di build del sistema operativo, numero di modello del dispositivo, numero IMEI, UDID, MEID, numero di serie, quantità di memoria, versione del firmware del modem, indirizzo MAC Bluetooth, indirizzo MAC Wi-Fi e dettagli sulla scheda SIM (ICCID nell'ambito dell'ID della scheda SIM).

    - Dettagli della rete mobile utilizzata dal dispositivo gestito: tipo di rete mobile, nome della rete mobile attualmente in uso, nome della rete mobile principale, versione delle impostazioni dell'operatore di rete mobile, stato di roaming per la voce e per i dati, codice paese della rete principale, codice del paese di residenza, codice del paese della rete attualmente in uso e livello di criptaggio.

    - Impostazioni di protezione del dispositivo mobile: utilizzo di una password e relativa conformità con le impostazioni del criterio, elenco dei profili di configurazione e dei profili di provisioning utilizzati per l'installazione delle applicazioni di terze parti.

    - Data dell'ultima sincronizzazione con Administration Server e stato di gestione del dispositivo.

- Dettagli delle applicazioni Kaspersky installate nel dispositivo. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent:

    - Impostazioni delle applicazioni Kaspersky installate nel dispositivo gestito: nome e versione dell'applicazione Kaspersky, stato, stato della protezione in tempo reale, data e ora dell'ultima scansione del dispositivo, numero delle minacce rilevate, numero di oggetti per i quali la disinfezione non è andata a buon fine, disponibilità e stato dei componenti dell'applicazione, ora dell'ultimo aggiornamento e versione dei database anti-virus, dettagli delle attività e delle impostazioni delle applicazioni Kaspersky, informazioni sulle chiavi di licenza attive e su quelle di riserva, ID e data di installazione dell'applicazione.

    - Statistiche sull'esecuzione dell'applicazione: eventi relativi alle modifiche dello stato dei componenti dell'applicazione Kaspersky nel dispositivo gestito e alle prestazioni delle attività avviate dai componenti dell'applicazione.

    - Stato del dispositivo definito dall'applicazione Kaspersky.

    - Tag assegnati dall'applicazione Kaspersky.

    - Set di aggiornamenti installati e applicabili per l'applicazione Kaspersky.

- Dati contenuti negli eventi dei componenti di Kaspersky Security Center e delle applicazioni Kaspersky gestite. Network Agent trasferisce i dati dal dispositivo ad Administration Server.

- Dati necessari per l'integrazione di Kaspersky Security Center con un sistema SIEM per l'esportazione degli eventi. L'Utente immette i dati in Administration Console o in Kaspersky Security Center Web Console.

- Impostazioni dei componenti Kaspersky Security Center e delle applicazioni Kaspersky gestite presenti nei criteri e nei profili criterio. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

- Impostazioni delle attività dei componenti Kaspersky Security Center e delle applicazioni Kaspersky gestite. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.
- Dati elaborati dalla funzionalità Vulnerability e patch management. Network Agent trasferisce i dati elencati di seguito dal dispositivo ad Administration Server:
  - Dettagli delle applicazioni e patch installate nei dispositivi gestiti (registro delle applicazioni).
  - Informazioni sull'hardware rilevato nei dispositivi gestiti (Registro hardware).

    Se Network Agent è installato in un dispositivo che esegue Windows, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo:

    - RAM
    - Dispositivi di archiviazione di massa
    - Scheda madre
    - CPU
    - Schede di rete
    - Monitor
    - Scheda video
    - Scheda audio

    Se Network Agent è installato in un dispositivo che esegue Linux o macOS, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo, se tali informazioni sono fornite dal sistema operativo:

    - Volume totale RAM
    - Volume totale dei dispositivi di archiviazione di massa
    - Scheda madre
    - CPU
    - Schede di rete
  - Dettagli delle vulnerabilità del software di terze parti rilevato nei dispositivi gestiti.
  - Dettagli degli aggiornamenti disponibili per le applicazioni di terze parti installate nei dispositivi gestiti.
  - Dettagli degli aggiornamenti Microsoft rilevati dalla funzionalità WSUS.
  - Elenco degli aggiornamenti Microsoft rilevati dalla funzionalità WSUS che devono essere installati nel dispositivo.
- Dati necessari per scaricare gli aggiornamenti in Administration Server isolato per correggere le vulnerabilità del software di terze parti nei dispositivi gestiti. L'utente immette e trasmette i dati utilizzando l'utilità klscflag di Administration Server.

- Dati necessari per la compatibilità di Kaspersky Security Center con gli ambienti cloud (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). L'Utente immette i dati in Administration Console o in Kaspersky Security Center Web Console.

- Categorie utente di applicazioni. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

- Elenco dei file eseguibili rilevati nei dispositivi gestiti dalla funzionalità Controllo Applicazioni. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Dettagli dei file presenti in Backup. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Dettagli dei file presenti in Quarantena. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Dettagli dei file richiesti dagli specialisti Kaspersky per l'analisi dettagliata. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Dettagli dello stato e attivazione delle regole di Controllo adattivo delle anomalie. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Dettagli dei dispositivi esterni (unità di memoria, strumenti di trasferimento delle informazioni, strumenti HCRP informativi e bus di connessione) installati o connessi al dispositivo gestito e rilevati dalla funzionalità Controllo Dispositivi. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Informazioni sui dispositivi criptati e sullo stato di criptaggio. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent.

- Dettagli degli errori di criptaggio dei dati nei dispositivi utilizzando la funzionalità Criptaggio dei dati delle applicazioni Kaspersky. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Elenco dei PLC (Programmable Logic Controller) gestiti. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Dati necessari per la creazione di una catena di sviluppo delle minacce. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Informazioni sui tentativi dei dipendenti di un'organizzazione di accedere ai servizi cloud. L'applicazione gestita trasferisce i dati dal dispositivo ad Administration Server tramite Network Agent. Un elenco completo di dati viene fornito nei file della Guida dell'applicazione corrispondente.

- Dati necessari per l'integrazione di Kaspersky Security Center con il servizio Kaspersky Managed Detection and Response (il plug-in dedicato deve essere installato per Kaspersky Security Center Web Console): token di avvio dell'integrazione, token di integrazione e token della sessione utente. L'Utente immette il token di avvio dell'integrazione nell'interfaccia di Kaspersky Security Center Web Console. Il servizio Kaspersky MDR trasferisce il token di integrazione e il token della sessione utente tramite il plug-in dedicato.

- Dettagli dei codici di attivazione immessi o dei file chiave specificati. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

- Account utente: nome, descrizione, nome completo, indirizzo e-mail, numero di telefono principale, password, chiave segreta generata da Administration Server e password monouso per la verifica in due passaggi. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

- Dati di cui IAM (Identity and Access Manager) ha bisogno per l'autenticazione centralizzata e per garantire Single Sign-on (SSO) tra le applicazioni Kaspersky integrate con Kaspersky Security Center: impostazioni di installazione e configurazione di IAM, sessione utente IAM, token IAM, stati delle applicazioni client e stati dei server delle risorse. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

- Cronologia delle revisioni degli oggetti di gestione. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

- Indirizzo IP del dispositivo in cui un utente ha creato una revisione. L'indirizzo IP viene definito automaticamente da Administration Server.

- Registro degli oggetti di gestione dettagliati. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

- Pacchetti di installazione creati dal file, nonché impostazioni di installazione. L'Utente immette i dati in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

- Dati necessari per la visualizzazione degli annunci di Kaspersky in Kaspersky Security Center Web Console. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Dati necessari per il funzionamento dei plug-in delle applicazioni gestite in Kaspersky Security Center Web Console e salvati dai plug-in nel database di Administration Server durante l'esecuzione standard. La descrizione e le modalità di invio dei dati sono specificate nei file della Guida dell'applicazione corrispondente.

- Impostazioni dell'utente di Kaspersky Security Center Web Console: lingua di localizzazione e tema dell'interfaccia, impostazioni di visualizzazione del riquadro Monitoraggio, informazioni sullo stato delle notifiche (Già letta/Non ancora letta), stato delle colonne nei fogli di calcolo (Mostra/Nascondi), avanzamento della modalità Training. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Registro eventi Kaspersky per i componenti Kaspersky Security Center e per le applicazioni Kaspersky gestite. Il registro eventi Kaspersky viene archiviato in ciascun dispositivo e non viene mai trasferito ad Administration Server.

- Certificato per la connessione sicura dei dispositivi gestiti ai componenti Kaspersky Security Center. L'utente immette i dati utilizzando l'utilità klsetsrvcert di Administration Server.

- Certificati per stabilire l'attendibilità delle risorse Web interne dell'organizzazione. L'Utente immette i dati nell'interfaccia di Kaspersky Security Center Web Console.

- Dati necessari per il funzionamento di Kaspersky Security Center negli ambienti cloud, come Amazon Web Services (AWS), Microsoft Azure, Google Cloud e Yandex.Cloud. Administration Server riceve i dati dalla macchina virtuale in cui viene eseguito.

- Informazioni sull'accettazione da parte dell'Utente dei termini e delle condizioni degli accordi legali con Kaspersky.

- I dati di Administration Server che l'Utente immette nei seguenti componenti:
  - Administration Console
  - Kaspersky Security Center Web Console
  - Terminale della riga di comando quando si utilizza l'utilità klscflag
  - Componenti che interagiscono con Administration Server tramite oggetti di automazione klakaut e Kaspersky Security Center OpenAPI
- Tutti i dati che l'Utente immette in Administration Console o nell'interfaccia di Kaspersky Security Center Web Console.

I dati elencati precedentemente possono essere presenti in Kaspersky Security Center se viene applicato uno dei seguenti metodi:

- L'Utente inserisce i dati nell'interfaccia dei seguenti componenti:
  - Administration Console
  - Kaspersky Security Center Web Console
  - Terminale della riga di comando quando si utilizza l'utilità klscflag
  - Componenti che interagiscono con Administration Server tramite oggetti di automazione klakaut e Kaspersky Security Center OpenAPI
- Network Agent riceve automaticamente i dati dal dispositivo e li trasferisce ad Administration Server.
- Network Agent riceve i dati recuperati dall'applicazione Kaspersky gestita e li trasferisce ad Administration Server. Gli elenchi dei dati elaborati dalle applicazioni Kaspersky gestite vengono forniti nei file della Guida per le applicazioni corrispondenti.
- Administration Server ottiene le informazioni sui dispositivi in rete in modo indipendente o riceve informazioni da un Network Agent che funge da punto di distribuzione.
- I dati vengono trasferiti dal dispositivo mobile ad Administration Server utilizzando il protocollo MDM iOS.

I dati elencati vengono archiviati nel database di Administration Server. Nomi utente e password sono archiviati in formato criptato.

Tutti i dati elencati precedentemente possono essere trasferiti a Kaspersky solo tramite file di dump, file di traccia o file di log dei componenti Kaspersky Security Center, tra cui i file di log creati da strumenti di installazione e utilità.

File di dump, file di traccia e file di log dei componenti Kaspersky Security Center contengono dati casuali di Administration Server, Network Agent, Administration Console, server MDM iOS e Kaspersky Security Center Web Console. Questi file possono contenere dati personali e sensibili. I file di dump, i file di traccia e i file di log sono archiviati nel dispositivo in formato non criptato. I file di dump, i file di traccia e i file di log non vengono trasferiti automaticamente a Kaspersky. L'amministratore può tuttavia trasferire manualmente i dati a Kaspersky su richiesta del Servizio di assistenza tecnica per la risoluzione dei problemi che si verificano durante l'esecuzione di Kaspersky Security Center.

Seguendo i collegamenti in Administration Console o Kaspersky Security Center Web Console, l'Utente accetta di trasferire automaticamente i seguenti dati:

- Codice di Kaspersky Security Center
- Versione Kaspersky Security Center
- Localizzazione di Kaspersky Security Center
- ID licenza
- Tipo di licenza
- Se la licenza è stata acquistata tramite un partner

L'elenco dei dati forniti tramite ciascun collegamento dipende dalla finalità e dalla posizione del collegamento.

Kaspersky utilizza i dati ricevuti in forma anonima e soltanto come statistiche generali. Le statistiche riassuntive vengono generate automaticamente dalle informazioni ricevute in origine e non contengono dati personali o riservati. Non appena vengono accumulati nuovi dati, i dati precedenti vengono cancellati (una volta all'anno). Le statistiche riassuntive vengono archiviate a tempo indeterminato.

Kaspersky protegge le informazioni ricevute in conformità alle leggi e ai regolamenti applicabili di Kaspersky. I dati vengono trasmessi tramite un canale sicuro.

Opzioni di licensing per Kaspersky Security Center

Kaspersky Security Center può funzionare nelle seguenti modalità:

- **Nessuna licenza (funzionalità di base)**

  Kaspersky Security Center funziona in questa modalità prima dell'attivazione dell'applicazione o dopo la scadenza della licenza commerciale. Kaspersky Security Center con il supporto delle funzionalità di base di Administration Console viene fornito insieme alle applicazioni Kaspersky per la protezione delle reti aziendali. Può inoltre essere scaricato dal sito Web di Kaspersky.

- **Licenza commerciale**

  Se sono necessarie funzionalità aggiuntive che non sono incluse nelle funzionalità di base di Administration Console, occorre acquistare una licenza commerciale.

  Quando si aggiunge una chiave di licenza nella finestra delle proprietà di Administration Server, assicurarsi di aggiungere una chiave di licenza che consente di utilizzare Kaspersky Security Center. Queste informazioni sono disponibili sul sito Web di Kaspersky. Ogni pagina Web della soluzione contiene l'elenco delle applicazioni incluse nella soluzione. Administration Server può accettare chiavi di licenza non supportate, ad esempio una chiave di licenza di Kaspersky Endpoint Security Cloud, ma tali chiavi di licenza non forniscono nuove funzionalità oltre alle funzionalità di base di Administration Console.

Funzionalità o proprietà	Modalità di funzionamento di Kaspersky Security Center	
	Nessuna licenza	Licenza commerciale
Funzionalità di base di Administration Console Sono disponibili le seguenti funzioni: • Creazione di Administration Server virtuali per gestire una rete di filiali remote o organizzazioni client. • Creazione di una gerarchia di gruppi di amministrazione per gestire dispositivi specifici come una singola entità. • Installazione remota delle applicazioni. • Configurazione centralizzata delle applicazioni installate nei dispositivi client. • Controllo dello stato della protezione anti-virus di un'organizzazione. • Gestione dei ruoli utente. • Statistiche e rapporti sul funzionamento dell'applicazione e notifiche sugli eventi critici. • Operazioni centralizzate con file spostati in Quarantena o Backup e file la cui elaborazione è stata rimandata. • Gestione del criptaggio e della protezione dei dati. • Visualizzazione e modifica di gruppi di applicazioni concesse in licenza esistenti. • Visualizzazione e modifica manuale dell'elenco di componenti hardware rilevati dal polling della rete. • Visualizzazione dell'elenco delle immagini dei sistemi operativi disponibili per l'installazione remota.	✓	✓
Vulnerability e patch management: funzionalità di base	✓	✓

Funzionalità o proprietà	Modalità di funzionamento di Kaspersky Security Center	
	Nessuna licenza	Licenza commerciale
Le seguenti attività non richiedono una licenza commerciale: • Attività *Trova vulnerabilità e aggiornamenti richiesti* Tramite questa attività, Kaspersky Security Center riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi gestiti. • L'attività *Installa aggiornamenti di Windows Update* Questa attività può essere utilizzata per installare solo gli aggiornamenti di Windows Update. Per utilizzare questa attività, è necessario specificare manualmente gli aggiornamenti richiesti nelle impostazioni dell'attività. • Attività *Correggi vulnerabilità* L'attività *Correggi vulnerabilità* utilizza le correzioni consigliate per il software Microsoft e le correzioni dell'utente per software di terze parti. Per utilizzare questa attività, è necessario specificare manualmente le correzioni dell'utente per le vulnerabilità nelle impostazioni dell'attività.		
Vulnerability e patch management: funzionalità avanzata Sono disponibili le seguenti funzioni: • Installazione remota degli aggiornamenti software e correzione automatica delle vulnerabilità, secondo le regole definite. • Utilizzo di Administration Server come server Windows Server Update Services (WSUS) per fornire aggiornamenti ai servizi Windows Update nei dispositivi in modalità centralizzata e con la frequenza impostata.	–	✓

Funzionalità o proprietà	Modalità di funzionamento di Kaspersky Security Center	
	Nessuna licenza	Licenza commerciale
Funzionalità Mobile Device Management nell'Administration Console basata su MMC La funzionalità Mobile Device Management viene utilizzata per gestire i dispositivi mobili MDM iOS e Android. Le seguenti funzioni sono disponibili per i dispositivi MDM iOS: • Aggiunta di nuovi dispositivi gestiti da Kaspersky Security Center. • Creazione e modifica di profili di configurazione, installazione dei profili di configurazione nei dispositivi mobili. • Installazione delle applicazioni nei dispositivi mobili tramite App Store® o utilizzando i file manifest (.plist) o i pacchetti di installazione mobile (.ipa). • Esecuzione dei comandi nei dispositivi MDM iOS, incluso il blocco dei dispositivi mobili, la reimpostazione della password del dispositivo mobile e l'eliminazione di tutti i dati dal dispositivo mobile. Le seguenti funzioni sono disponibili per i dispositivi Android: • Aggiunta di nuovi dispositivi gestiti da Kaspersky Security Center. • Gestione di Kaspersky Endpoint Security for Android tramite criteri. • Esecuzione dei comandi nei dispositivi. L'unità di misura della gestione per Mobile Device Management è un dispositivo mobile. Un dispositivo mobile viene considerato gestito quando si connette a un server per dispositivi mobili.	—	✓ (È necessario aggiungere una chiave di licenza alle proprietà di Administration Server).
Protezione dei dispositivi mobili in Kaspersky Security Center Web Console Kaspersky Security Center Web Console fornisce le seguenti funzionalità per gestire i dispositivi mobili Android e iOS: • Aggiunta di nuovi dispositivi gestiti da Kaspersky Security Center. • Gestione di Kaspersky Endpoint Security for Android e Kaspersky Security for iOS tramite criteri. • Invio di comandi ai dispositivi mobili tramite protocolli pertinenti ed esecuzione dei comandi.	—	✓ (È necessario aggiungere una chiave di licenza su ogni dispositivo mobile).

Funzionalità o proprietà	Modalità di funzionamento di Kaspersky Security Center	
	Nessuna licenza	Licenza commerciale
Gestione dei sistemi Sono disponibili le seguenti funzioni: • Installazione di sistemi operativi e applicazioni. Kaspersky Security Center consente di creare immagini dei sistemi operativi e distribuirle nei dispositivi client in rete, nonché di eseguire l'installazione remota delle applicazioni Kaspersky o di altri produttori. È possibile acquisire le immagini dei sistemi operativi dai dispositivi e trasferirle ad Administration Server. Le immagini dei sistemi operativi vengono archiviate in Administration Server in una cartella dedicata. L'immagine del sistema operativo di un dispositivo di riferimento viene acquisita e quindi creata attraverso un'attività di creazione del pacchetto di installazione. È possibile utilizzare le immagini ricevute per la distribuzione nei dispositivi della rete in cui non è stato ancora installato alcun sistema operativo. In questo caso, viene utilizzata una tecnologia denominata Preboot eXecution Environment (PXE). • Gestione gruppo di applicazioni concesse in licenza. • Autorizzazione remota di connessione ai dispositivi client tramite Connessione Desktop remoto, un componente di Microsoft® Windows®. • Connessione remota ai dispositivi client tramite Condivisione desktop Windows. • Connessione remota tramite **Visualizzatore sessione Desktop remoto Kaspersky**.	—	✓

Funzionalità o proprietà	Modalità di funzionamento di Kaspersky Security Center	
	Nessuna licenza	Licenza commerciale
Integrazione con gli ambienti cloud Kaspersky Security Center non solo funziona con i dispositivi in locale, ma fornisce anche speciali funzionalità per l'utilizzo in un ambiente cloud, come Configurazione guidata ambiente cloud. Kaspersky Security Center funziona con le seguenti macchine virtuali: • Istanze Amazon EC2 • Macchine virtuali Microsoft Azure • Istanze di macchine virtuali Google Cloud • Macchine virtuali Yandex.Cloud	—	✓
Esportazione degli eventi nei sistemi SIEM utilizzando il protocollo Syslog Utilizzando il protocollo Syslog è possibile inviare gli eventi che si verificano in Kaspersky Security Center Administration Server e nelle applicazioni Kaspersky installate nei dispositivi gestiti. Il protocollo Syslog è un protocollo standard per la registrazione dei messaggi. Può essere utilizzato per esportare gli eventi in qualsiasi sistema SIEM.	✓	✓

Funzionalità di gestione delle licenze di Kaspersky Security Center e delle applicazioni gestite

La gestione delle licenze di Administration Server e delle applicazioni gestite prevede quanto segue:

- È possibile aggiungere a un Administration Server una chiave di licenza o un codice di attivazione valido per attivare Vulnerability e patch management, Mobile Device Management o Integrazione con i sistemi SIEM. Alcune funzionalità di Kaspersky Security Center sono accessibili solo a seconda dei file chiave attivi o dei codici di attivazione validi aggiunti ad Administration Server.
- È possibile aggiungere più codici di attivazione e file chiave per applicazioni gestite nell'archivio di Administration Server.

Informazioni sulla gestione delle licenze di Kaspersky Security Center

Se una delle funzionalità concesse in licenza (ad esempio, Mobile Device Management) è stata attivata tramite un file chiave, ma si desidera utilizzare un'altra funzionalità concessa in licenza (ad esempio, Vulnerability e patch management), è necessario acquistare dal provider di servizi un file chiave che attivi entrambe le funzionalità e quindi attivare Administration Server utilizzando questo file chiave.

Funzionalità di gestione delle licenze delle applicazioni gestite

Per la gestione delle licenze delle applicazioni gestite, è possibile distribuire un codice di attivazione o un file chiave automaticamente o in un'altra modalità. Per distribuire un codice di attivazione o un file chiave possono essere applicati i seguenti metodi:

- Distribuzione automatica

  > Se si utilizzano diverse applicazioni gestite ed è necessario distribuire un file chiave specifico o un codice di attivazione specifico nei dispositivi, valutare altre modalità di distribuzione del codice di attivazione o del file chiave in questione.

  Kaspersky Security Center consente di distribuire automaticamente le chiavi di licenza disponibili nei dispositivi. Ad esempio, nell'archivio dell'Administration Server sono presenti tre chiavi di licenza. È stata selezionata la casella di controllo **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti** per tutte e tre le chiavi di licenza. Un'applicazione di protezione Kaspersky, ad esempio Kaspersky Endpoint Security for Windows, è installata nei dispositivi dell'organizzazione. Viene rilevato un nuovo dispositivo a cui deve essere distribuita una chiave di licenza. L'applicazione stabilisce, ad esempio, che due delle chiavi di licenza dell'archivio possono essere applicate al dispositivo: la chiave di licenza denominata *Key_1* e la chiave di licenza denominata *Key_2*. Una di queste chiavi di licenza viene distribuita nel dispositivo. In questo caso non è possibile prevedere quale delle due chiavi di licenza verrà distribuita nel dispositivo poiché la distribuzione automatica delle chiavi di licenza non offre nessuna attività di amministrazione.

  Quando una chiave di licenza viene distribuita, i dispositivi vengono ricalcolati per questa chiave di licenza. È necessario accertarsi che il numero di dispositivi in cui è stata distribuita la chiave di licenza non superi la limitazione licenza. Se il numero di dispositivi supera la limitazione licenza, a tutti i dispositivi non coperti dalla licenza verrà assegnato lo stato *Critico*.

- Aggiunta di un file chiave o di un codice di attivazione al pacchetto di installazione di un'applicazione gestita

  Se si installa un'applicazione gestita utilizzando un pacchetto di installazione, è possibile specificare un codice di attivazione o un file chiave nel pacchetto di installazione o nel criterio dell'applicazione. La chiave di licenza verrà distribuita nei dispositivi gestiti alla successiva sincronizzazione del dispositivo con Administration Server.

- Distribuzione tramite l'attività di aggiunta della chiave di licenza per un'applicazione gestita

  Se si sceglie di utilizzare l'attività di aggiunta della chiave di licenza per un'applicazione gestita, è possibile selezionare la chiave di licenza che deve essere distribuita nei dispositivi e selezionare i dispositivi nella modalità più opportuna, ad esempio selezionando un gruppo di amministrazione o una selezione dispositivi.

- Aggiunta manuale di un codice di attivazione o di un file chiave ai dispositivi

Applicazioni Kaspersky. Distribuzione centralizzata

In questa sezione vengono descritti i metodi per l'installazione remota delle applicazioni Kaspersky e la relativa rimozione dai dispositivi della rete.

> Prima di distribuire le applicazioni nei dispositivi client, verificare che l'hardware e il software dei dispositivi client soddisfino i rispettivi requisiti.

Network Agent è un componente che fornisce la connessione di Administration Server con i dispositivi client. Deve essere pertanto installato in ciascun dispositivo client, che deve essere connesso al sistema centralizzato di controllo remoto. Il dispositivo in cui è installato Administration Server può utilizzare solo la versione server di Network Agent, che viene installata e rimossa insieme ad Administration Server. Non è necessario installare Network Agent in tale dispositivo.

Network Agent può essere installato in remoto o in locale come qualsiasi applicazione. Durante la distribuzione centralizzata delle applicazioni di protezione tramite Administration Console, è possibile installare Network Agent insieme a tali applicazioni di protezione.

I Network Agent possono variare a seconda delle applicazioni Kaspersky con cui vengono utilizzati. In alcuni casi, Network Agent può essere installato solo in locale (per informazioni dettagliate, fare riferimento alla documentazione delle relative applicazioni). È necessario installare Network Agent in un dispositivo client una sola volta.

Le applicazioni Kaspersky sono gestite tramite Administration Console utilizzando i plug-in di gestione. Di conseguenza, per accedere all'interfaccia di gestione delle applicazioni mediante Kaspersky Security Center, il plug-in di gestione corrispondente deve essere installato nella workstation dell'amministratore.

È possibile eseguire l'installazione remota delle applicazioni dalla workstation dell'amministratore nella finestra principale di Kaspersky Security Center.

Per installare il software in remoto, è necessario creare un'attività di installazione remota.

L'attività creata per l'installazione remota verrà avviata in base alla relativa pianificazione. È possibile interrompere la procedura di installazione arrestando manualmente l'attività.

Se l'installazione remota di un'applicazione restituisce un errore, assicurarsi che siano soddisfatti i requisiti di preparazione del dispositivo.

È possibile monitorare lo stato di avanzamento dell'installazione remota delle applicazioni di Kaspersky in una rete utilizzando il rapporto sulla distribuzione.

Per informazioni dettagliate sulla gestione delle applicazioni elencate in Kaspersky Security Center, fare riferimento alla documentazione delle relative applicazioni.

Sostituzione di applicazioni di protezione di terzi

L'Installazione delle applicazioni di protezione Kaspersky tramite Kaspersky Security Center può richiedere la rimozione di software di terze parti incompatibile con l'applicazione da installare. Kaspersky Security Center offre diversi modi di rimuovere le applicazioni di terze parti.

Rimozione delle applicazioni incompatibili utilizzando il programma di installazione

Questa opzione è disponibile solo in Administration Console basata su Microsoft Management Console.

Il metodo del programma di installazione per la rimozione delle applicazioni incompatibili è supportato da vari tipi di installazione. Prima dell'installazione dell'applicazione di protezione, tutte le applicazioni incompatibili vengono rimosse automaticamente se nella finestra delle proprietà del pacchetto di installazione dell'applicazione di protezione (sezione **Applicazioni incompatibili**) è selezionata l'opzione **Disinstalla automaticamente le applicazioni incompatibili**.

Rimozione delle applicazioni incompatibili durante la configurazione dell'installazione remota di un'applicazione

È possibile abilitare l'opzione **Disinstalla automaticamente le applicazioni incompatibili** quando si configura l'installazione remota di un'applicazione di protezione. In Administration Console basata su Microsoft Management Console, questa opzione è disponibile nell'Installazione remota guidata. In Kaspersky Security Center Web Console, questa opzione è disponibile nella Distribuzione guidata della protezione. Quando questa opzione è abilitata, Kaspersky Security Center consente di rimuovere le applicazioni incompatibili prima di installare un'applicazione di protezione in un dispositivo gestito.

Istruzioni dettagliate:

- Administration Console: Rimozione delle applicazioni incompatibili tramite l'Installazione remota guidata
- Kaspersky Security Center Web Console: Rimozione delle applicazioni incompatibili prima dell'installazione

Rimozione delle applicazioni incompatibili tramite un'attività dedicata

Per rimuovere le applicazioni incompatibili, utilizzare l'attività **Disinstalla l'applicazione in remoto**. Questa attività deve essere eseguita nei dispositivi prima dell'attività di installazione dell'applicazione di protezione. Ad esempio, nell'attività di installazione è possibile selezionare il tipo di pianificazione **Al completamento di un'altra attività**, dove l'altra attività è **Disinstalla l'applicazione in remoto**.

Questo metodo di disinstallazione è consigliabile quando il programma di installazione dell'applicazione di protezione non è in grado di rimuovere correttamente un'applicazione incompatibile.

Istruzioni dettagliate per Administration Console: creazione di un'attività.

Installazione delle applicazioni tramite un'attività di installazione remota

Kaspersky Security Center consente di installare le applicazioni nei dispositivi in remoto, utilizzando le attività di installazione remota. Tali attività vengono create e assegnate ai dispositivi attraverso un'apposita procedura guidata. Per assegnare un'attività più in modo facile e rapido, è possibile specificare i dispositivi (fino a 1000 dispositivi) nella finestra della procedura guidata in uno dei seguenti modi:

- **Seleziona i dispositivi della rete rilevati da Administration Server**. In questo caso l'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**. È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

- **Assegna un'attività a una selezione dispositivi**. In questo caso l'attività viene assegnata ai dispositivi inclusi in una selezione creata precedentemente. È possibile specificare la selezione predefinita o una selezione personalizzata creata.

- **Assegna un'attività a un gruppo di amministrazione**. In questo caso l'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione creato precedentemente.

Per evitare problemi che possono verificarsi durante l'installazione dell'applicazione in un dispositivo client senza Network Agent installato, è necessario procedere come descritto nella distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center.

Installazione di un'applicazione nei dispositivi selezionati

Per installare un'applicazione nei dispositivi selezionati:

1. Nella struttura della console selezionare la cartella **Attività**.

2. Eseguire la creazione dell'attività facendo clic sul pulsante **Crea attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

   Nella finestra **Selezionare il tipo di attività** della Creazione guidata nuova attività, nel nodo **Kaspersky Security Center Administration Server**, selezionare **Installa l'applicazione in remoto** come tipo di attività.

   Verrà creata un'attività per l'installazione remota dell'applicazione selezionata per dispositivi specifici. La nuova attività creata viene visualizzata nell'area di lavoro della cartella **Attività**.

3. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di installazione remota, l'applicazione selezionata verrà installata nei dispositivi selezionati.

Installazione di un'applicazione nei dispositivi client di un gruppo di amministrazione

Per installare un'applicazione nei dispositivi client di un gruppo di amministrazione:

1. Stabilire una connessione all'Administration Server che controlla i gruppi di amministrazione desiderati.

2. Selezionare un gruppo di amministrazione nella struttura della console.

3. Nell'area di lavoro del gruppo selezionare la scheda **Attività**.

4. Eseguire la creazione dell'attività facendo clic sul pulsante **Crea attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

   Nella finestra **Selezionare il tipo di attività** della Creazione guidata nuova attività, nel nodo **Kaspersky Security Center Administration Server**, selezionare **Installa l'applicazione in remoto** come tipo di attività.

   Verrà creata un'attività di gruppo per l'installazione remota dell'applicazione selezionata. La nuova attività verrà visualizzata nell'area di lavoro del gruppo di amministrazione, nella scheda **Attività**.

5. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di installazione remota, l'applicazione selezionata verrà installata nei dispositivi client nel gruppo di amministrazione.

Installazione di un'applicazione utilizzando i criteri di gruppo di Active Directory

Kaspersky Security Center consente di installare le applicazioni Kaspersky nei dispositivi gestiti utilizzando i criteri di gruppo di Active Directory.

È possibile installare le applicazioni tramite i criteri di gruppo di Active Directory solo da pacchetti di installazione che includono Network Agent.

Per installare un'applicazione utilizzando i criteri di gruppo di Active Directory:

1. Avviare la configurazione dell'installazione dell'applicazione utilizzando l'Installazione remota guidata.
2. Nella finestra **Definizione delle impostazioni dell'attività di installazione remota** dell'Installazione remota guidata selezionare l'opzione **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory**.
3. Nella finestra **Selezionare gli account per l'accesso ai dispositivi** dell'Installazione remota guidata selezionare l'opzione **Account richiesto (Network Agent non utilizzato)**.
4. Aggiungere l'account con privilegi di amministratore nel dispositivo in cui è installato Kaspersky Security Center o l'account incluso nel gruppo di dominio Proprietari autori criteri di gruppo.

5. Concedere le autorizzazioni all'account selezionato:

    a. Accedere a **Pannello di controllo** → **Strumenti di amministrazione** e aprire **Gestione Criteri di gruppo**.

    b. Fare clic sul nodo con il dominio desiderato.

    c. Fare clic sulla sezione **Delega**.

    d. Nell'elenco a discesa **Autorizzazione** selezionare **Collega oggetti Criteri di gruppo**.

    e. Fare clic su **Aggiungi**.

    f. Nella finestra **Seleziona utente, computer o gruppo** visualizzata selezionare l'account necessario.

    g. Fare clic su **OK** per chiudere la finestra **Seleziona utente, computer o gruppo**.

    h. Nell'elenco **Gruppi e utenti** selezionare l'account appena aggiunto, quindi fare clic su **Avanzate** → **Avanzate**.

    i. Nell'elenco **Autorizzazioni** fare doppio clic sull'account appena aggiunto.

    j. Concedere le seguenti autorizzazioni:

    - **Creare oggetti Criteri di gruppo**
    - **Eliminare oggetti Criteri di gruppo**
    - **Creare oggetti del contenitore Criteri di gruppo**
    - **Eliminare oggetti dal contenitore Criteri di gruppo**

    k. Fare clic su **OK** per salvare le modifiche.

6. Definire altre impostazioni seguendo le istruzioni della procedura guidata.

7. Eseguire l'attività di installazione remota creata manualmente o attenderne l'avvio pianificato.

Verrà avviata la seguente sequenza di installazione remota:

1. Durante l'esecuzione dell'attività, verranno creati i seguenti oggetti nel dominio che include i dispositivi client per il set specificato:

    - Oggetto Criteri di gruppo denominato **Kaspersky_AK{GUID}**.
    - Un gruppo di protezione che corrisponde all'oggetto Criteri di gruppo. Questo gruppo di protezione include i dispositivi client coperti dall'attività. Il contenuto del gruppo di protezione definisce l'ambito dell'oggetto Criteri di gruppo.

2. Kaspersky Security Center installa le applicazioni Kaspersky selezionate nei dispositivi client direttamente da KLSHARE, ovvero la cartella di rete condivisa dell'applicazione. Nella cartella di installazione di Kaspersky Security Center verrà creata una sottocartella ausiliaria che contiene il file .msi per l'applicazione da installare.

3. Quando si aggiungono nuovi dispositivi all'ambito dell'attività, questi vengono aggiunti al gruppo di protezione al successivo avvio dell'attività. Se nella pianificazione dell'attività è selezionata l'opzione **Esegui attività non effettuate**, i dispositivi vengono aggiunti al gruppo di protezione immediatamente.

4. Quando si eliminano dispositivi dall'ambito dell'attività, questi vengono eliminati dal gruppo di protezione al successivo avvio dell'attività.

5. Quando si elimina un'attività da Active Directory, vengono eliminati anche l'oggetto Criteri di gruppo, il collegamento all'oggetto Criteri di gruppo e il gruppo di protezione corrispondente.

Se si desidera applicare un altro schema di installazione tramite Active Directory, è possibile configurare manualmente le impostazioni richieste. Questa operazione può essere ad esempio necessaria nei seguenti casi:

- Quando l'amministratore della protezione anti-virus non dispone dei diritti necessari per apportare modifiche ad Active Directory per determinati domini
- Quando il pacchetto di installazione originale deve essere archiviato in una risorsa di rete distinta
- Quando è necessario collegare un oggetto Criteri di gruppo a specifiche unità Active Directory

Sono disponibili le seguenti opzioni per l'utilizzo di uno schema di installazione alternativo tramite Active Directory:

- Se è necessario eseguire l'installazione direttamente dalla cartella condivisa di Kaspersky Security Center, nelle proprietà dell'oggetto Criteri di gruppo specificare il file .msi presente nella sottocartella exec della cartella del pacchetto di installazione per l'applicazione desiderata.
- Se il pacchetto di installazione deve essere posizionato in un'altra risorsa di rete, copiare in tale risorsa l'intero contenuto della cartella exec, perché questa contiene, oltre al file con estensione .msi, i file di configurazione generati al momento della creazione del pacchetto. Per installare la chiave di licenza insieme all'applicazione, copiare anche il file chiave in questa cartella.

Installazione remota delle applicazioni nei dispositivi macOS

Per installare le applicazioni nei dispositivi in cui viene eseguito macOS utilizzando un'attività di installazione remota:

1. Creare un archivio costituito da un pacchetto di installazione e da uno script di installazione .sh.

2. Disabilitare l'opzione **Verifica il tipo di sistema operativo prima del download** nella procedura guidata Nuova attività.

In alternativa, è possibile utilizzare l'attività **Esegui script da remoto**. Il seguente articolo descrive come configurare i file per questa attività: Installazione da remoto delle applicazioni nei dispositivi utilizzando l'attività Esegui script da remoto.

Installazione di applicazioni negli Administration Server secondari

Per installare un'applicazione negli Administration Server secondari:

1. Stabilire una connessione all'Administration Server che controlla gli Administration Server secondari desiderati.

2. Verificare che il pacchetto di installazione corrispondente all'applicazione da installare sia disponibile in ognuno degli Administration Server secondari selezionati. Se il pacchetto di installazione risulta mancante in uno qualsiasi dei server secondari, distribuirlo utilizzando l'attività di distribuzione pacchetto di installazione.

3. Creare l'attività di installazione dell'applicazione negli Administration Server secondari in uno dei seguenti modi:

   - Se si desidera creare un'attività per gli Administration Server secondari nel gruppo di amministrazione selezionato, creare un'attività di gruppo di installazione remota per questo gruppo.
   - Se si desidera creare un'attività per specifici Administration Server secondari, creare un'attività di installazione remota per dispositivi specifici.

   Verrà avviata la Creazione guidata attività di distribuzione per guidare l'utente durante la creazione dell'attività di installazione remota. Seguire le istruzioni della procedura guidata.

   Nella finestra **Selezionare il tipo di attività** della Creazione guidata nuova attività, nella sezione **Kaspersky Security Center Administration Server**, aprire la cartella **Avanzate** e selezionare **Installa l'applicazione negli Administration Server secondari in remoto** come tipo di attività.

   Verrà creata l'attività per l'installazione remota dall'applicazione selezionata in specifici Administration Server secondari.

4. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di installazione remota, l'applicazione selezionata verrà installata negli Administration Server secondari.

Installazione delle applicazioni tramite l'Installazione remota guidata

Per installare le applicazioni Kaspersky, è possibile utilizzare l'Installazione remota guidata. L'Installazione remota guidata consente l'installazione remota delle applicazioni con pacchetti di installazione creati appositamente o direttamente da un pacchetto di distribuzione.

Per il corretto funzionamento dell'attività di installazione remota in un dispositivo client in cui non è installato Network Agent, le seguenti porte devono essere aperte: TCP 139 e 445, UDP 137 e 138. Per impostazione predefinita, queste porte sono aperte per tutti i dispositivi inclusi nel dominio. In caso di errori di rete, fare riferimento alla knowledge base di Kaspersky Security Center.

Per installare un'applicazione nei dispositivi selezionati utilizzando l'Installazione remota guidata:

1. Nella struttura della console individuare la cartella **Installazione remota** e selezionare la sottocartella **Pacchetti di installazione**.
2. Nell'area di lavoro della cartella selezionare il pacchetto di installazione dell'applicazione da installare.
3. Nel menu di scelta rapida del pacchetto di installazione selezionare **Installa applicazione**.

   Verrà avviata l'Installazione remota guidata.

4. Nella finestra **Selezionare i dispositivi per l'installazione** è possibile creare un elenco di dispositivi in cui verrà installata l'applicazione:

   - **Installa in un gruppo di dispositivi gestiti**

     Se questa opzione è selezionata, l'attività di installazione remota viene creata per un gruppo di dispositivi.

   - **Selezionare i dispositivi per l'installazione**

     Se questa opzione è selezionata, l'attività di installazione remota viene creata per dispositivi specifici. Questi dispositivi specifici possono includere sia dispositivi gestiti che dispositivi non assegnati.

5. Nella finestra **Definizione delle impostazioni dell'attività di installazione remota** specificare le impostazioni per l'installazione remota dell'applicazione.

   Nel gruppo di impostazioni **Forza il download del pacchetto di installazione** specificare la modalità di distribuzione dei file necessari per l'installazione dell'applicazione ai dispositivi client:

   - **Utilizzando Network Agent**

     Se questa opzione è abilitata, i pacchetti di installazione vengono distribuiti ai dispositivi client da Network Agent installato nei dispositivi client.

     Se questa opzione è disabilitata, i pacchetti di installazione vengono distribuiti utilizzando gli strumenti del sistema operativo dei dispositivi client.

     È consigliabile abilitare questa opzione se l'attività è stata assegnata a dispositivi in cui sono installati Network Agent.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Utilizzando le risorse del sistema operativo tramite Administration Server**

     Se questa opzione è selezionata, i file vengono trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo dei dispositivi client tramite l'Administration Server. È possibile abilitare questa opzione se Network Agent non è installato nel dispositivo client, ma il dispositivo client si trova nella stessa rete di Administration Server.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**

     Se questa opzione è abilitata, i pacchetti di installazione verranno trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo tramite i punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete.

     Se l'opzione **Utilizzo di Network Agent** è abilitata, i file vengono inviati tramite gli strumenti del sistema operativo solo se gli strumenti di Network Agent non sono disponibili.

     Per impostazione predefinita, questa opzione è abilitata per le attività di installazione remota create in un Administration Server virtuale.

   - **Numero di tentativi di installazione**

Se, durante l'esecuzione dell'attività Installazione remota, Kaspersky Security Center non riesce a installare un'applicazione in un dispositivo gestito entro il numero di esecuzioni del programma di installazione specificate dal parametro, Kaspersky Security Center interrompe la distribuzione del pacchetto di installazione a tale dispositivo gestito e non avvia più il programma di installazione nel dispositivo.

L'opzione `Numero di tentativi di installazione` consente di salvare le risorse del dispositivo gestito, nonché di ridurre il traffico (disinstallazione, esecuzione del file MSI e messaggi di errore).

I tentativi ricorrenti di avvio dell'attività possono indicare un problema nel dispositivo che impedisce l'installazione. L'amministratore deve risolvere il problema entro il numero specificato di tentativi di installazione (ad esempio assegnando spazio su disco sufficiente, rimuovendo le applicazioni incompatibili o modificando le impostazioni di altre applicazioni che impediscono l'installazione) e riavviare l'attività (manualmente o in base a una pianificazione).

Se l'installazione non va a buon fine, il problema è ritenuto irrisolvibile e ulteriori tentativi di avvio dell'attività sono considerati dispendiosi in termini di risorse e traffico.

Quando viene creata l'attività, il numero di tentativi è impostato su `0`. Per ogni esecuzione del programma di installazione che restituisce un errore nel dispositivo il numero aumenta.

Se il numero di tentativi specificati nel parametro è stato superato e il dispositivo è pronto per l'installazione dell'applicazione, è possibile aumentare il valore del parametro `Numero di tentativi di installazione` e avviare l'attività per installare l'applicazione. In alternativa, è possibile creare una nuova attività Installazione remota.

Definire come procedere con i dispositivi client gestiti da un altro Administration Server:

- **Installa in tutti i dispositivi**

  L'applicazione verrà installata anche nei dispositivi gestiti da altri Administration Server.

  Questa opzione è selezionata per impostazione predefinita. Non è necessario modificare l'impostazione se si dispone di un solo Administration Server nella rete.

- **Installa solo nei dispositivi gestiti tramite questo Administration Server**

  L'applicazione verrà installata solo nei dispositivi gestiti da questo Administration Server. Selezionare questa opzione se si dispone di più Administration Server nella rete per evitare conflitti tra di essi.

Definire le impostazioni aggiuntive:

- **Non reinstallare l'applicazione se è già installata**

  Se questa opzione è abilitata, l'applicazione selezionata non verrà reinstallata se è già stata installata nel dispositivo client.

  Se questa opzione è disabilitata, l'applicazione verrà installata in ogni caso.

  Per impostazione predefinita, questa opzione è abilitata.

- **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory**

Se questa opzione è abilitata, un pacchetto di installazione viene installato utilizzando i criteri di gruppo di Active Directory.

Questa opzione è disponibile se il pacchetto di installazione di Network Agent è selezionato.

Per impostazione predefinita, questa opzione è disabilitata.

6. Nella finestra **Selezione di una chiave di licenza** selezionare una chiave di licenza e un metodo per la relativa distribuzione:

- **Non inserire la chiave di licenza nel pacchetto di installazione (opzione consigliata)**

  La chiave viene distribuita automaticamente a tutti i dispositivi con cui è compatibile:
  - Se la distribuzione automatica è stata abilitata nelle proprietà della chiave.
  - Se l'attività **Aggiungi chiave** è stata creata.

- **Inserire la chiave di licenza nel pacchetto di installazione**

  La chiave verrà distribuita ai dispositivi insieme al pacchetto di installazione.

  Non è consigliabile distribuire la chiave utilizzando questo metodo poiché i diritti di accesso condiviso in lettura sono abilitati nell'archivio dei pacchetti di installazione.

La finestra **Selezione di una chiave di licenza** è visualizzata se il pacchetto di installazione non include alcuna chiave di licenza.

Se il pacchetto di installazione include una chiave di licenza, viene visualizzata la finestra **Proprietà chiave di licenza**, contenente i dettagli della chiave.

7. Nella finestra **Selezione dell'opzione per il riavvio del sistema operativo** specificare se i dispositivi devono essere riavviati o meno se è necessario il riavvio del sistema operativo durante l'installazione delle applicazioni:

- **Non riavviare il dispositivo**

  Se questa opzione è selezionata, il dispositivo non verrà riavviato dopo l'installazione dell'applicazione di protezione.

- **Riavvia il dispositivo**

  Se questa opzione è selezionata, il dispositivo verrà riavviato dopo l'installazione dell'applicazione di protezione.

- **Richiedi l'intervento dell'utente**

  Se questa opzione è selezionata, dopo l'installazione di un'applicazione di protezione verrà visualizzata una notifica che informa l'utente della necessità di riavviare il dispositivo. Utilizzando il collegamento **Modifica**, è possibile modificare il testo del messaggio, il periodo di visualizzazione del messaggio e l'ora del riavvio automatico.

  Per impostazione predefinita, questa opzione è selezionata.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

  Se questa opzione è abilitata, viene forzata la chiusura delle applicazioni nei dispositivi bloccati prima del riavvio.

  Per impostazione predefinita, questa opzione è disabilitata.

8. Nella finestra **Selezionare gli account per l'accesso ai dispositivi** è possibile aggiungere gli account che saranno utilizzati per avviare l'attività Installazione remota:

   - **Nessun account richiesto (Network Agent installato)**

     Se questa opzione è selezionata, non è necessario specificare un account con cui verrà eseguito il programma di installazione dell'applicazione. L'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

     Se Network Agent non è stato installato nei dispositivi client, questa opzione non è disponibile.

   - **Account richiesto (Network Agent non utilizzato)**

     Selezionare questa opzione se Network Agent non è installato nei dispositivi a cui si assegna l'attività di installazione remota. In questo caso, è possibile specificare un account utente o un certificato SSH per installare l'applicazione.

     - **Account locale**. Se questa opzione è selezionata, specificare l'account utente con cui verrà eseguito il programma di installazione dell'applicazione. Fare clic sul pulsante **Aggiungi**, selezionare **Account locale** e quindi specificare le credenziali dell'account utente.

       È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi per cui si assegna l'attività. In questo caso, tutti gli account aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

     - **Certificato SSH**. Se si desidera installare un'applicazione in un dispositivo client basato su Linux, è possibile specificare un certificato SSH anziché un account utente. Fare clic sul pulsante **Aggiungi**, selezionare **Certificato SSH**, quindi specificare la chiave privata e quella pubblica del certificato.

       Per generare una chiave privata, è possibile utilizzare l'utilità ssh-keygen. Si noti che Kaspersky Security Center supporta il formato PEM delle chiavi private, ma l'utilità ssh-keygen genera chiavi SSH nel formato OPENSSH per impostazione predefinita. Il formato OPENSSH non è supportato da Kaspersky Security Center. Per creare una chiave privata nel formato PEM supportato, aggiungere l'opzione -m PEM nel comando ssh-keygen. Ad esempio:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail dell'utente>"
       ```

9. Nella finestra **Avvio dell'installazione** fare clic sul pulsante **Avanti** per creare e avviare un'attività Installazione remota nei dispositivi selezionati.

   Se la finestra **Avvio dell'installazione** ha l'opzione **Non eseguire l'attività dopo il completamento dell'installazione remota guidata** selezionata, l'attività di installazione remota non verrà avviata. È possibile avviare manualmente questa attività in un secondo momento. Il nome dell'attività corrisponde al nome del pacchetto di installazione per l'applicazione: **installazione di <Nome del pacchetto di installazione>**.

Per installare l'applicazione nei dispositivi in un gruppo di amministrazione utilizzando l'Installazione remota guidata:

1. Stabilire una connessione all'Administration Server che controlla i gruppi di amministrazione desiderati.
2. Selezionare un gruppo di amministrazione nella struttura della console.
3. Nell'area di lavoro del gruppo fare clic sul pulsante **Esegui azione** e selezionare **Installa applicazione** nell'elenco a discesa.

   Verrà avviata l'Installazione remota guidata. Seguire le istruzioni della procedura guidata.

4. Durante il passaggio finale della procedura guidata, fare clic su **Avanti** per creare ed eseguire un'attività di installazione remota nei dispositivi selezionati.

Al termine dell'Installazione remota guidata, Kaspersky Security Center esegue le seguenti azioni:

- Creazione di un pacchetto di installazione per l'installazione dell'applicazione (se non è già stato creato). Il pacchetto di installazione è disponibile nella cartella **Installazione remota** della sottocartella **Pacchetti di installazione** e ha un nome che corrisponde al nome e alla versione dell'applicazione. È possibile utilizzare questo pacchetto di installazione per l'installazione dell'applicazione in futuro.

- Creazione ed esecuzione di un'attività di installazione remota per dispositivi specifici o per un gruppo di amministrazione. La nuova attività di installazione remota creata viene memorizzata nella cartella **Attività** o viene aggiunta alle attività del gruppo di amministrazione per cui è stata creata. È possibile avviare manualmente questa attività in un secondo momento. Il nome dell'attività corrisponde al nome del pacchetto di installazione per l'applicazione: **installazione di <Nome del pacchetto di installazione>**.

Utilizzo dei plug-in di gestione

Le applicazioni Kaspersky sono gestite tramite Administration Console utilizzando i plug-in di gestione. Ciascuna applicazione Kaspersky che può essere gestita tramite Kaspersky Security Center include un plug-in di gestione. Utilizzando il plug-in di gestione dell'applicazione, è possibile eseguire le seguenti azioni in Administration Console:

- Creare e modificare le impostazioni e i criteri dell'applicazione, nonché le impostazioni delle attività dell'applicazione.

- Ottenere informazioni sulle attività dell'applicazione, sugli eventi che si verificano durante l'esecuzione e sulle statistiche di esecuzione dell'applicazione ricevute dai dispositivi client.

Per controllare l'elenco dei plug-in installati e le relative versioni:

1. Nella struttura di Administration Console, fare clic con il pulsante destro del mouse su **Administration Server <nome_server>** e selezionare **Proprietà**.

2. Fare clic su **Avanzate** → **Dettagli dei plug-in di gestione applicazioni installati**.

L'elenco dei plug-in di gestione installati e delle relative versioni viene visualizzato nel riquadro a destra.

È possibile installare i plug-in per le applicazioni gestite quando si esegue l'Avvio rapido guidato di Administration Server durante la configurazione iniziale di Kaspersky Security Center. Inoltre, è possibile installare manualmente i plug-in di gestione.

Per installare manualmente un plug-in di gestione:

1. Scaricare il plug-in di gestione per l'applicazione Kaspersky e la versione richiesta (ad esempio, Kaspersky Endpoint Security for Windows 12.6) dalla pagina Web dell'Assistenza tecnica Kaspersky.

2. Se Administration Console è in esecuzione, chiuderlo.

3. Decomprimere il file del plug-in scaricato ed eseguire il file klcfginst.msi o klcfginst.exe. Seguire le istruzioni dell'installazione guidata.

4. Al termine dell'installazione, eseguire Administration Console e verificare che il plug-in sia presente nell'elenco dei plug-in installati, come descritto nella procedura precedente.

Quando si esegue Administration Console dopo l'installazione di un plug-in di gestione che supporta l'Avvio rapido guidato delle applicazioni gestite, questa procedura guidata viene avviata automaticamente. È possibile eseguire i passaggi dell'Avvio rapido guidato delle applicazioni gestite per creare attività e criteri predefiniti dell'applicazione Kaspersky. La procedura guidata si avvia automaticamente solo quando si esegue Administration Console dopo l'installazione iniziale del plug-in o dopo aver aggiornato il plug-in di gestione a una versione compatibile con un'altra versione dell'applicazione Kaspersky per la quale non sono stati ancora creati attività e criteri. È inoltre possibile avviare manualmente l'Avvio rapido guidato delle applicazioni gestite.

Per avviare manualmente l'Avvio rapido guidato delle applicazioni gestite:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Nel menu di scelta rapida del nodo di Administration Server, selezionare **Tutte le attività → Avvio rapido guidato delle applicazioni gestite**.
3. L'Avvio rapido guidato delle applicazioni gestite viene avviato. Seguire i passaggi della procedura guidata per creare le attività e i criteri predefiniti dell'applicazione Kaspersky.

Per rimuovere un plug-in di gestione:

1. Se Administration Console è in esecuzione, chiuderlo.
2. Aprire l'editor del registro di sistema di Windows.
3. Trovare la seguente chiave:
   - `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins` per sistemi a 32 bit.
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins` per sistemi a 64 bit.

   La chiave contiene i plug-in di gestione installati. Per ogni plug-in, il valore `DisplayName` contiene il nome del plug-in e il valore `UninstallString` contiene il comando per disinstallare il plug-in.
4. Trovare la chiave del plug-in che si desidera disinstallare e copiarne il valore `UninstallString` negli appunti.
5. Incollare il valore nella stringa di comando ed eseguirlo con diritti di amministratore di sistema.

La versione del plug-in di gestione non deve essere precedente alla versione dell'applicazione gestita Kaspersky. Se si aggiorna l'applicazione Kaspersky nei dispositivi, è necessario installare il plug-in di gestione della stessa versione.

Quando si apre il criterio creato in una versione precedente del plug-in, verrà chiesto di accettare l'informativa di Kaspersky Security Network.

Quando si disinstalla Kaspersky Security Center Web Console, vengono disinstallati anche tutti i plug-in di gestione.

Se si apre e si salva il criterio nella versione del plug-in successiva a quella dell'applicazione gestita, il criterio verrà aggiornato e non sarà possibile aprirlo nel plug-in della versione precedente.

Visualizzazione di un rapporto sulla distribuzione della protezione

È possibile utilizzare il rapporto sulla distribuzione della protezione per monitorare l'avanzamento della distribuzione della protezione della rete.

Per visualizzare un rapporto sulla distribuzione della protezione:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Nella cartella **Rapporti** dell'area di lavoro selezionare il modello di rapporto denominato **Rapporto sulla distribuzione della protezione**.

Nell'area di lavoro verrà visualizzato un rapporto con informazioni sulla distribuzione della protezione in tutti i dispositivi in rete.

È possibile generare un nuovo rapporto sulla distribuzione della protezione e specificare il tipo di dati da includere:

- Per un gruppo di amministrazione
- Per dispositivi specifici
- Per una selezione dispositivi
- Per tutti i dispositivi

Kaspersky Security Center presuppone che la protezione sia distribuita in un dispositivo se è installata un'applicazione di protezione ed è abilitata la protezione in tempo reale.

Rimozione remota delle applicazioni

Kaspersky Security Center consente di disinstallare le applicazioni dai dispositivi in remoto, utilizzando le attività di disinstallazione remota. Tali attività vengono create e assegnate ai dispositivi attraverso un'apposita procedura guidata. Per assegnare un'attività ai dispositivi più in modo facile e rapido, è possibile specificare i dispositivi nella finestra della procedura guidata in uno dei seguenti modi:

- **Seleziona i dispositivi della rete rilevati da Administration Server**. In questo caso l'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.
- **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**. È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

- **Assegna un'attività a una selezione dispositivi**. In questo caso l'attività viene assegnata ai dispositivi inclusi in una selezione creata precedentemente. È possibile specificare la selezione predefinita o una selezione personalizzata creata.

- **Assegna un'attività a un gruppo di amministrazione**. In questo caso l'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione creato precedentemente.

Problemi di rimozione remota

Quando si esegue la rimozione remota di applicazioni di terzi, gli amministratori potrebbero visualizzare un avviso che recita: "La disinstallazione remota è terminata su questo dispositivo con avvisi: l'applicazione per la rimozione delle applicazioni non è installata". Questo problema si verifica in genere quando l'applicazione da rimuovere è installata solo per l'utente che ha effettuato l'accesso. Se l'utente non ha effettuato l'accesso, tale applicazione diventa invisibile e non può essere rimossa da remoto.

Questo comportamento è diverso con le applicazioni pensate per essere utilizzate da più utenti sullo stesso dispositivo, in cui le applicazioni sono globalmente visibili e accessibili a tutti gli utenti del dispositivo.

In Kaspersky Security Center, l'algoritmo del registro delle applicazioni gestisce le applicazioni per singoli utenti e quelle per più utenti in modo diverso:

- Le applicazioni per più utenti vengono gestite in un elenco aggiornato in tempo reale delle applicazioni installate.

- Le applicazioni per singoli utenti vengono monitorate tramite un meccanismo di memorizzazione nella cache.

  Se un utente aveva effettuato l'accesso al momento del rilevamento dell'applicazione, Kaspersky Security Center memorizza nella cache le informazioni sulle applicazioni di tale utente. Anche se l'utente successivamente si disconnette, Kaspersky Security Center continua a mostrare queste applicazioni come installate in base ai dati memorizzati nella cache, sebbene non siano più visibili o accessibili sul dispositivo.

Questa discrepanza può causare situazioni in cui Kaspersky Security Center identifica un'applicazione come installata in base ai dati memorizzati nella cache, ma l'attività di rimozione delle applicazioni non riesce perché l'applicazione non è accessibile quando l'utente è disconnesso.

Per impostazione predefinita, la durata dei dati delle applicazioni memorizzati nella cache è impostata su 30 giorni. Gli amministratori possono modificare questa impostazione per ridurre la durata della cache, riducendo al minimo le discrepanze tra i dati visualizzati e l'effettiva visibilità dell'applicazione sui dispositivi.

Per impostare la durata della cache su 1 ora (3600 secondi), eseguire il seguente comando sull'Administration Server:

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

Dopo aver eseguito questo comando, riavviare l'Administration Server affinché le modifiche abbiano effetto.

Fonte di informazioni sulle applicazioni installate

Network Agent recupera informazioni sul software installato sui dispositivi Windows dalle seguenti chiavi di registro:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contiene informazioni sulle applicazioni installate per tutti gli utenti.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Contiene informazioni sulle applicazioni installate per tutti gli utenti.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contiene informazioni sulle applicazioni installate per l'utente corrente.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contiene informazioni sulle applicazioni installate per utenti specifici.

Rimozione remota di un'applicazione dai dispositivi client del gruppo di amministrazione

Per rimuovere in remoto un'applicazione dai dispositivi client del gruppo di amministrazione:

1. Stabilire una connessione all'Administration Server che controlla i gruppi di amministrazione desiderati.
2. Selezionare un gruppo di amministrazione nella struttura della console.
3. Nell'area di lavoro del gruppo selezionare la scheda **Attività**.
4. Eseguire la creazione dell'attività facendo clic sul pulsante **Nuova attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

   Nella finestra **Selezionare il tipo di attività** della Creazione guidata nuova attività, nel nodo **Kaspersky Security Center Administration Server**, nella cartella **Avanzate** selezionare **Disinstalla l'applicazione in remoto** come tipo di attività.

   Verrà creata un'attività di gruppo per la rimozione remota dell'applicazione selezionata. La nuova attività verrà visualizzata nell'area di lavoro del gruppo di amministrazione, nella scheda **Attività**.
5. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di rimozione remota, l'applicazione selezionata verrà rimossa dai dispositivi client nel gruppo di amministrazione.

Rimozione remota di un'applicazione dai dispositivi selezionati

Per rimuovere in remoto un'applicazione dai dispositivi selezionati:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Eseguire la creazione dell'attività facendo clic su **Nuova attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

   Nella finestra **Selezionare il tipo di attività** della Creazione guidata nuova attività, nel nodo **Kaspersky Security Center Administration Server**, nella cartella **Avanzate** selezionare **Disinstalla l'applicazione in remoto** come tipo di attività.

   Verrà creata un'attività per la rimozione remota dell'applicazione selezionata da dispositivi specifici. La nuova attività creata viene visualizzata nell'area di lavoro della cartella **Attività**.
3. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di rimozione remota, l'applicazione selezionata verrà rimossa dai dispositivi selezionati.

Utilizzo dei pacchetti di installazione

Nel corso della creazione delle attività di installazione remota, il sistema utilizza pacchetti di installazione che contengono set di parametri necessari per l'installazione del software.

I pacchetti di installazione possono contenere un file chiave. È consigliabile evitare di condividere l'accesso ai pacchetti di installazione che contengono un file chiave.

È possibile utilizzare più volte lo stesso pacchetto di installazione.

I pacchetti di installazione creati da Administration Server vengono spostati nella struttura della console e inseriti nella cartella **Installazione remota**, nella sottocartella **Pacchetti di installazione**. I pacchetti di installazione sono memorizzati in Administration Server, nella sottocartella Pacchetti della cartella condivisa specificata.

Se necessario, è possibile eliminare un pacchetto di installazione dalla sottocartella **Pacchetti di installazione** seguendo le istruzioni nell'articolo Eliminazione di un oggetto.

Non modificare manualmente il contenuto dei pacchetti di installazione in una cartella condivisa. Se necessario, è possibile creare una copia di un pacchetto di installazione, apportare le modifiche necessarie e creare nuove attività di installazione.

Creazione di un pacchetto di installazione

Questo articolo descrive la procedura di creazione dei seguenti tipi di pacchetti di installazione:

- Pacchetto di installazione per un'applicazione Kaspersky
- Pacchetto di installazione per un file eseguibile specificato
- Pacchetto di installazione per un'applicazione dal database Kaspersky

Non è necessario creare manualmente un pacchetto di installazione per l'installazione remota di Network Agent. Viene creato automaticamente durante l'installazione di Kaspersky Security Center ed è memorizzato nella cartella **Pacchetti di installazione**. Se il pacchetto per l'installazione remota di Network Agent è stato eliminato, è possibile crearlo nuovamente selezionando il file nagent.kud nella cartella NetAgent del pacchetto di distribuzione di Kaspersky Security Center.

Per creare un pacchetto di installazione:

1. Eseguire la connessione all'Administration Server desiderato.
2. Nella struttura della console ,selezionare **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.
3. Avviare la creazione di un nuovo pacchetto di installazione in uno dei seguenti modi:
   - Fare clic con il pulsante destro del mouse sulla cartella **Pacchetti di installazione**, quindi selezionare **Nuovo** → **Pacchetto di installazione** nel menu di scelta rapida.
   - Fare clic con il pulsante destro del mouse nell'area vuota dell'elenco dei pacchetti di installazione, quindi selezionare **Crea** → **Pacchetto di installazione** nel menu di scelta rapida.
   - Fare clic su **Crea pacchetto di installazione** nella sezione di gestione dell'elenco dei pacchetti di installazione.

   Viene avviata la Creazione guidata nuovo pacchetto.
4. Selezionare uno dei seguenti tipi di pacchetto di installazione facendo clic sull'icona corrispondente:
   - Pacchetto di installazione per un'applicazione Kaspersky.
   - Pacchetto di installazione per un file eseguibile specificato.
   - Pacchetto di installazione per un'applicazione dal database Kaspersky.
5. Specificare il nome del pacchetto di installazione da creare.

   È possibile specificare qualsiasi nome.

6. Selezionare l'applicazione o il file eseguibile per cui creare il pacchetto di installazione in uno dei seguenti modi:

   - Fare clic sul pulsante **Sfoglia** e, nella finestra standard **Apri** di Windows, selezionare il pacchetto di distribuzione dell'applicazione richiesta situato nei dischi disponibili.

     Questa opzione è applicabile se si sceglie di creare un pacchetto di installazione per un'applicazione Kaspersky o per un file eseguibile specificato.

   - Fare clic sul pulsante **Sfoglia** e, nella finestra **Seleziona applicazione**, selezionare il pacchetto di distribuzione dell'applicazione richiesta.

     Questa opzione è applicabile se si sceglie di creare un pacchetto di installazione per un'applicazione dal database Kaspersky.

   Se si crea un pacchetto di installazione per Administration Server, selezionare il file sc.kud. Il file sc.kud si trova nella cartella radice del pacchetto di distribuzione di Kaspersky Security Center.

   Non specificare dettagli degli account privilegiati nei parametri dei pacchetti di installazione.

7. Rivedere il Contratto di licenza con l'utente finale e l'Informativa sulla privacy.

   Quando si crea un pacchetto di installazione per un'applicazione, potrebbe essere richiesto di visualizzare e accettare un Contratto di licenza con l'utente finale e l'Informativa sulla privacy per l'applicazione.

   Leggere entrambi i documenti. Se si concorda con tutti i termini del Contratto di licenza e dell'Informativa sulla privacy, accettarli selezionando le caselle di controllo corrispondenti.

   L'installazione dell'applicazione nel dispositivo prosegue e la creazione del pacchetto di installazione viene ripresa.

   Quando si crea un pacchetto di installazione per Kaspersky Endpoint Security for Mac, è possibile scegliere la lingua del Contratto di licenza e dell'Informativa sulla privacy.

8. Se necessario, abilitare l'installazione automatica dei componenti di sistema.

   Se si crea un pacchetto di installazione per un'applicazione dal database Kaspersky, è possibile abilitare l'installazione automatica dei componenti di sistema necessari. La Creazione guidata nuovo pacchetto contiene un elenco di tutti i componenti di sistema disponibili per l'applicazione selezionata. Questo elenco è disponibile in qualsiasi momento nelle proprietà del pacchetto di installazione.

   Se si crea un pacchetto di installazione delle patch, l'elenco include tutti i componenti di sistema necessari per la distribuzione della patch.

9. Fare clic sul pulsante **Fine** per completare il processo di creazione del pacchetto.

Al termine della Creazione guidata nuovo pacchetto, il nuovo pacchetto di installazione verrà visualizzato nell'area di lavoro della cartella **Pacchetti di installazione** nella struttura della console.

Creazione di pacchetti di installazione indipendenti

Gli utenti dei dispositivi nell'organizzazione possono utilizzare pacchetti di installazione indipendenti per installare manualmente le applicazioni nei dispositivi.

Un pacchetto di installazione indipendente è un file eseguibile (installer.exe) che può essere archiviato nel server Web o in una cartella condivisa oppure trasferito a un dispositivo client utilizzando un altro metodo. È inoltre possibile inviare un collegamento al pacchetto di installazione indipendente tramite e-mail. Nel dispositivo client l'utente può eseguire il file ricevuto in locale per installare un'applicazione senza coinvolgere Kaspersky Security Center.

Assicurarsi che il pacchetto di installazione indipendente non sia disponibile per persone non autorizzate.

È possibile creare pacchetti di installazione indipendenti per le applicazioni Kaspersky e per applicazioni di terze parti per piattaforme Windows, macOS e Linux. Per creare un pacchetto di installazione indipendente per un'applicazione di terze parti, è innanzitutto necessario creare un pacchetto di installazione personalizzato.

L'origine per la creazione di pacchetti di installazione indipendenti sono i pacchetti di installazione nell'elenco dei pacchetti creati in Administration Server.

Per creare un pacchetto di installazione indipendente:

1. Nella struttura della console selezionare **Administration Server → Avanzate → Installazione remota → Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Nell'elenco dei pacchetti di installazione selezionare un pacchetto di installazione per il quale si desidera creare un pacchetto indipendente.

3. Nel menu di scelta rapida selezionare **Crea pacchetto di installazione indipendente**.

   Verrà avviata la Creazione guidata pacchetto di installazione indipendente. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Nella prima pagina della procedura guidata, se è stato selezionato un pacchetto di installazione per l'applicazione Kaspersky e si desidera installare Network Agent insieme all'applicazione selezionata, assicurarsi che l'opzione **Installa Network Agent con questa applicazione** sia abilitata.

   Per impostazione predefinita, questa opzione è abilitata. È consigliabile abilitare questa opzione se non si è sicuri che Network Agent sia installato nel dispositivo. Se Network Agent è già installato nel dispositivo, dopo l'installazione del pacchetto di installazione indipendente con Network Agent, Network Agent verrà aggiornato alla versione più recente.

   Se si disabilita questa opzione, Network Agent non verrà installato nel dispositivo e il dispositivo non sarà gestito.

   Se un pacchetto di installazione indipendente per l'applicazione selezionata esiste già in Administration Server, la procedura guidata informa l'utente. In questo caso, è necessario selezionare una delle seguenti azioni:

   - **Crea pacchetto di installazione indipendente**. Selezionare questa opzione se, ad esempio, si desidera creare un pacchetto di installazione indipendente per una nuova versione dell'applicazione e si desidera mantenere anche un pacchetto di installazione indipendente creato per una versione precedente dell'applicazione. Il nuovo pacchetto di installazione indipendente viene inserito in un'altra cartella.

   - **Usa pacchetto di installazione indipendente esistente**. Selezionare questa opzione se si desidera utilizzare un pacchetto di installazione indipendente esistente. Il processo di creazione del pacchetto non verrà avviato.

   - **Ricrea pacchetto di installazione indipendente esistente**. Selezionare questa opzione se si desidera creare nuovamente un pacchetto di installazione indipendente per la stessa applicazione. Il pacchetto di installazione indipendente viene inserito nella stessa cartella.

5. Nella pagina successiva della procedura guidata selezionare l'opzione **Sposta i dispositivi non assegnati in questo gruppo** e specificare un gruppo di amministrazione in cui si desidera spostare il dispositivo client dopo l'installazione di Network Agent.

   Per impostazione predefinita, il dispositivo viene spostato nel gruppo **Dispositivi gestiti**.

   Se non si desidera spostare il dispositivo client in un gruppo di amministrazione dopo l'installazione di Network Agent, selezionare l'opzione **Non spostare i dispositivi**.

6. Nella pagina successiva della procedura guidata, al termine del processo di creazione del pacchetto di installazione indipendente, vengono visualizzati il risultato della creazione del pacchetto indipendente e il percorso del pacchetto indipendente.

   È possibile fare clic sui collegamenti ed effettuare una delle seguenti operazioni:

   - Aprire la cartella con il pacchetto di installazione indipendente.
   - Inviare tramite e-mail il collegamento al pacchetto di installazione indipendente creato. Per eseguire questa azione, è necessario che sia avviata un'applicazione di posta elettronica.
   - Codice HTML di esempio per la pubblicazione del collegamento su un sito Web. Viene creato e aperto un file TXT in un'applicazione associata a un formato TXT. Nel file viene visualizzato il tag HTML <a> con attributi.

7. Nella pagina successiva della procedura guidata, se si desidera aprire l'elenco dei pacchetti di installazione indipendenti, abilitare l'opzione **Apri l'elenco dei pacchetti indipendenti**.

8. Fare clic sul pulsante **FINE**.

   La Creazione guidata pacchetto di installazione indipendente si chiude.

Il pacchetto di installazione indipendente viene creato e inserito nella sottocartella PkgInst della cartella condivisa di Administration Server. È possibile visualizzare l'elenco dei pacchetti indipendenti facendo clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti** sopra l'elenco dei pacchetti di installazione.

Creazione di pacchetti di installazione personalizzati

È possibile utilizzare pacchetti di installazione personalizzati per effettuare le seguenti operazioni:

- Installare qualsiasi applicazione (ad esempio, un editor di testo) in un dispositivo client, ad esempio mediante un'attività.
- Creare un pacchetto di installazione indipendente.

Un pacchetto di installazione personalizzato è una cartella con un set di file. L'origine per creare un pacchetto di installazione personalizzato è un *file di archivio*. Il file di archivio contiene uno o più file che devono essere inclusi nel pacchetto di installazione personalizzato. Con la creazione di un pacchetto di installazione personalizzato, è possibile specificare i parametri della riga di comando, ad esempio per installare l'applicazione in modalità automatica.

Per creare un pacchetto di installazione personalizzato:

1. Nella struttura della console selezionare **Administration Server → Avanzate → Installazione remota → Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Sopra l'elenco dei pacchetti di installazione, fare clic sul pulsante **Crea pacchetto di installazione**.

   Viene avviata la Creazione guidata nuovo pacchetto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nella prima pagina della procedura guidata selezionare **Creare un pacchetto di installazione per il file eseguibile specificato**.

4. Nella pagina successiva della procedura guidata, specificare il nome del pacchetto di installazione personalizzato.

5. Nella pagina successiva della procedura guidata, fare clic sul pulsante **Sfoglia** e, in una finestra **Apri** standard di Windows, scegliere un file di archivio posizionato nei dischi disponibili per creare un pacchetto di installazione personalizzato.

   È possibile caricare un archivio ZIP, CAB, TAR o TAR.GZ. Non è possibile creare un pacchetto di installazione da un file SFX (archivio autoestraente).

   I file vengono scaricati in Kaspersky Security Center Administration Server.

6. Nella pagina successiva della procedura guidata, specificare i parametri della riga di comando di un file eseguibile.

   È possibile specificare i parametri della riga di comando per installare l'applicazione dal pacchetto di installazione in modalità automatica. Specificare i parametri della riga di comando è un'operazione facoltativa.

   Se lo si desidera, è possibile configurare le seguenti opzioni:

   - **Copia intera cartella nel pacchetto di installazione**

     Selezionare questa opzione se il file eseguibile è corredato da file aggiuntivi richiesti per l'installazione dell'applicazione. Prima di abilitare questa opzione, assicurarsi che tutti i file richiesti siano archiviati nella stessa cartella. Se questa opzione è abilitata, l'applicazione aggiunge tutti i contenuti nella cartella, incluso il file eseguibile specificato, nel pacchetto di installazione.

   - **Convertire le impostazioni nei valori consigliati per le applicazioni riconosciute da Kaspersky Security Center**

     L'applicazione verrà installata con le impostazioni consigliate se le informazioni sull'applicazione specificata sono contenute nel database Kaspersky.

     Se nel campo **Riga di comando file eseguibile** sono stati immessi parametri, questi vengono riscritti con le impostazioni consigliate.

     Per impostazione predefinita, questa opzione è abilitata.

     Il database Kaspersky viene creato e gestito dagli analisti di Kaspersky. Per ogni applicazione aggiunta al database, gli analisti Kaspersky definiscono le impostazioni di installazione ottimali. Le impostazioni vengono definite in modo da garantire la corretta installazione remota di un'applicazione in un dispositivo client. Il database viene automaticamente aggiornato in Administration Server quando viene eseguita l'attività Scarica aggiornamenti nell'archivio dell'Administration Server.

   Viene avviata la procedura per creare il pacchetto di installazione personalizzato.

   La procedura guidata informa l'utente al termine della procedura.

   Se il pacchetto di installazione personalizzato non viene creato, viene visualizzato un messaggio appropriato.

7. Fare clic sul pulsante **Fine** per chiudere la procedura guidata.

Il pacchetto di installazione creato viene scaricato nella sottocartella Pacchetti della cartella condivisa di Administration Server. Dopo il download, il pacchetto di installazione personalizzato viene visualizzato nell'elenco dei pacchetti di installazione.

Nell'elenco dei pacchetti di installazione in Administration Server è possibile visualizzare e modificare le proprietà del pacchetto di installazione personalizzato.

Visualizzazione e modifica delle proprietà dei pacchetti di installazione personalizzati

Dopo la creazione di un pacchetto di installazione personalizzato, è possibile visualizzare le informazioni generali del pacchetto di installazione e specificare le impostazioni di installazione nella finestra delle proprietà.

Per visualizzare e modificare le proprietà di un pacchetto di installazione personalizzato:

1. Nella struttura della console selezionare **Administration Server** → **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Nel menu di scelta rapida di un pacchetto di installazione selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del pacchetto di installazione selezionato.

3. Visualizzare le seguenti informazioni:

   - Nome pacchetto di installazione
   - Nome dell'applicazione inclusa nel pacchetto di installazione personalizzato
   - Versione applicazione
   - Data di creazione del pacchetto di installazione
   - Percorso del pacchetto di installazione personalizzato in Administration Server
   - Riga di comando file eseguibile

4. Specificare le seguenti impostazioni:

   - Nome pacchetto di installazione
   - **Installa i componenti generali del sistema richiesti**

     Se questa opzione è abilitata, prima di installare un aggiornamento l'applicazione installa automaticamente tutti i componenti di sistema generali (prerequisiti) richiesti per installare l'aggiornamento. Questi prerequisiti possono ad esempio essere aggiornamenti del sistema operativo.

     Se questa opzione è disabilitata, può essere necessario installare manualmente i prerequisiti.

     Per impostazione predefinita, questa opzione è disabilitata.

     Questa opzione è disponibile solo quando l'applicazione aggiunta al pacchetto di installazione è riconosciuta da Kaspersky Security Center.

   - **Riga di comando file eseguibile**

     Se l'applicazione richiede parametri aggiuntivi per l'installazione automatica, specificarli in questo campo. Fare riferimento alla documentazione del fornitore per ulteriori dettagli.

     È possibile immettere anche altri parametri.

     Questa opzione è disponibile solo per i pacchetti che non sono creati sulla base delle applicazioni Kaspersky.

5. Fare clic sul pulsante **OK** o **Applica** per salvare le eventuali modifiche.

Le nuove impostazioni vengono salvate.

Come ottenere il pacchetto di installazione di Network Agent dal kit di distribuzione di Kaspersky Security Center

È possibile ottenere il pacchetto di installazione di Network Agent dal kit di distribuzione di Kaspersky Security Center, senza dover installare Kaspersky Security Center. È quindi possibile utilizzare il pacchetto di installazione per installare Network Agent nei dispositivi client.

Per ottenere il pacchetto di installazione di Network Agent dal kit di distribuzione di Kaspersky Security Center:

1. Eseguire il file eseguibile ksc_<numero versione>.<numero build>_full_<lingua di localizzazione>.exe dal kit di distribuzione di Kaspersky Security Center.
2. Nella finestra visualizzata, fare clic sul collegamento **Estrai pacchetti di installazione**.
3. Nell'elenco dei pacchetti di installazione selezionare la casella di controllo accanto al pacchetto di installazione di Network Agent, quindi fare clic sul pulsante **Avanti**.
4. Se necessario, fare clic sul pulsante **Sfoglia** per modificare la cartella visualizzata in cui estrarre il pacchetto di installazione.
5. Fare clic sul pulsante **Estrai**.

   L'applicazione estrae il pacchetto di installazione di Network Agent.
6. Al termine del processo, fare clic sul pulsante **Chiudi**.

Il pacchetto di installazione di Network Agent viene estratto nella cartella selezionata.

È possibile utilizzare il pacchetto di installazione per installare Network Agent con uno dei seguenti metodi.

- In locale eseguendo il file setup.exe dalla cartella estratta
- Tramite installazione automatica
- Utilizzando i criteri di gruppo di Microsoft Windows

Distribuzione dei pacchetti di installazione agli Administration Server secondari

Per distribuire i pacchetti di installazione agli Administration Server secondari:

1. Stabilire una connessione all'Administration Server che controlla gli Administration Server secondari desiderati.
2. Creare un'attività di distribuzione del pacchetto di installazione negli Administration Server secondari in uno dei seguenti modi:
   - Se si desidera creare un'attività per gli Administration Server secondari del gruppo di amministrazione selezionato, avviare la creazione di un'attività di gruppo.
   - Se si desidera creare un'attività per specifici Administration Server secondari, avviare la creazione di un'attività per dispositivi specifici.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

   Nella finestra **Selezionare il tipo di attività** della Creazione guidata nuova attività, nel nodo **Kaspersky Security Center Administration Server**, nella cartella **Avanzate** selezionare **Distribuisci pacchetto di installazione** come tipo di attività.

   Verrà creata l'attività per la distribuzione dei pacchetti di installazione selezionati a specifici Administration Server secondari.
3. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

I pacchetti di installazione selezionati verranno copiati negli specifici Administration Server secondari.

Distribuzione dei pacchetti di installazione tramite punti di distribuzione

È possibile utilizzare i punti di distribuzione per distribuire i pacchetti di installazione in un gruppo di amministrazione.

Dopo aver ricevuto i pacchetti di installazione dall'Administration Server, i punti di distribuzione li distribuiscono automaticamente ai dispositivi client utilizzando la modalità IP multicast. La modalità IP multicast dei nuovi pacchetti di installazione all'interno di un gruppo di amministrazione si verifica una sola volta. Se un dispositivo client è disconnesso dalla rete aziendale al momento della distribuzione, Network Agent (installato nel dispositivo client) scarica automaticamente il pacchetto di installazione appropriato da un punto di distribuzione all'avvio dell'attività di installazione.

Trasferimento dei risultati sull'installazione delle applicazioni a Kaspersky Security Center

Dopo aver creato il pacchetto di installazione dell'applicazione, è possibile configurarlo in modo che tutte le informazioni di diagnostica sui risultati dell'installazione dell'applicazione vengano trasferite a Kaspersky Security Center. Per i pacchetti di installazione delle applicazioni di Kaspersky, per impostazione predefinita viene configurato il trasferimento delle informazioni di diagnostica sui risultati dell'installazione dell'applicazione. Non sono necessarie configurazioni aggiuntive.

Per configurare il trasferimento delle informazioni di diagnostica sui risultati dell'installazione delle applicazioni a Kaspersky Security Center:

1. Passare alla cartella del pacchetto di installazione creato utilizzando Kaspersky Security Center per l'applicazione selezionata. La cartella è contenuta nella cartella condivisa specificata durante l'installazione di Kaspersky Security Center.

2. Aprire il file con estensione .kpd o .kud per la modifica (ad esempio, nel Blocco note di Microsoft Windows).

   Il file presenta il formato dei normali file di configurazione .ini.

3. Aggiungere le seguenti righe al file:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Questo comando configura Kaspersky Security Center in modo da attendere il completamento dell'installazione dell'applicazione per cui è stato creato il pacchetto di installazione e analizzare il codice restituito dal programma di installazione. Se è necessario disabilitare il trasferimento dei dati di diagnostica, impostare il valore Wait su 0.

4. Aggiungere la descrizione dei codici restituiti per la riuscita dell'installazione. A questo scopo, aggiungere nel file le seguenti righe:

   ```
   [SetupProcessResult_SuccessCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   Le parentesi quadre contengono elementi facoltativi.

   Sintassi delle righe:

   - `<return code>`. Qualsiasi numero corrispondente al codice restituito dal programma di installazione. Il numero dei codici restituiti può essere arbitrario.
   - `<description>`. Testo descrittivo del risultato dell'installazione. La descrizione può essere omessa.

5. Aggiungere la descrizione dei codici restituiti per la mancata riuscita dell'installazione. A questo scopo, aggiungere nel file le seguenti righe:

   ```
   [SetupProcessResult_ErrorCodes]
   <return code>=[<description>]
   <return code 1>=[<description>]
   ...
   ```

   La sintassi di queste righe è identica a quella delle righe contenenti i codici restituiti per la riuscita dell'installazione.

6. Chiudere il file .kpd o .kud salvando tutte le modifiche.

Infine, le informazioni sui risultati dell'installazione dell'applicazione definita dall'utente verranno inserite nei registri di Kaspersky Security Center e saranno visualizzate nell'elenco degli eventi, nei rapporti e nei registri delle attività.

Definizione dell'indirizzo del server proxy KSN per i pacchetti di installazione

In caso di variazione dell'indirizzo o del dominio di Administration Server, è possibile definire l'indirizzo del server proxy KSN per il pacchetto di installazione.

Per definire l'indirizzo del server proxy KSN per il pacchetto di installazione:

1. Nella struttura della console, nella cartella **Installazione remota** fare doppio clic sulla sottocartella **Pacchetti di installazione**.
2. Nel menu visualizzato selezionare **Proprietà**.
3. Nella finestra delle proprietà visualizzata selezionare la sottosezione **Generale**.
4. Nella sottosezione **Generale** della finestra delle proprietà inserire l'indirizzo del server proxy KSN.

I pacchetti di installazione utilizzeranno questo indirizzo come indirizzo predefinito.

Ricezione delle versioni aggiornate delle applicazioni

Kaspersky Security Center consente di ricevere versioni aggiornate delle applicazioni aziendali archiviate nei server Kaspersky.

Per ricevere versioni aggiornate delle applicazioni aziendali di Kaspersky:

1. Eseguire una delle seguenti operazioni:

   - Nella struttura della console selezionare il nodo con il nome dell'Administration Server richiesto, assicurarsi che la scheda **Monitoraggio** sia selezionata e nella sezione **Distribuzione** fare clic sul collegamento **Sono disponibili nuove versioni delle applicazioni Kaspersky**.

     Il collegamento **Sono disponibili nuove versioni delle applicazioni Kaspersky** diventa disponibile quando Administration Server rileva una nuova versione di un'applicazione aziendale in un server Kaspersky.

   - Nella struttura della console selezionare **Avanzate → Installazione remota → Pacchetti di installazione** e nell'area di lavoro fare clic su **Azioni aggiuntive**, quindi nell'elenco a discesa selezionare **Visualizza le versioni correnti delle applicazioni Kaspersky**.

   Viene visualizzato l'elenco delle versioni correnti delle applicazioni Kaspersky.

2. È possibile filtrare l'elenco delle applicazioni Kaspersky per semplificare la ricerca dell'applicazione richiesta.

   Nella parte superiore della finestra **Versioni correnti delle applicazioni**, fare clic sul collegamento **Filtro** per filtrare l'elenco delle applicazioni in base ai seguenti criteri:

   - **Componenti**. Utilizzare questo criterio per filtrare l'elenco delle applicazioni Kaspersky in base alle aree di protezione utilizzate nella rete.
   - **Tipo di software scaricato**. Utilizzare questo criterio per filtrare l'elenco delle applicazioni Kaspersky in base al tipo di applicazione.
   - **Prodotti software e aggiornamenti da visualizzare**. Utilizzare questo criterio per visualizzare le applicazioni Kaspersky disponibili in base alle versioni specifiche.
   - **Lingue visualizzate per software e aggiornamenti**. Utilizzare questo criterio per visualizzare le applicazioni Kaspersky con una lingua di localizzazione specifica.

   Fare clic sul pulsante **Applica** per applicare i filtri selezionati.

3. Selezionare l'applicazione desiderata dall'elenco.

4. Scaricare il pacchetto di distribuzione dell'applicazione facendo clic sul collegamento nella stringa **Indirizzo Web pacchetto di distribuzione**.

   Gli aggiornamenti delle applicazioni gestite potrebbero richiedere l'installazione di una versione minima specifica di Kaspersky Security Center. Se questa versione è successiva alla versione corrente, gli aggiornamenti vengono visualizzati ma non possono essere approvati. Inoltre, nessun pacchetto di installazione può essere creato da tali aggiornamenti finché non si esegue l'upgrade di Kaspersky Security Center. Viene richiesto di eseguire l'upgrade dell'istanza di Kaspersky Security Center alla versione minima richiesta.

Se viene visualizzato il pulsante **Scarica le applicazioni e crea i pacchetti di installazione** per l'applicazione selezionata, è possibile fare clic sul pulsante per scaricare il pacchetto di distribuzione dell'applicazione e creare automaticamente un pacchetto di installazione. Kaspersky Security Center avvierà il download del pacchetto di distribuzione dell'applicazione in Administration Server, nella cartella condivisa specificata durante l'installazione di Kaspersky Security Center. Il pacchetto di installazione creato automaticamente viene visualizzato nella cartella **Installazione remota** della struttura della console, nella sottocartella **Pacchetti di installazione**.

Dopo la chiusura della finestra **Versioni correnti delle applicazioni**, il collegamento **Sono disponibili nuove versioni delle applicazioni Kaspersky** scompare dalla sezione **Distribuzione**.

È possibile creare pacchetti di installazione per le nuove versioni delle applicazioni e gestire i nuovi pacchetti di installazione creati nella cartella **Installazione remota** della struttura della console, nella sottocartella **Pacchetti di installazione**.

È anche possibile aprire la finestra **Versioni correnti delle applicazioni** facendo clic sul collegamento **Visualizza le versioni correnti delle applicazioni Kaspersky** nell'area di lavoro della cartella **Pacchetti di installazione**.

Preparazione di un dispositivo Windows per l'installazione remota

L'installazione remota dell'applicazione in un dispositivo client può restituire un errore per i seguenti motivi:

- L'attività è già stata eseguita nel dispositivo.

  In questo caso, non è necessario eseguire nuovamente l'attività.

- All'avvio di un'attività, il dispositivo era spento.

  In questo caso, accendere il dispositivo e avviare nuovamente l'attività.

- Non è stata stabilita la connessione tra l'Administration Server e il Network Agent installato nel dispositivo client.

  Per determinare la causa del problema, utilizzare l'utilità per la diagnostica remota dei dispositivi client (klactgui).

- Se nel dispositivo non è installato alcun Network Agent, durante l'installazione remota possono verificarsi i seguenti problemi:

  - Il dispositivo client ha l'opzione **Disattiva il Simple File Sharing** abilitata.
  - Il servizio Server non è in esecuzione nel dispositivo client.
  - Le porte richieste sono chiuse nel dispositivo client.
  - L'account utilizzato per l'esecuzione dell'attività dispone di privilegi insufficienti.

  Per evitare problemi che possono verificarsi durante l'installazione dell'applicazione in un dispositivo client senza Network Agent installato, è necessario procedere come descritto nella distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center.

In precedenza, veniva utilizzata l'utilità riprep per preparare un dispositivo per l'installazione remota. Questo è ormai considerato un metodo obsoleto per la configurazione dei sistemi operativi. L'utilizzo dell'utilità riprep non è consigliabile nei sistemi operativi più recenti di Windows XP e Windows Server 2003 R2.

Preparazione di un dispositivo Linux e installazione di Network Agent in un dispositivo Linux da remoto

L'installazione di Network Agent comprende due passaggi:

- Una preparazione per il dispositivo Linux
- Installazione remota di Network Agent

Una preparazione per il dispositivo Linux

Per preparare un dispositivo Linux per l'installazione remota di Network Agent:

1. Verificare che il dispositivo in cui si desidera installare Network Agent for Linux esegua una delle distribuzioni Linux supportate.
2. Scaricare il pacchetto di installazione di Network Agent utilizzando l'interfaccia dell'applicazione o dal sito Web di Kaspersky.
3. Accertarsi che il seguente software sia installato nel dispositivo Linux di destinazione.
   - Sudo (per Ubuntu 10.04, la versione di Sudo è 1.7.2p1 o successiva)
   - Interprete del linguaggio Perl versione 5.10 o successiva
   - ps utility

4. Testare la configurazione del dispositivo:

   a. Verificare se è possibile connettersi al dispositivo tramite un client SSH (ad esempio, PuTTY).

      Se non è possibile connettersi al dispositivo, aprire il file `/etc/ssh/sshd_config` e verificare che per le seguenti impostazioni siano specificati i valori elencati:

      ```
      PasswordAuthentication no
      ```

      ```
      ChallengeResponseAuthentication yes
      ```

      > Non modificare il file /etc/ssh/sshd_config se è possibile connettersi al dispositivo senza problemi; in caso contrario, è possibile che si verifichi un errore di autenticazione SSH durante l'esecuzione di un'attività di installazione remota.

      Salvare il file (se necessario) e riavviare il servizio SSH utilizzando il comando `sudo service ssh restart`.

   b. Disabilitare la password sudo per l'account utente con cui deve essere eseguita la connessione del dispositivo.

   c. Utilizzare il comando `visudo` in sudo per aprire il file di configurazione sudoers.

      Nel file aperto, aggiungere la seguente riga alla fine del file: `<nome utente> > ALL = (ALL) NOPASSWD: ALL`. In questo caso, `< username >` è l'account utente che deve essere utilizzato per la connessione del dispositivo tramite SSH. Se si utilizza il sistema operativo Astra Linux, nel file /etc/sudoers aggiungere l'ultima riga con il seguente testo: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Salvare e chiudere il file sudoers.

   e. Eseguire di nuovo la connessione al dispositivo tramite SSH e verificare che il servizio Sudo non richieda l'immissione di una password. A tale scopo, utilizzare il comando `sudo whoami`.

5. Aprire il file `/etc/systemd/logind.conf`, quindi eseguire una delle seguenti operazioni:

   - Specificare "no" come valore per l'impostazione: `KillUserProcesses=no`.
   - Per l'impostazione KillExcludeUsers, digitare il nome utente dell'account con il quale deve essere eseguita l'installazione remota, ad esempio, `KillExcludeUsers=root`.

   Se nel dispositivo di destinazione viene eseguito Astra Linux, aggiungere la stringa `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` nel file `/home/< nome utente >/.bashrc`, dove `< nome utente >` è l'account utente da utilizzare per la connessione del dispositivo tramite SSH.

   Per applicare l'impostazione modificata, riavviare il dispositivo Linux o eseguire il seguente comando:

   ```
   sudo systemctl restart systemd-logind.service
   ```

6. Se si desidera installare Network Agent nei dispositivi con sistema operativo SUSE Linux Enterprise Server 15, installare il pacchetto insserv-compat prima di configurare Network Agent.

7. Se si desidera installare Network Agent nei dispositivi con il sistema operativo Astra Linux in esecuzione in modalità ambiente software chiuso, eseguire passaggi aggiuntivi per preparare i dispositivi Astra Linux.

8. Se si desidera installare Network Agent nei dispositivi con il sistema operativo RED OS 7.3.4 o versione successiva o MSVSPHERE 9.2 o versione successiva, installare il pacchetto libxcrypt-compat per il corretto funzionamento di Network Agent.

Installazione remota di Network Agent

Per installare Network Agent nei dispositivi Linux da remoto:

1. Scaricare e creare un pacchetto di installazione:

   a. Prima di installare il pacchetto nel dispositivo, verificare di avere già installato tutte le dipendenze (programmi e librerie) per questo pacchetto.

   È possibile visualizzare le dipendenze per ciascun pacchetto autonomamente, utilizzando le utilità specifiche per la distribuzione Linux in cui deve essere installato il pacchetto. Per informazioni dettagliate sulle utilità, fare riferimento alla documentazione del sistema operativo.

   b. Per creare un pacchetto di installazione remota, utilizzare i seguenti file:

   - klnagent.kpd
   - akinstall.sh
   - Pacchetto .deb o .rpm di Network Agent

2. Crea un'attività di installazione remota con le seguenti impostazioni:

   - Nella pagina **Impostazioni** della Creazione guidata nuova attività, selezionare la casella di controllo **Utilizzo delle risorse del sistema operativo tramite Administration Server**. Deselezionare tutte le altre caselle di controllo.
   - Nella pagina **Selezione di un account per l'esecuzione dell'attività**, specificare le impostazioni dell'account utente utilizzato per la connessione del dispositivo tramite SSH.

3. Eseguire l'attività di installazione remota. Utilizzare l'opzione per il comando `su` per preservare l'ambiente: `-m, -p, --preserve-environment`.

Preparazione di un dispositivo che esegue SUSE Linux Enterprise Server 15 per l'installazione di Network Agent

Per installare Network Agent in un dispositivo con il sistema operativo SUSE Linux Enterprise Server 15,

Prima dell'installazione di Network Agent, eseguire il seguente comando:

```
sudo zypper install insserv-compat
```

Questo consente di installare il pacchetto insserv-compat e di configurare correttamente Network Agent.

> Eseguire il comando `rpm -q insserv-compat` per verificare se il pacchetto è già installato.

Se la rete include molti dispositivi che eseguono SUSE Linux Enterprise Server 15, è possibile utilizzare il software apposito per la configurazione e la gestione dell'infrastruttura aziendale. Utilizzando questo software, è possibile installare automaticamente il pacchetto insserv-compat in tutti i dispositivi necessari contemporaneamente. È ad esempio possibile utilizzare Puppet, Ansible, Chef o è possibile creare il proprio script, usando il metodo più conveniente.

Se il dispositivo non dispone delle chiavi di firma GPG per SUSE Linux Enterprise, è possibile che venga visualizzato il seguente avviso: `Package header is not signed!` Selezionare l'opzione `i` per ignorare l'avviso.

Oltre all'installazione del pacchetto insserv-compat, assicurarsi di aver preparato in modo esaustivo i dispositivi Linux. Successivamente, distribuire e installare Network Agent.

Preparazione di un dispositivo macOS per l'installazione remota di Network Agent

Per preparare un dispositivo macOS per l'installazione remota di Network Agent:

1. Accertarsi che Sudo sia installato nel dispositivo macOS di destinazione.

2. Testare la configurazione del dispositivo:

   a. Assicurarsi che la porta 22 sia aperta sul dispositivo client. A tale scopo, in **Preferenze di sistema**, aprire il riquadro **Condivisione**, quindi verificare che la casella di controllo **Accesso remoto** sia selezionata.

   È possibile connettersi al dispositivo client tramite Secure Shell (SSH) solo attraverso la porta 22. Non è possibile modificare il numero di porta.

   È possibile utilizzare il comando `ssh <nome_dispositivo>` per accedere in remoto al dispositivo macOS. Nel riquadro **Condivisione** è possibile utilizzare l'opzione **Consenti accesso per** impostare l'ambito degli utenti a cui è consentito l'accesso al dispositivo macOS.

   b. Disabilitare la password sudo per l'account utente con cui deve essere eseguita la connessione del dispositivo.

   Utilizzare il comando `sudo visudo` in Terminale per aprire il file di configurazione sudoers. Nella voce `Specifica privilegi utente` del file aperto specificare quanto segue: `username ALL = (ALL) NOPASSWD: ALL`. In questo caso, `username` è l'account utente che deve essere utilizzato per la connessione del dispositivo tramite SSH.

   c. Salvare e chiudere il file sudoers.

   d. Eseguire di nuovo la connessione al dispositivo tramite SSH e verificare che il servizio Sudo non richieda l'immissione di una password. A tale scopo, utilizzare il comando `sudo whoami`.

3. Scaricare e creare un pacchetto di installazione:

   a. Scaricare il pacchetto di installazione di Network Agent utilizzando uno dei seguenti metodi:

      - Nella struttura della console, aprendo il menu di scelta rapida in **Installazione remota** → **Pacchetti di installazione** e selezionando **Mostra versioni correnti delle applicazioni** per scegliere tra i pacchetti disponibili
      - Scaricando la versione adeguata di Network Agent dal sito Web del Servizio di assistenza tecnica all'indirizzo https://support.kaspersky.com/
      - Richiedendo il pacchetto di installazione agli specialisti del Servizio di assistenza tecnica

   b. Per creare un pacchetto di installazione remota, utilizzare i seguenti file:

      - klnagent.kud
      - install.sh
      - klnagentmac.dmg

4. Crea un'attività di installazione remota con le seguenti impostazioni:

   - Nella pagina **Impostazioni** della Creazione guidata nuova attività, selezionare la casella di controllo **Utilizzando le risorse del sistema operativo tramite Administration Server**. Deselezionare tutte le altre caselle di controllo.
   - Nella pagina **Selezione di un account per l'esecuzione dell'attività** specificare le impostazioni dell'account utente utilizzato per la connessione del dispositivo tramite SSH.

Il dispositivo client è pronto per l'installazione remota di Network Agent tramite l'attività corrispondente che è stata creata.

Applicazioni Kaspersky: licensing e attivazione

In questa sezione vengono descritte le funzionalità di Kaspersky Security Center relative all'utilizzo delle chiavi di licenza delle applicazioni Kaspersky gestite.

Kaspersky Security Center consente la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi client, il monitoraggio del relativo utilizzo e il rinnovo delle licenze.

Quando si aggiunge una chiave di licenza utilizzando Kaspersky Security Center, le impostazioni della chiave di licenza vengono salvate nell'Administration Server. In base a queste informazioni, l'applicazione genera un rapporto sull'utilizzo delle chiavi di licenza e segnala all'amministratore la scadenza delle licenze e la violazione delle limitazioni di licenza specificate nelle proprietà delle chiavi di licenza. È possibile configurare le notifiche dell'utilizzo delle chiavi di licenza nelle impostazioni di Administration Server.

Licensing delle applicazioni gestite

Le applicazioni Kaspersky installate nei dispositivi gestiti devono essere concesse in licenza applicando un codice di attivazione o un file chiave a ognuna delle applicazioni. È possibile distribuire un codice di attivazione o un file chiave nei seguenti modi:

- Distribuzione automatica
- Il pacchetto di installazione di un'applicazione gestita
- Attività *Aggiungi chiave di licenza* per un'applicazione gestita
- Attivazione manuale di un'applicazione gestita

È possibile aggiungere una nuova chiave di licenza attiva o di riserva con uno dei metodi sopra elencati. Un'applicazione Kaspersky utilizza una chiave attiva al momento e memorizza una chiave di riserva da applicare dopo la scadenza della chiave attiva. L'applicazione per la quale si aggiunge una chiave di licenza definisce se la chiave è attiva o aggiuntiva. La definizione della chiave non dipende dal metodo utilizzato per aggiungere una nuova chiave di licenza.

Distribuzione automatica

Se si utilizzano diverse applicazioni gestite ed è necessario distribuire un file chiave specifico o un codice di attivazione specifico nei dispositivi, valutare altre modalità di distribuzione del codice di attivazione o del file chiave in questione.

Kaspersky Security Center consente di distribuire automaticamente le chiavi di licenza disponibili nei dispositivi. Ad esempio, nell'archivio dell'Administration Server sono presenti tre chiavi di licenza. È stata selezionata la casella di controllo **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti** per tutte e tre le chiavi di licenza. Un'applicazione di protezione Kaspersky, ad esempio Kaspersky Endpoint Security for Windows, è installata nei dispositivi dell'organizzazione. Viene rilevato un nuovo dispositivo a cui deve essere distribuita una chiave di licenza. L'applicazione stabilisce, ad esempio, che due delle chiavi di licenza dell'archivio possono essere distribuite al dispositivo: la chiave di licenza denominata *Key_1*e la chiave di licenza denominata *Key_2*. Una di queste chiavi di licenza viene distribuita nel dispositivo. In questo caso non è possibile prevedere quale delle due chiavi di licenza verrà distribuita nel dispositivo poiché la distribuzione automatica delle chiavi di licenza non offre nessuna attività di amministrazione.

Quando una chiave di licenza viene distribuita, i dispositivi vengono ricalcolati per questa chiave di licenza. È necessario accertarsi che il numero di dispositivi in cui è stata distribuita la chiave di licenza non superi la limitazione licenza. Se il numero di dispositivi supera la limitazione licenza, a tutti i dispositivi non coperti dalla licenza verrà assegnato lo stato *Critico*.

Prima della distribuzione, è necessario aggiungere il codice di attivazione o il file chiave all'archivio di Administration Server.

Istruzioni dettagliate:

- Administration Console:
  - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
  - Distribuzione automatica di una chiave di licenza

  o
- Kaspersky Security Center Web Console:
  - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
  - Distribuzione automatica di una chiave di licenza

Si noti che una chiave di licenza distribuita automaticamente potrebbe non essere visualizzata nell'archivio dell'Administration Server virtuale nei seguenti casi:

- La chiave di licenza non è valida per l'applicazione.
- L'Administration Server virtuale non dispone di dispositivi gestiti.
- La chiave di licenza è già stata utilizzata per i dispositivi sotto la gestione di un altro Administration Server virtuale ed è stato raggiunto il limite del numero di dispositivi.

Aggiunta di un file chiave o di un codice di attivazione al pacchetto di installazione di un'applicazione gestita

Per motivi di sicurezza, questa opzione non è consigliata. Un codice di attivazione o un file chiave di licenza aggiunto a un pacchetto di installazione può essere compromesso.

Se si installa un'applicazione gestita utilizzando un pacchetto di installazione, è possibile specificare un codice di attivazione o un file chiave nel pacchetto di installazione o nel criterio dell'applicazione. La chiave di licenza verrà distribuita nei dispositivi gestiti alla successiva sincronizzazione del dispositivo con Administration Server.

Istruzioni dettagliate:

- Administration Console:
  - Creazione di un pacchetto di installazione
  - Installazione delle applicazioni nei dispositivi client

  o
- Kaspersky Security Center Web Console: Aggiunta di una chiave di licenza a un pacchetto di installazione

Distribuzione tramite l'attività di aggiunta della chiave di licenza per un'applicazione gestita

Se si sceglie di utilizzare l'attività *Aggiungi chiave di licenza* per un'applicazione gestita, è possibile selezionare la chiave di licenza che deve essere distribuita nei dispositivi e selezionare i dispositivi nella modalità più opportuna, ad esempio selezionando un gruppo di amministrazione o una selezione dispositivi.

Prima della distribuzione, è necessario aggiungere il codice di attivazione o il file chiave all'archivio di Administration Server.

Istruzioni dettagliate:

- Administration Console:
  - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
  - Distribuzione di una chiave di licenza ai dispositivi client

  o
- Kaspersky Security Center Web Console:
  - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
  - Distribuzione di una chiave di licenza ai dispositivi client

Aggiunta manuale di un codice di attivazione o di un file chiave ai dispositivi

È possibile attivare l'applicazione Kaspersky installata in locale utilizzando gli strumenti disponibili nell'interfaccia dell'applicazione. Fare riferimento alla documentazione dell'applicazione installata.

Visualizzazione delle informazioni sulle chiavi di licenza in uso

Per visualizzare le informazioni sulle chiavi di licenza in uso,

Nella struttura della console selezionare la cartella **Licenze di Kaspersky**.

Nell'area di lavoro della cartella verrà visualizzato un elenco delle chiavi di licenza utilizzate nei dispositivi client.

Accanto a ognuna delle chiavi di licenza è visualizzata un'icona, che corrisponde al tipo di utilizzo:

-  - Le informazioni sulla chiave di licenza attualmente in uso vengono ricevute da un dispositivo client connesso ad Administration Server. Il file di questa chiave di licenza è memorizzato all'esterno dell'Administration Server.
-  - La chiave di licenza è memorizzata nell'archivio di Administration Server. La distribuzione automatica è disabilitata per questa chiave di licenza.
-  - La chiave di licenza è memorizzata nell'archivio di Administration Server. La distribuzione automatica è abilitata per questa chiave di licenza.

È possibile visualizzare le informazioni sulle chiavi di licenza utilizzate per l'applicazione in un dispositivo client aprendo la sezione **Applicazioni** della finestra delle proprietà del dispositivo client.

Per definire le impostazioni aggiornate delle chiavi di licenza dell'Administration Server virtuale, l'Administration Server invia una richiesta ai server di attivazione di Kaspersky almeno una volta al giorno. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici.

Se si riceve una chiave di licenza da un dispositivo client, non è possibile esportarla come file.

Aggiunta di una chiave di licenza all'archivio dell'Administration Server

Per aggiungere una chiave di licenza all'archivio dell'Administration Server:

1. Nella struttura della console selezionare la cartella **Licenze di Kaspersky**.
2. Avviare l'attività di aggiunta della chiave di licenza in uno dei seguenti modi:
   - Selezionare **Aggiungi codice di attivazione o file chiave** nel menu di scelta rapida dell'elenco delle chiavi di licenza.
   - Facendo clic sul collegamento **Aggiungi codice di attivazione o file chiave** nell'area di lavoro dell'elenco delle chiavi di licenza.
   - Fare clic sul pulsante **Aggiungi codice di attivazione o file chiave**.

   Verrà visualizzata l'Aggiunta guidata chiave di licenza.
3. Selezionare la modalità di attivazione di Administration Server: tramite codice di attivazione o file chiave.
4. Specificare il codice di attivazione o un file chiave.
5. Selezionare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti** se si desidera distribuire immediatamente una chiave di licenza attinente nella rete. Se non si seleziona questa opzione, è possibile distribuire manualmente una chiave di licenza in un secondo momento.

Di conseguenza, il file chiave viene scaricato e la procedura Aggiunta guidata chiave di licenza viene terminata. Adesso è possibile visualizzare la chiave di licenza aggiunta nell'elenco delle licenze Kaspersky.

Rimozione di una chiave di licenza di Administration Server

Per rimuovere una chiave di licenza di Administration Server:

1. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server che verrà visualizzata selezionare la sezione **Chiavi di licenza**.
3. Rimuovere la chiave di licenza facendo clic sul pulsante **Rimuovi**.

   La chiave di licenza verrà rimossa.

Se è stata aggiunta una chiave di licenza di riserva, questa diventa automaticamente la chiave di licenza attiva quando viene rimossa la precedente chiave di licenza attiva.

Dopo che la chiave di licenza attiva di Administration Server è stata rimossa, Vulnerability e patch management e Mobile Device Management non saranno più disponibili. È possibile aggiungere nuovamente una chiave di licenza rimossa o aggiungerne una nuova.

Distribuzione di una chiave di licenza ai dispositivi client

Kaspersky Security Center consente la distribuzione della chiave di licenza ai dispositivi client tramite l'attività di *distribuzione della chiave di licenza*.

Prima della distribuzione, aggiungere una chiave di licenza all'archivio dell'Administration Server.

Per distribuire una chiave di licenza ai dispositivi client:

1. Nella struttura della console selezionare la cartella **Licenze di Kaspersky**.
2. Nell'area di lavoro dell'elenco delle chiavi di licenza, fare clic sul pulsante **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

   Viene avviata la **Creazione guidata attività di attivazione dell'applicazione**. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nell'elenco delle applicazioni, selezionare l'applicazione per la quale si desidera creare un'attività.

4. Nel passaggio **Aggiungi chiave** della procedura guidata, aggiungere la chiave di licenza utilizzando una delle seguenti opzioni:

   - Selezionare l'opzione **Codice di attivazione** per aggiungere un codice di attivazione dall'archivio di Kaspersky Security Center.

     Fare clic su **Seleziona**. Nella finestra visualizzata, selezionare il codice di attivazione, quindi fare clic su **OK**.

   - Selezionare l'opzione **Chiave o file chiave**, quindi effettuare le seguenti operazioni:

     a. Fare clic su **Seleziona**.

     b. Nel menu contestuale, selezionare una delle opzioni:

     - **$SelectKeyIdDropdownOption1**.

       Nella finestra visualizzata, selezionare il file chiave dal dispositivo, quindi fare clic su **Apri**.

     - **$SelectKeyIdDropdownOption2**.

       Nella finestra visualizzata, selezionare la chiave dall'archivio di Kaspersky Security Center, quindi fare clic su **OK**.

5. Se si desidera sostituire la chiave di licenza attiva, deselezionare la casella di controllo **Usa come chiave di riserva**.

   Ad esempio, questo è necessario quando l'organizzazione cambia ed è richiesta la chiave di un'altra organizzazione nel dispositivo o se la chiave è stata riemessa e una nuova licenza scade prima della licenza corrente. Per evitare errori, è necessario deselezionare la casella di controllo **Usa come chiave di riserva**.

   Per ulteriori informazioni sui problemi che possono verificarsi durante l'aggiunta di una chiave di licenza a Kaspersky Security Center Windows e sui modi per risolverli, fare riferimento alla Knowledge Base di Kaspersky Security Center.

6. Controllare le informazioni sulla chiave di licenza, quindi fare clic su **Avanti**.

7. In questo passaggio della procedura guidata, selezionare i dispositivi a cui si desidera assegnare l'attività di aggiunta della chiave. È possibile specificare i dispositivi (fino a 1000 dispositivi) in uno dei seguenti modi:

   - **Seleziona i dispositivi della rete rilevati da Administration Server**. In questo caso l'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

   - **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**. È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

   - **Assegna un'attività a una selezione dispositivi**. In questo caso l'attività viene assegnata ai dispositivi inclusi in una selezione creata precedentemente. È possibile specificare la selezione predefinita o una selezione personalizzata creata.

   - **Assegna un'attività a un gruppo di amministrazione**. In questo caso, l'attività viene assegnata ai dispositivi inclusi nel gruppo di amministrazione creato precedentemente.

8. Nel passaggio **Configurare la pianificazione delle attività** della procedura guidata, creare una pianificazione per l'avvio dell'attività:

- **Avvio pianificato**:
  - **Una sola volta**

    L'attività viene eseguita una volta, nella data e nell'ora specificate (per impostazione predefinita, il giorno in cui è stata creata l'attività).

  - **Manualmente**

    L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Quando vengono scaricati nuovi aggiornamenti nell'archivio**

    L'attività viene eseguita dopo il download degli aggiornamenti nell'archivio. È ad esempio possibile utilizzare questa pianificazione per l'attività Trova vulnerabilità e aggiornamenti richiesti.

  - **Durante un'epidemia di virus**

    L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:
    - Anti-virus per workstation e file server
    - Anti-virus per la difesa perimetrale
    - Anti-virus per i sistemi di posta

    Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

    Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

  - **Al completamento di un'altra attività**

L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

- Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
- Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

  Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
- Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

9. Nel passaggio **Definire il nome dell'attività** della procedura guidata, specificare il nome dell'attività. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

10. Nel passaggio **Completare la creazione dell'attività** della procedura guidata fare clic sul pulsante **Fine** per chiudere la procedura guidata.

    Se si desidera che l'attività venga avviata al termine della Creazione guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Le attività create tramite la **Creazione guidata attività di attivazione dell'applicazione** sono attività per dispositivi specifici memorizzate nella cartella **Attività** della struttura della console.

È inoltre possibile creare un'attività di distribuzione della chiave di licenza di gruppo o locale utilizzando la Creazione guidata attività per un gruppo di amministrazione e per un dispositivo client.

Distribuzione automatica di una chiave di licenza

Kaspersky Security Center consente la distribuzione automatica delle chiavi di licenza ai dispositivi gestiti, se sono presenti nell'archivio delle chiavi di licenza in Administration Server. La distribuzione automatica delle chiavi di licenza non si applica ai dispositivi nella cartella **Dispositivi non assegnati**.

Per distribuire automaticamente una chiave di licenza ai dispositivi gestiti:

1. Nella struttura della console selezionare la cartella **Licenze di Kaspersky**.

2. Nell'area di lavoro della cartella selezionare la chiave di licenza da distribuire automaticamente ai dispositivi.

3. Aprire la finestra delle proprietà della chiave di licenza selezionata in uno dei seguenti modi:

   - Selezionando **Proprietà** nel menu di scelta rapida della chiave di licenza.

   - Facendo clic sul collegamento **Visualizza proprietà della chiave di licenza** nella finestra di informazioni per la chiave di licenza selezionata.

4. Nella finestra delle proprietà della chiave di licenza visualizzata selezionare la casella di controllo **Chiave di licenza distribuita automaticamente**. Chiudere la finestra delle proprietà della chiave di licenza.

La chiave di licenza verrà automaticamente distribuita a tutti i dispositivi compatibili.

La distribuzione della chiave di licenza viene eseguita tramite Network Agent. Non vengono create attività di distribuzione della chiave di licenza per l'applicazione.

Durante la distribuzione automatica di una chiave di licenza, viene presa in considerazione la limitazione relativa al licensing sul numero di dispositivi. La limitazione relativa al licensing è impostata nelle proprietà della chiave di licenza. Se viene raggiunta la limitazione relativa al licensing, la distribuzione di questa chiave di licenza nei dispositivi si interrompe automaticamente.

L'Administration Server virtuale distribuisce automaticamente le chiavi di licenza dal proprio archivio e dall'archivio di Administration Server. È consigliabile:

- Utilizzare l'attività *Aggiungi chiave di licenza* per selezionare la chiave di licenza da distribuire nei dispositivi.
- Evitare di disabilitare l'opzione **Consenti la distribuzione automatica delle chiavi di licenza di questo Administration Server virtuale nei relativi dispositivi** nelle impostazioni dell'Administration Server virtuale. In caso contrario, l'Administration Server virtuale non distribuirà le chiavi di licenza ai dispositivi, comprese le chiavi di licenza dall'archivio di Administration Server.

Se si seleziona la casella di controllo **Chiave di licenza distribuita automaticamente** nella finestra delle proprietà della chiave di licenza, nella rete viene immediatamente distribuita una chiave di licenza. Se non si seleziona questa opzione, è possibile distribuire manualmente una chiave di licenza in un secondo momento.

Creazione e visualizzazione di un rapporto sull'utilizzo delle chiavi di licenza

Per creare un rapporto sull'utilizzo delle chiavi di licenza nei dispositivi client:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Selezionare il modello di rapporto denominato **Rapporto sull'utilizzo delle chiavi di licenza** o creare un nuovo modello di rapporto dello stesso tipo.

Nell'area di lavoro del rapporto sull'utilizzo delle chiavi di licenza verranno visualizzate informazioni sulle chiavi di licenza attive e di riserva utilizzate nei dispositivi client. Il rapporto contiene inoltre informazioni sui dispositivi in cui vengono utilizzate le chiavi di licenza e sulle limitazioni specificate nelle proprietà di tali chiavi di licenza.

Visualizzazione delle informazioni sulle chiavi di licenza dell'applicazione

Per sapere quali chiavi di licenza sono in uso per un'applicazione Kaspersky:

1. Nella struttura della console di Kaspersky Security Center selezionare il nodo **Dispositivi gestiti** e passare alla scheda **Dispositivi**.
2. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida del dispositivo desiderato, quindi selezionare **Proprietà**.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la sezione **Applicazioni**.

4. Nell'elenco delle applicazioni visualizzato selezionare l'applicazione di cui si desidera visualizzare le chiavi di licenza, quindi fare clic sul pulsante **Proprietà**.

5. Nella finestra delle proprietà dell'applicazione visualizzata selezionare la sezione **Chiavi di licenza**.

   Le informazioni vengono visualizzate nell'area di lavoro di questa sezione.

Esportazione di un file di chiave di licenza

Se la chiave di licenza è stata eliminata accidentalmente e si desidera ripristinarla, è possibile esportare un file della chiave di licenza da un altro Administration Server.

Per esportare un file della chiave di licenza, è necessario disporre del diritto **Esporta file chiave** nell'area funzionale **Caratteristiche generali: Key management**.

Se si riceve una chiave di licenza da un dispositivo client, non è possibile esportarla.

Per esportare una chiave di licenza:

1. Nella struttura della console selezionare la cartella **Licenze di Kaspersky**.

2. Nell'elenco, selezionare la chiave di licenza che si desidera esportare come file.

3. Nella casella delle informazioni visualizzata, fare clic sul collegamento **Esporta file chiave**.

4. Nella finestra visualizzata, specificare il percorso della cartella in cui si desidera salvare un file della chiave di licenza, quindi specificare un nome file. Successivamente, fai clic su **Salva**.

Il file della chiave di licenza in formato .key viene esportato nella cartella selezionata.

Se la chiave di licenza il cui file è stato esportato è stata aggiunta all'archivio di Administration Server come codice di attivazione e si desidera aggiungere il file della chiave di licenza esportato all'archivio di un altro Administration Server, è necessario aggiungerlo come codice di attivazione, non come file chiave. In caso contrario, si verifica un errore. È necessario aprire il file della chiave di licenza esportato in un qualsiasi editor di testo e quindi copiare il codice di attivazione.

Configurazione della protezione di rete

Questa sezione contiene informazioni sulla configurazione manuale di criteri e attività, sui ruoli utente, sulla creazione di una struttura di gruppi di amministrazione e sulla gerarchia delle attività.

Scenario: Configurazione della protezione di rete

L'avvio rapido guidato crea criteri e attività con le impostazioni predefinite. Queste impostazioni possono risultare non ottimali o addirittura non consentite dall'organizzazione. Pertanto, è consigliabile ottimizzare tali criteri e attività e creare altri criteri e attività, se necessario per la rete.

Prerequisiti

Prima di iniziare, verificare di avere:

- Installato Kaspersky Security Center Administration Server
- Installato Kaspersky Security Center Web Console (facoltativo)
- completato lo scenario di installazione principale di Kaspersky Security Center
- completato l'Avvio rapido guidato o creato manualmente i seguenti criteri e attività nel gruppo di amministrazione **Dispositivi gestiti**:
  - Criterio di Kaspersky Endpoint Security
  - Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
  - Criterio di Network Agent
  - Attività *Trova vulnerabilità e aggiornamenti richiesti*

La configurazione della protezione della rete procede per fasi:

1. **Installazione e propagazione dei criteri e dei profili criterio delle applicazioni Kaspersky**

   Per configurare e propagare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti, è possibile utilizzare due diversi metodi di gestione della protezione: quello incentrato sui dispositivi o quello incentrato sugli utenti. Questi due metodi possono anche essere combinati. Per l'implementazione della gestione della protezione incentrata sui dispositivi, è possibile utilizzare gli strumenti offerti in Administration Console basata su Microsoft Management Console o Kaspersky Security Center Web Console. La gestione della protezione incentrata sugli utenti può essere implementata solo tramite Kaspersky Security Center Web Console.

2. **Configurazione delle attività per la gestione remota delle applicazioni Kaspersky**

   Controllare le attività create con l'avvio rapido guidato e, se necessario, ottimizzarle.

   Istruzioni dettagliate:

   - Administration Console:
     - Configurazione dell'attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
     - Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
   - Kaspersky Security Center Web Console:
     - Configurazione dell'attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security

- Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

Se necessario, creare attività aggiuntive per gestire le applicazioni Kaspersky installate nei dispositivi client.

3. **Valutazione e limitazione del carico di eventi nel database**

   Le informazioni sugli eventi che si verificano durante il funzionamento delle applicazioni gestite vengono trasferite da un dispositivo client e registrate nel database di Administration Server. Per ridurre il carico su Administration Server, valutare e limitare il numero massimo di eventi che possono essere archiviati nel database.

   Istruzioni dettagliate:

   - Administration Console: Impostazione del numero massimo di eventi
   - Kaspersky Security Center Web Console: Impostazione del numero massimo di eventi

Risultati

Quando viene completato questo scenario, la rete sarà protetta tramite la configurazione delle applicazioni Kaspersky, delle attività e degli eventi ricevuti da parte di Administration Server:

- Le applicazioni Kaspersky sono configurate in base ai criteri e ai profili criterio.
- Le applicazioni vengono gestite attraverso un set di attività.
- Viene impostato il numero massimo di eventi che è possibile archiviare nel database.

Al termine della configurazione della protezione di rete, è possibile procedere alla configurazione degli aggiornamenti standard nei database e nelle applicazioni Kaspersky.

Per informazioni dettagliate su come configurare le risposte automatiche alle minacce rilevate da Kaspersky Sandbox, fare riferimento alla Guida in linea di Kaspersky Sandbox 2.0.

Configurazione e propagazione dei criteri: approccio incentrato sui dispositivi

Al termine di questo scenario, le applicazioni saranno configurate in tutti i dispositivi gestiti in base ai criteri delle applicazioni e ai profili criterio specificati.

Prerequisiti

Prima di iniziare, verificare di aver installato Kaspersky Security Center Administration Server e Kaspersky Security Center Web Console (opzionale). Se è stato installato Kaspersky Security Center Web Console, è inoltre consigliabile valutare la gestione della protezione incentrata sugli utenti come opzione alternativa o aggiuntiva rispetto all'approccio incentrato sui dispositivi.

Passaggi

Lo scenario di gestione incentrata sui dispositivi delle applicazioni Kaspersky comprende i seguenti passaggi:

1. **Configurazione dei criteri delle applicazioni**

Configurare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti tramite la creazione di un criterio per ogni applicazione. Questo set di criteri sarà propagato ai dispositivi client.

Quando si configura la protezione della rete in Avvio rapido guidato, Kaspersky Security Center crea il criterio predefinito per le seguenti applicazioni:

- Kaspersky Endpoint Security for Windows: per dispositivi client basati su Windows
- Kaspersky Endpoint Security for Linux: per dispositivi client basati su Linux

Se è stata completata la configurazione tramite questa procedura guidata, non è necessario creare un nuovo criterio per questa applicazione. Passare alla configurazione manuale del criterio di Kaspersky Endpoint Security.

Se si dispone di una struttura gerarchica con più Administration Server e/o gruppi di amministrazione, per impostazione predefinita gli Administration Server secondari e i gruppi di amministrazione figlio ereditano i criteri dall'Administration Server primario. È possibile forzare l'ereditarietà da parte dei gruppi figlio e degli Administration Server secondari per impedire eventuali modifiche delle impostazioni configurate nel criterio upstream. Se si desidera forzare l'ereditarietà solo di una parte delle impostazioni, è possibile bloccarle nel criterio upstream. Le restanti impostazioni sbloccate saranno disponibili per la modifica nei criteri downstream. La gerarchia di criteri creata consente di gestire in modo efficace i dispositivi nei gruppi di amministrazione.

Istruzioni dettagliate:

- Administration Console: Creazione di un criterio
- Kaspersky Security Center Web Console: Creazione di un criterio

2. **Creazione dei profili criterio (facoltativo)**

Se si desidera applicare differenti impostazioni dei criteri ai dispositivi all'interno di un singolo gruppo di amministrazione, creare profili criterio per tali dispositivi. Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo nel dispositivo gestito.

Utilizzando le condizioni di attivazione del profilo, è possibile applicare diversi profili criterio, ad esempio ai dispositivi appartenenti a un determinato gruppo di protezione o a un'unità specifica di Active Directory, con una specifica configurazione hardware o contrassegnati con tag specifici. Utilizzare i tag per filtrare i dispositivi che soddisfano i criteri specificati. È ad esempio possibile creare un tag denominato *Windows*, contrassegnare tutti i dispositivi con sistema operativo Windows con questo tag e quindi specificare il tag come condizione di attivazione per un profilo criterio. Come risultato, le applicazioni Kaspersky installate in tutti i dispositivi che eseguono Windows verranno gestite dal profilo criterio corrispondente.

Istruzioni dettagliate:

- Administration Console:
  - Creazione di un profilo criterio
  - Creazione di una regola di attivazione del profilo criterio
- Kaspersky Security Center Web Console:
  - Creazione di un profilo criterio
  - Creazione di una regola di attivazione del profilo criterio

3. **Propagazione di criteri e profili criterio nei dispositivi gestiti**

Per impostazione predefinita, Administration Server si sincronizza automaticamente con i dispositivi gestiti ogni 15 minuti. È possibile ignorare la sincronizzazione automatica ed eseguire manualmente la sincronizzazione utilizzando il comando Forza sincronizzazione. Anche la sincronizzazione viene forzata dopo aver creato o modificato un criterio o un profilo criterio. Durante la sincronizzazione, i criteri e i profili criterio nuovi o modificati vengono propagati ai dispositivi gestiti.

Se si utilizza Kaspersky Security Center Web Console, è possibile verificare se a un dispositivo sono stati inviati criteri e profili criterio. Kaspersky Security Center specifica la data e l'ora di invio nelle proprietà del dispositivo.

Istruzioni dettagliate:

- Administration Console: Sincronizzazione forzata
- Kaspersky Security Center Web Console: Sincronizzazione forzata

Risultati

Al termine dello scenario incentrato sui dispositivi, le applicazioni Kaspersky vengono configurate in base alle impostazioni specificate e propagate tramite la gerarchia di criteri.

I criteri delle applicazioni e i profili criterio configurati verranno applicati automaticamente ai nuovi dispositivi aggiunti ai gruppi di amministrazione.

Informazioni sui metodi di gestione della protezione incentrati sui dispositivi e incentrati sugli utenti

È possibile gestire le impostazioni di protezione dal punto di vista delle funzionalità del dispositivo e dal punto di vista dei ruoli utente. Il primo metodo è denominato *gestione della protezione incentrata sui dispositivi* e il secondo è denominato *gestione della protezione incentrata sugli utenti*. Per applicare impostazioni dell'applicazione diverse a diversi dispositivi è possibile utilizzare uno o entrambi i tipi di gestione insieme. Per l'implementazione della gestione della protezione incentrata sui dispositivi, è possibile utilizzare gli strumenti offerti in Administration Console basata su Microsoft Management Console o Kaspersky Security Center Web Console. La gestione della protezione incentrata sugli utenti può essere implementata solo tramite Kaspersky Security Center Web Console.

La gestione della protezione incentrata sui dispositivi consente di applicare diverse impostazioni dell'applicazione di protezione ai dispositivi gestiti in base alle funzionalità specifiche del dispositivo. È ad esempio possibile applicare impostazioni diverse ai dispositivi allocati in diversi gruppi di amministrazione. È inoltre possibile differenziare i dispositivi in base all'utilizzo di tali dispositivi in Active Directory o alle relative specifiche hardware.

La gestione della protezione incentrata sugli utenti consente di applicare diverse impostazioni dell'applicazione di protezione a diversi ruoli utente. È possibile creare diversi ruoli utente, assegnare un ruolo utente appropriato a ciascun utente e definire diverse impostazioni dell'applicazione per i dispositivi di proprietà di utenti con ruoli diversi. È ad esempio possibile applicare differenti impostazioni dell'applicazione ai dispositivi degli addetti alla contabilità e degli specialisti delle risorse umane (HR). Di conseguenza, quando viene implementata la gestione della protezione incentrata sugli utenti, ciascun reparto (reparto account e reparto HR) dispone della propria configurazione delle impostazioni per le applicazioni Kaspersky. Una configurazione delle impostazioni definisce le impostazioni delle applicazioni che possono essere modificate dagli utenti e quelle che vengono forzatamente impostate e bloccate dall'amministratore.

Utilizzando la gestione della protezione incentrata sugli utenti è possibile applicare impostazioni specifiche di un'applicazione per singoli utenti. Questo può essere necessario quando un dipendente ha un ruolo esclusivo nell'azienda o quando si desidera monitorare i problemi di sicurezza relativi ai dispositivi di una persona specifica. A seconda del ruolo di questo dipendente nell'azienda, è possibile espanderne o limitarne i diritti di modifica delle impostazioni dell'applicazione. È ad esempio possibile espandere i diritti di un amministratore di sistema che gestisce i dispositivi client in una sede locale.

È inoltre possibile combinare gli approcci di gestione della protezione incentrata sui dispositivi e incentrata sugli utenti. È ad esempio possibile configurare uno specifico criterio dell'applicazione per ogni gruppo di amministrazione e quindi creare profili criterio per uno o più ruoli utente dell'azienda. In questo caso criteri e profili criterio vengono applicati nel seguente ordine:

1. Vengono applicati i criteri creati per la gestione della protezione incentrata sui dispositivi.
2. Questi vengono modificati dai profili criterio secondo le priorità dei profili criterio.
3. I criteri vengono modificati dai profili criterio associati ai ruoli utente.

Configurazione manuale del criterio di Kaspersky Endpoint Security

Questa sezione fornisce raccomandazioni su come configurare il criterio di Kaspersky Endpoint Security, creato dall'Avvio rapido guidato. È possibile eseguire la configurazione nella finestra delle proprietà del criterio.

Durante la modifica di un'impostazione, tenere presente che è necessario fare clic sull'icona di blocco sopra l'impostazione appropriata per consentire l'utilizzo del relativo valore su una workstation.

Configurazione del criterio nella sezione Protezione minacce avanzata

Per una descrizione completa delle impostazioni in questa sezione, fare riferimento alla documentazione di Kaspersky Endpoint Security for Windows.

Nella sezione **Protezione minacce avanzata** è possibile configurare l'utilizzo di Kaspersky Security Network per Kaspersky Endpoint Security for Windows. È inoltre possibile configurare i moduli di Kaspersky Endpoint Security for Windows, ad esempio Rilevamento del Comportamento, Prevenzione Exploit, Prevenzione Intrusioni Host e Motore di Remediation.

Nella sottosezione **Kaspersky Security Network** è consigliabile abilitare l'opzione **Kaspersky Security Network**. L'utilizzo di questa opzione consente di ridistribuire e ottimizzare il traffico nella rete. Se l'opzione **Kaspersky Security Network** è disabilitata, è possibile abilitare l'uso diretto dei server KSN.

Configurazione del criterio nella sezione Protezione minacce essenziale

Per una descrizione completa delle impostazioni in questa sezione, fare riferimento alla documentazione di Kaspersky Endpoint Security for Windows.

Nella sezione **Protezione minacce essenziale** della finestra delle proprietà del criterio, si consiglia di specificare impostazioni aggiuntive nelle sottosezioni **Firewall** e **Protezione minacce file**.

La sottosezione **Firewall** contiene le impostazioni che consentono di controllare le attività di rete delle applicazioni sui dispositivi client. Un dispositivo client utilizza una rete a cui è assegnato uno dei seguenti stati: pubblico, locale o attendibile. A seconda dello stato della rete, Kaspersky Endpoint Security può consentire o negare le attività di rete su un dispositivo. Quando si aggiunge una nuova rete all'organizzazione, è necessario assegnare uno stato di rete appropriato a questa. Ad esempio, se il dispositivo client è un laptop, si consiglia che questo dispositivo utilizzi la rete pubblica o attendibile, poiché il laptop non è sempre connesso alla rete locale. Nella sottosezione **Firewall**, è possibile verificare se sono stati assegnati correttamente gli stati alle reti utilizzate nell'organizzazione.

Per controllare l'elenco delle reti:

1. Nelle proprietà del criterio, passare a **Protezione minacce essenziale** → **Firewall**.
2. Nella sezione **Reti disponibili**, fare clic sul pulsante **Impostazioni**.
3. Nella finestra **Firewall** visualizzata, passare alla scheda **Reti** per visualizzare l'elenco delle reti.

Nella sottosezione **Protezione minacce file**, è possibile disabilitare la scansione delle unità di rete. La scansione delle unità di rete può comportare un carico significativo per le unità di rete. È più pratico eseguire la scansione indiretta sui file server.

Per disabilitare la scansione delle unità di rete:

1. Nelle proprietà del criterio, passare a **Protezione minacce essenziale** → **Protezione minacce file**.
2. Nella sezione **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
3. Nella finestra **Protezione minacce file** visualizzata, nella scheda **Generali**, deselezionare la casella di controllo **Tutte le unità di rete**.

Configurazione del criterio nella sezione Impostazioni generali

Per una descrizione completa delle impostazioni in questa sezione, fare riferimento alla documentazione di Kaspersky Endpoint Security for Windows.

Nella sezione **Impostazioni generali** della finestra delle proprietà del criterio, si consiglia di specificare impostazioni aggiuntive nelle sottosezioni **Rapporti e archivi** e **Interfaccia**.

Nella sottosezione **Rapporti e archivi**, passare alla sezione **Trasferimento dei dati ad Administration Server**. La casella di controllo **Informazioni sulle applicazioni avviate** specifica se il database di Administration Server salva informazioni su tutte le versioni di tutti i moduli software nei dispositivi connessi alla rete. Se questa casella di controllo è selezionata, le informazioni salvate possono richiedere una quantità significativa di spazio su disco nel database di Kaspersky Security Center (decine di gigabyte). Deselezionare la casella di controllo **Informazioni sulle applicazioni avviate** se è selezionata nel criterio di livello superiore.

Se Administration Console gestisce la protezione dalle minacce nella rete dell'organizzazione in modalità centralizzata, disabilitare la visualizzazione dell'interfaccia utente di Kaspersky Endpoint Security for Windows sulle workstation. A tale scopo, nella sottosezione **Interfaccia**, passare alla sezione **Interazione con l'utente**, quindi selezionare **Non visualizzare l'interfaccia utente**.

Per abilitare la protezione tramite password sulle workstation, nella sottosezione **Interfaccia**, passare alla sezione **Protezione tramite password**, fare clic sul pulsante **Impostazioni**, quindi selezionare la casella di controllo **Abilita protezione tramite password**.

Configurazione del criterio nella sezione Configurazione eventi

Nella sezione **Configurazione eventi** è consigliabile disabilitare il salvataggio di qualsiasi evento in Administration Server, tranne i seguenti:

- Nella scheda **Critico**:
  - *L'esecuzione automatica dell'applicazione è disabilitata*
  - *Accesso negato*
  - *Avvio dell'applicazione non consentito*
  - *Disinfezione impossibile*
  - *Contratto di licenza con l'utente finale violato*
  - *Impossibile caricare il modulo di criptaggio*
  - *Impossibile avviare due attività contemporaneamente*
  - *È stata rilevata una minaccia attiva. Si consiglia di avviare Disinfezione avanzata*
  - *Attacco di rete rilevato*
  - *Non tutti i componenti sono stati aggiornati*
  - *Errore di attivazione*
  - *Errore durante l'abilitazione della modalità portatile*
  - *Errore durante l'interazione con Kaspersky Security Center*
  - *Errore durante la disabilitazione della modalità portatile*
  - *Errore durante la modifica dei componenti dell'applicazione*
  - *Errore durante l'applicazione delle regole di criptaggio/decriptaggio dei file*
  - *Il criterio non può essere applicato*
  - *Processo terminato*
  - *Attività di rete bloccata*
- Nella scheda **Errore funzionale**: *Impostazioni attività non valide. Impostazioni non applicate*

- Nella scheda **Avviso**:
  - *L'Auto-difesa è disabilitata*
  - *Chiave di riserva errata*
  - *L'utente ha scelto di non applicare il criterio di criptaggio*
- Nella scheda **Informazioni**: *Avvio dell'applicazione non consentito in modalità di test*

Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security

L'opzione di pianificazione ottimale e consigliata per Kaspersky Endpoint Security versione 10 e successive è **Quando vengono scaricati nuovi aggiornamenti nell'archivio** quando la casella di controllo **Usa automaticamente il ritardo casuale per l'avvio delle attività** è selezionata.

Configurazione manuale dell'attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security

L'Avvio rapido guidato crea un'attività di gruppo per la scansione di un dispositivo. Per impostazione predefinita, all'attività viene assegnata una pianificazione **Esegui il venerdì alle 19:00** con un'impostazione casuale automatica e la casella di controllo **Esegui attività non effettuate** è deselezionata.

Di conseguenza, se i dispositivi in un'organizzazione vengono spenti ad esempio il venerdì alle 18:30, l'attività di scansione del dispositivo non verrà eseguita. È necessario impostare la pianificazione appropriata per questa attività in base alle regole per l'ambiente di lavoro adottate nell'organizzazione.

Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti

L'Avvio rapido guidato crea l'attività *Trova vulnerabilità e aggiornamenti richiesti* per Network Agent. Per impostazione predefinita, all'attività viene assegnata una pianificazione **Esegui il martedì alle 19:00** con un'impostazione casuale automatica e la casella di controllo **Esegui attività non effettuate** è selezionata.

Se le regole dell'organizzazione per l'ambiente di lavoro prevedono lo spegnimento di tutti i dispositivi in tale orario, l'attività *Trova vulnerabilità e aggiornamenti richiesti* verrà eseguita dopo la riaccensione dei dispositivi, il mercoledì mattina. Un'attività di questo tipo potrebbe essere indesiderabile perché una Scansione vulnerabilità può aumentare il carico sui sottosistemi del disco e della CPU. È necessario impostare la pianificazione appropriata per l'attività in base alle regole per l'ambiente di lavoro adottate nell'organizzazione.

Configurazione manuale dell'attività di gruppo per l'installazione degli aggiornamenti e la correzione delle vulnerabilità

L'Avvio rapido guidato crea un'attività di gruppo per l'installazione degli aggiornamenti e la correzione delle vulnerabilità per Network Agent. Per impostazione predefinita, l'attività è impostata per l'esecuzione ogni giorno alle 01:00, con un'impostazione casuale automatica, e l'opzione **Esegui attività non effettuate** non è abilitata.

Se le regole dell'organizzazione per l'ambiente di lavoro prevedono lo spegnimento dei dispositivi durante la notte, l'installazione degli aggiornamenti non verrà eseguita. È necessario impostare la pianificazione appropriata per l'attività Scansione vulnerabilità in base alle regole per l'ambiente di lavoro adottate nell'organizzazione. È anche importante tenere presente che l'installazione degli aggiornamenti può richiedere il riavvio del dispositivo.

Impostazione del numero massimo di eventi nell'archivio eventi

Nella sezione **Archivio eventi** della finestra delle proprietà di Administration Server è possibile modificare le impostazioni per l'archiviazione degli eventi nel database di Administration Server, limitando il numero di record degli eventi e il periodo di archiviazione dei record. Quando si specifica il numero massimo di eventi, l'applicazione calcola approssimativamente la quantità di spazio di archiviazione necessario per il numero specificato. È possibile utilizzare questo calcolo approssimativo per valutare se è necessario liberare spazio su disco per evitare l'overflow del database. La capacità predefinita del database di Administration Server è di 400.000 eventi. La capacità massima consigliata del database è di 45 milioni di eventi.

L'applicazione controlla il database ogni 10 minuti. Se il numero di eventi raggiunge il valore massimo specificato più 10.000, l'applicazione elimina gli eventi meno recenti in modo che rimanga solo il numero massimo di eventi specificato.

Quando l'Administration Server elimina gli eventi meno recenti, non può salvare i nuovi eventi nel database. Durante questo periodo di tempo, le informazioni sugli eventi rifiutati vengono scritte nel registro eventi Kaspersky. I nuovi eventi vengono accodati e quindi salvati nel database al termine dell'operazione di eliminazione.

Per limitare il numero di eventi che è possibile archiviare nell'archivio eventi di Administration Server:

1. Fare clic con il pulsante destro del mouse su Administration Server, quindi selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nell'area di lavoro della sezione **Archivio eventi** specificare il numero massimo di eventi archiviati nel database.

3. Fare clic su **OK**.

È inoltre possibile modificare le impostazioni di qualsiasi attività per salvare gli eventi relativi all'avanzamento dell'attività oppure salvare solo i risultati dell'esecuzione dell'attività. In tal modo si riduce il numero di eventi nel database, si aumenta la velocità di esecuzione degli scenari associati all'analisi della tabella degli eventi nel database e si limita il rischio che gli eventi critici vengano sovrascritti da un ampio numero di eventi.

Impostazione del periodo di archiviazione massimo per le informazioni sulle vulnerabilità corrette

Per impostare il periodo di archiviazione massimo nel database per le informazioni sulle vulnerabilità già corrette nei dispositivi gestiti:

1. Fare clic con il pulsante destro del mouse su Administration Server, quindi selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nell'area di lavoro della sezione **Archivio eventi** specificare il periodo di archiviazione massimo per le informazioni sulle vulnerabilità corrette nel database.

   Per impostazione predefinita, il periodo di archiviazione è di 90 giorni.

3. Fare clic su **OK**.

Il periodo di archiviazione massimo per le informazioni sulle vulnerabilità corrette si limita al numero di giorni specificato. Successivamente, l'attività di manutenzione di Administration Server eliminerà le informazioni obsolete dal database.

Gestione di attività

Kaspersky Security Center consente di gestire le applicazioni installate nei dispositivi creando ed eseguendo varie attività. Le attività sono necessarie per l'installazione, l'avvio e l'arresto delle applicazioni, la scansione dei file, l'aggiornamento dei database e dei moduli software, oltre che per eseguire altre azioni sulle applicazioni.

Le attività sono suddivise nei seguenti tipi:

- *Attività di gruppo*. Attività eseguite nei dispositivi del gruppo di amministrazione selezionato.
- *Attività di Administration Server*. Attività eseguite in Administration Server.
- *Attività per dispositivi specifici*. Attività eseguite su dispositivi selezionati, indipendentemente dalla loro appartenenza a un gruppo di amministrazione.
- *Attività locali*. Attività eseguite in un dispositivo specifico.

È possibile creare un attività dell'applicazione solo se il plug-in di gestione dell'applicazione corrispondente è installato nella workstation dell'amministratore.

È possibile compilare un elenco di dispositivi (fino a 1000 dispositivi) per cui creare un'attività in uno dei seguenti modi:

- Selezionando i dispositivi della rete individuati da Administration Server.
- Specificando manualmente un elenco di dispositivi. È possibile utilizzare un indirizzo IP (o un intervallo IP), un nome NetBIOS o un nome DNS come indirizzo del dispositivo.
- Importare un elenco di dispositivi da un file .txt che contiene gli indirizzi dei dispositivi da aggiungere (ogni indirizzo deve essere specificato su una riga distinta).

  Se si importa un elenco di dispositivi da un file o se ne crea uno manualmente e i dispositivi vengono identificati con i rispettivi nomi, l'elenco deve contenere solo dispositivi per cui sono già state immesse le informazioni nel database di Administration Server al momento della connessione dei dispositivi o durante la device discovery.

Per ogni applicazione è possibile creare attività di gruppo, attività per dispositivi specifici o attività locali.

Lo scambio di informazioni sulle attività tra un'applicazione installata in un dispositivo e il database di Kaspersky Security Center avviene al momento della connessione di Network Agent ad Administration Server.

È possibile apportare modifiche alle impostazioni delle attività, visualizzarne l'avanzamento, copiarle, esportarle, importarle ed eliminarle.

Le attività vengono avviate in un dispositivo solo se l'applicazione per cui l'attività è stata creata è in esecuzione. Quando l'applicazione non è in esecuzione, tutte le attività in esecuzione vengono annullate.

I risultati delle attività completate sono salvati nei registri eventi di Microsoft Windows e di Kaspersky Security Center, sia in modo centralizzato in Administration Server che localmente in ogni dispositivo.

Non includere dati privati nelle impostazioni dell'attività. Ad esempio, non specificare la password dell'amministratore del dominio.

Dettagli della gestione delle attività per le applicazioni con supporto multi-tenancy

Un'attività di gruppo per un'applicazione con supporto multi-tenancy viene applicata all'applicazione a seconda della gerarchia di Administration Server e dispositivi client. L'Administration Server virtuale da cui viene creata l'attività deve essere nello stesso gruppo di amministrazione o in un gruppo di amministrazione di livello inferiore rispetto al dispositivo client in cui è installata l'applicazione.

Negli eventi che corrispondono ai risultati dell'esecuzione dell'attività, per un amministratore di un provider di servizi vengono visualizzate le informazioni sul dispositivo in cui è stata eseguita l'attività. Al contrario, per un amministratore del tenant viene visualizzato **Nodo multi-tenant**.

Creazione di un'attività

In Administration Console è possibile creare le attività direttamente nella cartella del gruppo di amministrazione per cui è necessario creare un'attività di gruppo o nell'area di lavoro della cartella **Attività**.

Per creare un'attività di gruppo nella cartella di un gruppo di amministrazione:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui si desidera creare un'attività.
2. Nell'area di lavoro del gruppo selezionare la scheda **Attività**.
3. Eseguire la creazione dell'attività facendo clic sul pulsante **Crea attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

*Per creare un'attività nell'area di lavoro della cartella **Attività**:*

1. Nella struttura della console selezionare la cartella **Attività**.
2. Eseguire la creazione dell'attività facendo clic sul pulsante **Fine**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

Non includere dati privati nelle impostazioni dell'attività. Ad esempio, non specificare la password dell'amministratore del dominio.

Creazione dell'attività di Administration Server

Administration Server esegue le seguenti attività:

- Invia rapporti
- Scarica aggiornamenti nell'archivio dell'Administration Server
- Backup dei dati di Administration Server
- Manutenzione di Administration Server
- Esegui sincronizzazione di Windows Update
- Crea pacchetto di installazione in base all'immagine del sistema operativo del dispositivo
- Installa l'applicazione in remoto
- Disinstalla l'applicazione in remoto
- Distribuisci pacchetto di installazione
- Installa l'applicazione negli Administration Server secondari in remoto

In un Administration Server virtuale sono disponibili solo l'attività di invio automatico dei rapporti e l'attività di creazione del pacchetto di installazione dall'immagine del sistema operativo di un dispositivo di riferimento. L'archivio dell'Administration Server virtuale visualizza gli aggiornamenti scaricati nell'Administration Server primario. Il backup dei dati dell'Administration Server virtuale viene eseguito durante il backup dei dati dell'Administration Server primario.

Per creare l'attività di Administration Server:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Avviare la creazione dell'attività in uno dei seguenti modi:
   - Selezionando **Nuovo** → **Attività** nel menu di scelta rapida della cartella **Attività** nella struttura della console.
   - Facendo clic sul pulsante **Crea attività** nell'area di lavoro della cartella **Attività**.

Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

Le attività Scarica aggiornamenti nell'archivio dell'Administration Server, Esegui sincronizzazione di Windows Update, Manutenzione Administration Server e *Backup dei dati di Administration Server* possono essere create una sola volta. Se le attività *Scarica gli aggiornamenti nell'archivio dell'Administration Server*, *Manutenzione Administration Server*, *Backup dei dati di Administration Server* ed *Esegui sincronizzazione di Windows Update* sono già state create per Administration Server, non verranno visualizzate nella finestra di selezione del tipo di attività della Creazione guidata nuova attività.

Creazione di un'attività per dispositivi specifici

In Kaspersky Security Center è possibile creare attività per dispositivi specifici. I dispositivi di un set possono essere inclusi in vari gruppi di amministrazione o non appartenere ad alcun gruppo. Kaspersky Security Center può eseguire le seguenti attività principali per dispositivi specifici:

- Installazione remota di un'applicazione
- Invia messaggio all'utente
- Modifica di Administration Server
- Gestisci dispositivi
- Verifica aggiornamenti
- Distribuzione dei pacchetti di installazione
- Installa l'applicazione negli Administration Server secondari in remoto
- Disinstallazione di un'applicazione in remoto

Per creare un'attività per dispositivi specifici:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Avviare la creazione dell'attività in uno dei seguenti modi:
   - Selezionando **Nuovo** → **Attività** nel menu di scelta rapida della cartella **Attività** nella struttura della console.
   - Facendo clic sul pulsante **Crea attività** nell'area di lavoro della cartella **Attività**.

Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

Creazione di un'attività locale

Per creare un'attività locale per un dispositivo:

1. Selezionare la scheda **Dispositivi** nell'area di lavoro del gruppo che include il dispositivo.
2. Dall'elenco dei dispositivi nella scheda **Dispositivi** selezionare il dispositivo per cui è necessario creare un'attività locale.
3. Avviare la creazione dell'attività per il dispositivo selezionato in uno dei seguenti modi:
   - Fare clic sul pulsante **Esegui azione** e selezionare **Crea attività** nell'elenco a discesa.
   - Fare clic sul collegamento **Crea attività** nell'area di lavoro del dispositivo.
   - Utilizzare le proprietà del dispositivo come segue:
     a. Nel menu di scelta rapida del dispositivo selezionare **Proprietà**.
     b. Nella finestra delle proprietà del dispositivo visualizzata selezionare la sezione **Attività**, quindi fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

Le istruzioni dettagliate su come creare e configurare le attività locali sono fornite nelle Guide delle rispettive applicazioni Kaspersky.

Visualizzazione di un'attività di gruppo ereditata nell'area di lavoro di un gruppo nidificato

Per abilitare la visualizzazione delle attività ereditate di un gruppo nidificato nell'area di lavoro:

1. Selezionare la scheda **Attività** nell'area di lavoro di un gruppo nidificato.
2. Nell'area di lavoro della scheda **Attività** fare clic sul pulsante **Mostra attività ereditate**.

Le attività ereditate verranno visualizzate nell'elenco delle attività con una delle seguenti icone:

-  – Se sono stati ereditati da un gruppo creato nell'Administration Server primario.
-  – Se sono stati ereditati da un gruppo di livello superiore.

Se è abilitata la modalità di ereditarietà, le attività ereditate possono essere modificate solo nel gruppo in cui sono state create. Le attività ereditate non possono essere modificate nel gruppo che eredita le attività.

Accensione automatica dei dispositivi prima dell'avvio di un'attività

Kaspersky Security Center non esegue attività sui dispositivi spenti. È possibile configurare Kaspersky Security Center per l'accensione automatica di questi dispositivi prima di avviare un'attività, utilizzando la funzione Wake-on-LAN.

Per configurare l'accensione automatica dei dispositivi prima dell'avvio di un'attività:

1. Nella finestra delle proprietà dell'attività selezionare la sezione **Pianificazione**.
2. Per configurare le azioni sui dispositivi, fare clic sul collegamento **Avanzate**.
3. Nella finestra **Avanzate** visualizzata selezionare la casella di controllo **Accendi i dispositivi utilizzando la funzione Wake-on-LAN prima di avviare l'attività (min)** e specificare l'intervallo di tempo in minuti.

Di conseguenza, per il numero di minuti specificato prima dell'avvio dell'attività, Kaspersky Security Center accende i dispositivi e carica il sistema operativo su questi utilizzando la funzione Wake-on-LAN. Al termine dell'attività, i dispositivi vengono automaticamente spenti se gli utenti del dispositivo non accedono al sistema. Si noti che Kaspersky Security Center spegne automaticamente solo i dispositivi accesi utilizzando la funzione Wake-on-LAN.

Kaspersky Security Center può avviare automaticamente i sistemi operativi solo sui dispositivi che supportano lo standard Wake-on-LAN (WoL).

Spegnimento automatico di un dispositivo dopo il completamento di un'attività

Kaspersky Security Center consente di configurare un'attività in modo che i dispositivi a cui è distribuita vengano spenti automaticamente dopo il completamento dell'attività.

Per spegnere automaticamente un dispositivo dopo il completamento di un'attività:

1. Nella finestra delle proprietà dell'attività selezionare la sezione **Pianificazione**.
2. Fare clic sul collegamento **Avanzate** per aprire la finestra per la configurazione delle azioni sui dispositivi.
3. Nella finestra **Avanzate** visualizzata selezionare la casella di controllo **Spegni i dispositivi dopo il completamento dell'attività**.

Limitazione del tempo di esecuzione delle attività

Per limitare il tempo di esecuzione di un'attività nei dispositivi:

1. Nella finestra delle proprietà dell'attività selezionare la sezione **Pianificazione**.
2. Fare clic su **Avanzate** per aprire la finestra per la configurazione delle azioni nei dispositivi client.
3. Nella finestra **Avanzate** visualizzata selezionare la casella di controllo **Arresta se l'attività viene eseguita per più di (min)** e specificare l'intervallo di tempo in minuti.

Se l'attività non è ancora stata completata nel dispositivo al termine dell'intervallo di tempo specificato, Kaspersky Security Center interrompe automaticamente l'attività.

Esportazione di un'attività

È possibile esportare in un file attività di gruppo e attività per dispositivi specifici. Le attività di Administration Server non sono disponibili per l'esportazione.

Per esportare un'attività:

1. Nel menu di scelta rapida dell'attività selezionare **Tutte le attività** → **Esporta**.
2. Nella finestra **Salva con nome** visualizzata specificare il percorso e il nome del file.
3. Fare clic sul pulsante **Salva**.

I diritti degli utenti locali non vengono esportati.

Importazione di un'attività

È possibile importare attività di gruppo e attività per dispositivi specifici. Le attività di Administration Server non sono disponibili per l'importazione.

Per importare un'attività:

1. Selezionare l'elenco in cui deve essere importata l'attività:
   - Per importare l'attività nell'elenco delle attività di gruppo, selezionare la scheda **Attività** nell'area di lavoro del gruppo di amministrazione desiderato.
   - Per importare un'attività nell'elenco delle attività per dispositivi specifici, selezionare la cartella **Attività** nella struttura della console.
2. Selezionare una delle seguenti opzioni per importare l'attività:
   - Nel menu di scelta rapida dell'elenco dell'attività selezionare **Tutte le attività** → **Importa**.
   - Fare clic sul collegamento **Importa attività da file** nella sezione di gestione dell'elenco attività.
3. Nella finestra visualizzata specificare il percorso del file da cui si desidera importare un'attività.
4. Fare clic sul pulsante **Apri**.

   L'attività verrà visualizzata nell'elenco delle attività.

Se l'attività appena importata ha un nome identico a un'attività esistente, il nome dell'attività importata viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Conversione di attività

È possibile utilizzare Kaspersky Security Center per convertire le attività delle versioni precedenti delle applicazioni Kaspersky in attività delle versioni correnti delle stesse applicazioni.

La conversione è disponibile per le attività delle seguenti applicazioni:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

Per convertire le attività:

1. Nella struttura della console selezionare un Administration Server per cui si desidera convertire le attività.
2. Nel menu di scelta rapida di Administration Server selezionare **Tutte le attività** → **Conversione guidata in batch criteri e attività**.

   Verrà avviata la Conversione guidata criteri e attività. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata vengono create nuove attività, che utilizzano le impostazioni delle attività delle versioni precedenti delle applicazioni.

Avvio e arresto manuale di un'attività

È possibile avviare e arrestare manualmente le attività tramite uno dei seguenti metodi: dal menu di scelta rapida dell'attività o nella finestra delle proprietà del dispositivo client a cui è stata assegnata l'attività.

L'avvio di attività di gruppo dal menu di scelta rapida del dispositivo è consentito solo agli utenti appartenenti al gruppo **KLAdmins**.

Per avviare o arrestare un'attività dal menu di scelta rapida o dalla finestra delle proprietà dell'attività:

1. Selezionare un'attività nell'elenco delle attività.
2. Avviare o interrompere l'attività in uno dei seguenti modi:
   - Selezionando **Avvia** o **Arresta** nel menu di scelta rapida dell'attività.
   - Fare clic su **Avvia** o **Arresta** nella sezione **Generale** della finestra delle proprietà dell'attività.

Per avviare o arrestare un'attività dal menu di scelta rapida o dalla finestra delle proprietà del dispositivo client:

1. Selezionare il dispositivo nell'elenco dei dispositivi.
2. Avviare o interrompere l'attività in uno dei seguenti modi:
   - Selezionare **Tutte le attività** → **Esegui attività** nel menu di scelta rapida del dispositivo. Selezionare l'attività di riferimento dall'elenco delle attività.

     L'elenco dei dispositivi a cui è assegnata l'attività verrà sostituito dal dispositivo selezionato. L'attività viene avviata.
   - Fare clic sul pulsante di avvio () o sul pulsante di interruzione () nella sezione **Attività** della finestra delle proprietà del dispositivo.

Sospensione e ripresa manuale di un'attività

Per sospendere o riprendere manualmente un'attività in esecuzione:

1. Selezionare un'attività nell'elenco delle attività.
2. Sospendere o riprendere l'attività in uno dei seguenti modi:
   - Selezionando **Sospendi** o **Riprendi** nel menu di scelta rapida dell'attività.
   - Selezionando la sezione **Generale** nella finestra delle proprietà dell'attività e facendo clic su **Sospendi** or **Riprendi**.

Monitoraggio dell'esecuzione delle attività

Per monitorare l'esecuzione delle attività:

nella finestra delle proprietà dell'attività selezionare la sezione **Generale**.

Nella parte centrale della sezione **Generale** viene visualizzato lo stato corrente dell'attività.

Visualizzazione dei risultati dell'esecuzione delle attività memorizzati in Administration Server

Kaspersky Security Center consente di visualizzare i risultati dell'esecuzione delle attività di gruppo, le attività per dispositivi specifici e le attività di Administration Server.

Per visualizzare i risultati di un'attività:

1. Nella finestra delle proprietà dell'attività selezionare la sezione **Generale**.
2. Fare clic sul collegamento **Risultati** per aprire la finestra **Risultati attività**.

Per visualizzare i risultati dell'attività per un Administration Server secondario:

1. Nella finestra delle proprietà dell'attività selezionare la sezione **Generale**.
2. Fare clic sul collegamento **Risultati** per aprire la finestra **Risultati attività**.
3. Fare clic su **Statistiche dai server secondari**.
4. Selezionare il server secondario per cui si desidera visualizzare la finestra **Risultati attività**.

Configurazione di filtri per le informazioni sui risultati dell'esecuzione delle attività

Kaspersky Security Center consente di filtrare le informazioni relative ai risultati dell'esecuzione delle attività di gruppo, le attività per dispositivi specifici e le attività di Administration Server. Non sono disponibili filtri per le attività locali.

Per configurare i filtri per le informazioni sui risultati dell'esecuzione delle attività:

1. Nella finestra delle proprietà dell'attività selezionare la sezione **Generale**.
2. Fare clic sul collegamento **Risultati** per aprire la finestra **Risultati attività**.

   La tabella superiore contiene un elenco di tutti i dispositivi a cui è assegnata l'attività. La tabella inferiore visualizza i risultati dell'attività eseguita nel dispositivo selezionato.

3. Fare clic con il pulsante destro del mouse sulla tabella desiderata per aprire il menu di scelta rapida e selezionare **Filtro**.

4. Nella finestra **Imposta filtro** visualizzata definire le impostazioni del filtro nelle sezioni **Eventi**, **Dispositivi** e **Data/ora**. Fare clic su **OK**.

Nella finestra **Risultati attività** verranno visualizzate le informazioni che soddisfano le impostazioni specificate nel filtro.

Modifica di un'attività. Rollback delle modifiche

Per modificare un'attività:

1. Nella struttura della console selezionare la cartella **Attività**.

2. Nell'area di lavoro della cartella **Attività** selezionare un'attività e passare alla finestra delle proprietà dell'attività utilizzando il menu di scelta rapida.

3. Apportare le modifiche desiderate.

> Nella sezione **Esclusioni dall'ambito dell'attività** è possibile configurare l'elenco dei sottogruppi a cui non viene applicata l'attività.

4. Fare clic su **Applica**.

Le modifiche apportate all'attività saranno salvate nella finestra delle proprietà dell'attività, nella sezione **Cronologia revisioni**.

È possibile eseguire il rollback delle modifiche apportate all'attività, se necessario.

Per eseguire il rollback delle modifiche apportate a un'attività:

1. Nella struttura della console selezionare la cartella **Attività**.

2. Selezionare l'attività in cui è necessario eseguire il rollback delle modifiche e aprire la finestra delle proprietà dell'attività utilizzando il menu di scelta rapida.

3. Nella finestra delle proprietà dell'attività selezionare la sezione **Cronologia revisioni**.

4. Nell'elenco delle revisioni dell'attività selezionare il numero della revisione a cui eseguire il rollback delle modifiche.

5. Fare clic sul pulsante **Avanzate** e selezionare il valore **Rollback** nell'elenco a discesa.

Confronto delle attività

È possibile confrontare attività dello stesso tipo: ad esempio, è possibile confrontare due attività di scansione malware, ma non è possibile confrontare un'attività di scansione malware e un'attività di installazione degli aggiornamenti. Dopo il confronto, è visualizzato un rapporto che indica quali impostazioni delle attività corrispondono e quali sono diverse. È possibile stampare il rapporto di confronto delle attività o salvarlo in un file. Potrebbe essere necessario un confronto delle attività quando a diverse unità di un'azienda sono assegnate varie attività dello stesso tipo. Ad esempio, per i dipendenti del reparto contabilità viene eseguita un'attività di scansione malware solo per i dischi locali dei dispositivi, mentre per i dipendenti del reparto vendite (che comunicano con i clienti) viene eseguita un'attività di scansione sia dei messaggi e-mail che dei dischi locali. Per notare velocemente tale differenza, non è necessario visualizzare tutte le impostazioni delle attività: è sufficiente confrontare le attività.

È possibile confrontare solo attività dello stesso tipo.

È possibile confrontare le attività solo in coppia.

È possibile confrontare le attività in uno dei seguenti modi: selezionando un'attività e confrontandola con un'altra o confrontando una coppia di attività dall'elenco delle attività.

Per selezionare un'attività e confrontarla con un'altra:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Nell'area di lavoro della cartella **Attività** selezionare l'attività da confrontare con un'altra.
3. Nel menu di scelta rapida dell'attività selezionare **Tutte le attività** → **Confronta con un'altra attività**.
4. Nella finestra **Selezionare un'attività** selezionare l'attività per il confronto.
5. Fare clic su **OK**.

   Verrà visualizzato un rapporto in formato HTML che confronta le due attività.

Per confrontare una coppia di attività dall'elenco delle attività:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Nella cartella **Attività**, nell'elenco delle attività, premere il tasto **MAIUSC** o **CTRL** per selezionare due attività dello stesso tipo.
3. Nel menu di scelta rapida selezionare **Confronta**.

   Verrà visualizzato un rapporto in formato HTML che confronta le attività selezionate.

Quando vengono confrontate le attività, se le password sono differenti nel rapporto di confronto attività verranno visualizzati degli asterischi (******).

Se nelle proprietà delle attività è stata modificata la password, nel rapporto di confronto delle revisioni verranno visualizzati degli asterischi (******).

Account per l'avvio delle attività

È possibile specificare un account con cui eseguire l'attività.

Per eseguire un'attività di scansione su richiesta, ad esempio, sono necessari i diritti di accesso per l'oggetto sottoposto a scansione, mentre per eseguire un'attività di aggiornamento sono necessari i diritti utente per il server proxy. La possibilità di specificare un account per l'esecuzione dell'attività consente di evitare problemi relativi alle attività di scansione su richiesta e di aggiornamento se l'utente che esegue l'attività non dispone dei diritti di accesso richiesti.

Durante l'esecuzione delle attività di installazione o disinstallazione remota, viene utilizzato l'account specificato per scaricare nei dispositivi client i file necessari per installare o disinstallare un'applicazione nel caso Network Agent non sia installato o disponibile. Se Network Agent è installato e disponibile, l'account viene utilizzato se, in base alle impostazioni delle attività, il trasferimento dei file viene eseguito solo tramite le utilità di Microsoft Windows dalla cartella condivisa. In questo caso, l'account deve disporre dei seguenti diritti per il dispositivo:

- Diritto di avviare le applicazioni in remoto.
- Diritto di utilizzare la risorsa Admin$.
- Diritto di *accesso come servizio*.

Se i file vengono inviati ai dispositivi tramite Network Agent, l'account non verrà utilizzato. Tutte le operazioni di copia e installazione dei file verranno eseguite da **Network Agent** (**account LocalSystem**).

Esportazione delle cronologia di esecuzione delle attività

Se si riscontrano problemi durante un'attività, potrebbe essere necessario indagare sulle cause sottostanti. A tale scopo, è possibile esportare e analizzare ulteriormente la cronologia di esecuzione delle attività.

Per esportare la cronologia di esecuzione delle attività:

1. Creare un file TXT vuoto in una directory sul dispositivo.

   La cronologia di esecuzione delle attività verrà esportata in questo file.

2. Aprire la finestra dei risultati delle attività.
3. Nella parte superiore della finestra dei risultati delle attività, selezionare il dispositivo che presenta problemi.
4. Nella parte inferiore della finestra dei risultati delle attività, in cui viene visualizzata la cronologia delle esecuzioni per il dispositivo selezionato, selezionare uno o più eventi.

   Per selezionare più eventi, utilizzare il tasto **Maiusc** o **Ctrl**.

5. Fare clic con il pulsante destro del mouse sugli eventi selezionati per aprire il menu di scelta rapida e selezionare **Esporta**.

   Verrà avviata l'Esportazione guidata eventi.

6. Nella fase **File di esportazione** della procedura guidata, fare clic sul pulsante **Sfoglia**, quindi selezionare il file TXT creato per esportare la cronologia di esecuzione delle attività.

   Se si desidera esportare solo gli eventi selezionati, abilitare l'opzione **Esporta solo gli eventi selezionati**.

   Se si desidera esportare l'intera cronologia dell'esecuzione delle attività (tutti gli eventi), l'opzione **Esporta solo gli eventi selezionati** deve essere disabilitato.

7. Fare clic sul pulsante **Avanti**.

8. Nella fase **Formato di esportazione** della procedura guidata, abilitare una delle seguenti opzioni:

   - **Esporta come testo Unicode delimitato da tabulazioni**

     Abilitare questa opzione se i dati esportati includono caratteri speciali e simboli di diverse lingue e si desidera garantire che tutti i caratteri vengano mantenuti correttamente quando il file TXT con i dati esportati viene aperto in applicazioni diverse.

   - **Esporta come testo delimitato da tabulazioni**

     Abilitare questa opzione se si desidera mantenere la compatibilità con sistemi o applicazioni meno recenti che potrebbero non supportare Unicode.

9. Fare clic sul pulsante **Avanti** per terminare la procedura guidata.

La cronologia di esecuzione delle attività viene esportata nel file TXT selezionato.

Procedura guidata per la modifica della password delle attività

Per un'attività non locale, è possibile specificare un account con il quale deve essere eseguita l'attività. È possibile specificare l'account durante la creazione dell'attività o nelle proprietà di un'attività esistente. Se l'account specificato è utilizzato conformemente alle istruzioni di sicurezza dell'organizzazione, queste istruzioni possono occasionalmente richiedere la modifica della password dell'account. Quando scade la password dell'account e viene impostata una nuova password, l'attività non verrà avviata fino a quando non viene specificata la nuova password valida nelle proprietà dell'attività.

La Procedura guidata per la modifica della password delle attività consente di sostituire automaticamente la vecchia password con la nuova in tutte le attività in cui è specificato l'account. In alternativa è possibile eseguire manualmente l'operazione nelle proprietà di ogni attività.

Per avviare la Procedura guidata per la modifica della password delle attività:

1. Nella struttura della console selezionare il nodo **Attività**.

2. Nel menu di scelta rapida del nodo selezionare **Procedura guidata per la modifica della password delle attività**.

Seguire le istruzioni della procedura guidata.

Passaggio 1. Immissione delle credenziali

Nei campi **Account** e **Password** specificare le nuove credenziali attualmente valide nel sistema (ad esempio in Active Directory). Quando si passa al passaggio successivo della procedura guidata, Kaspersky Security Center verifica se il nome dell'account specificato corrisponde al nome dell'account nelle proprietà di ogni attività non locale. Se il nome dell'account corrisponde, la password nelle proprietà dell'attività verrà automaticamente sostituita con quella nuova.

Se si compila il campo **Password precedente (opzionale)**, Kaspersky Security Center sostituisce la password solo per le attività in cui si trovano sia il nome dell'account sia la password precedente. La sostituzione viene eseguita automaticamente. In tutti gli altri casi è necessario scegliere un'azione da eseguire nel passaggio successivo della procedura guidata.

Passaggio 2. Selezione di un'azione da eseguire

Se non è stata specificata la password precedente nel primo passaggio della procedura guidata o se la password precedente specificata non corrisponde alle password nelle attività, è necessario scegliere un'azione da eseguire per le attività rilevate.

Per ciascuna attività con lo stato *Richiesta approvazione*, decidere se rimuovere la password nelle proprietà dell'attività o sostituirla con quella nuova. Se si sceglie di rimuovere la password, l'attività viene eseguita con l'account predefinito.

Passaggio 3. Visualizzazione dei risultati

Nell'ultimo passaggio della procedura guidata, visualizzare i risultati per ciascuna attività rilevata. Per completare la procedura guidata, fare clic sul pulsante **Fine**.

Creazione di una gerarchia di gruppi di amministrazione subordinati a un Administration Server virtuale

Dopo la creazione dell'Administration Server virtuale, questo contiene per impostazione predefinita un gruppo di amministrazione denominato **Dispositivi gestiti**.

La procedura per la creazione di una gerarchia di gruppi di amministrazione subordinati a un Administration Server virtuale è identica alla procedura per la creazione di una gerarchia di gruppi di amministrazione subordinati all'Administration Server fisico.

Non è possibile aggiungere Administration Server secondari e virtuali ai gruppi di amministrazione subordinati a un Administration Server virtuale. Ciò è dovuto alle limitazioni degli Administration Server virtuali.

Criteri e profili criterio

In Kaspersky Security Center Web Console è possibile creare criteri per le applicazioni Kaspersky. Questa sezione descrive i criteri e i profili criterio e fornisce istruzioni per crearli e modificarli.

Gerarchia di criteri tramite i profili criterio

Questa sezione fornisce informazioni su come applicare i criteri ai dispositivi nei gruppi di amministrazione. Questa sezione fornisce anche informazioni sui profili dei criteri.

Gerarchia dei criteri

In Kaspersky Security Center i criteri vengono utilizzati per definire una singola raccolta di impostazioni per più dispositivi. Ad esempio, l'ambito del criterio dell'applicazione P definito per il gruppo di amministrazione G include i dispositivi gestiti in cui è installata l'applicazione P che sono stati distribuiti nel gruppo G e in tutti i relativi sottogruppi, ad eccezione dei sottogruppi in cui la casella di controllo **Eredita da gruppo padre** è deselezionata nelle proprietà.

Un criterio differisce da qualsiasi impostazione locale in base alle icone di blocco (🔒) accanto alle relative impostazioni. Se un'impostazione (o un gruppo di impostazioni) è bloccata nelle proprietà del criterio, è necessario in primo luogo utilizzare questa impostazione (o gruppo di impostazioni) durante la creazione delle impostazioni da applicare e, in secondo luogo, scrivere le impostazioni o il gruppo di impostazioni nel criterio downstream.

La creazione delle impostazioni da applicare in un dispositivo può essere descritta come segue: i valori di tutte le impostazioni che non sono state bloccate vengono ottenuti dal criterio, quindi sono sovrascritti con i valori delle impostazioni locali. La raccolta risultante viene quindi sovrascritta con i valori delle impostazioni bloccate ottenuti dal criterio.

I criteri della stessa applicazione si influenzano reciprocamente attraverso la gerarchia dei gruppi di amministrazione: le impostazioni bloccate del criterio upstream sovrascrivono le stesse impostazioni del criterio downstream.

Esiste un criterio speciale per gli utenti fuori sede. Questo criterio ha effetto su un dispositivo quando il dispositivo passa in modalità fuori sede. I criteri fuori sede non influiscono sugli altri criteri attraverso la gerarchia dei gruppi di amministrazione.

Profili criterio

L'applicazione dei criteri ai dispositivi solo tramite la gerarchia dei gruppi di amministrazione in molte circostanze può essere poco pratica. Può essere necessario creare più istanze di un singolo criterio con una o due impostazioni differenti per gruppi di amministrazione diversi e sincronizzare i contenuti di questi criteri in futuro.

Per contribuire a evitare tali problemi, Kaspersky Security Center supporta *profili di criteri*. Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo sul dispositivo client (computer o dispositivo mobile). L'attivazione di un profilo determina la modifica delle impostazioni del criterio attivo nel dispositivo prima dell'attivazione del profilo. Tali impostazioni assumono i valori specificati nel profilo.

Attualmente ai profili criterio si applicano le seguenti limitazioni:

- Un criterio può includere al massimo 100 profili.
- Un profilo criterio non può contenere altri profili.
- Un profilo criterio non può contenere impostazioni di notifica.

Contenuto di un profilo

Un profilo criterio contiene i seguenti elementi:

- Nome. I profili con nomi identici si influenzano reciprocamente attraverso la gerarchia dei gruppi di amministrazione con regole comuni.
- Sottoinsieme di impostazioni dei criteri. A differenza del criterio, che contiene tutte le impostazioni, un profilo contiene solo le impostazioni che sono effettivamente richieste (le impostazioni bloccate).
- Condizione di attivazione è un'espressione logica con le proprietà del dispositivo. Un profilo è attivo (integra il criterio) solo quando la condizione di attivazione del profilo diventa vera. In tutti gli altri casi, il profilo è inattivo e viene ignorato. Le seguenti proprietà del dispositivo possono essere incluse nell'espressione logica:
  - Stato della modalità fuori sede.
  - Proprietà dell'ambiente di rete - Nome della regola attiva per la connessione di Network Agent.
  - Presenza o assenza dei tag specificati nel dispositivo.
  - Posizione del dispositivo in un'unità di Active Directory: esplicita (il dispositivo è direttamente nell'unità organizzativa specificata) o implicita (il dispositivo è in un'unità organizzativa che è contenuta nell'unità organizzativa specificata a qualsiasi livello di annidamento).
  - Appartenenza del dispositivo a un gruppo di protezione di Active Directory (esplicita o implicita).
  - Appartenenza del proprietario del dispositivo a un gruppo di protezione di Active Directory (esplicita o implicita).
- Casella di controllo per la disabilitazione del profilo. I profili disabilitati vengono sempre ignorati e le relative condizioni di attivazione non sono verificate.
- Priorità del profilo. Le condizioni di attivazione di differenti profili sono indipendenti, quindi è possibile attivare contemporaneamente più profili. Se i profili attivi contengono raccolte di impostazioni che non si sovrappongono, non si verifica alcun problema. Se invece due profili attivi contengono valori diversi della stessa impostazione, si verifica un'ambiguità. Questa ambiguità deve essere evitata tramite le priorità dei profili: il valore della variabile ambigua viene ottenuto dal profilo che ha la priorità più alta (quello al livello superiore nell'elenco dei profili).

Comportamento dei profili quando i criteri si influenzano reciprocamente attraverso la gerarchia

I profili con lo stesso nome vengono uniti in base alle regole di unione dei criteri. I profili di un criterio upstream hanno una priorità più alta rispetto ai profili di un criterio downstream. Se la modifica delle impostazioni non è consentita nel criterio upstream (è bloccata), il criterio downstream utilizza le condizioni di attivazione del profilo di quello upstream. Se la modifica delle impostazioni è consentita nel criterio upstream, vengono utilizzate le condizioni di attivazione del profilo del criterio downstream.

Poiché un profilo criterio può contenere la proprietà **Il dispositivo è offline** nella relativa condizione di attivazione, i profili sostituiscono completamente la funzionalità dei criteri per gli utenti fuori sede, che non saranno non più supportati.

Un criterio per gli utenti fuori sede può contenere profili, ma questi profili possono essere attivati solo una volta che il dispositivo passa alla modalità fuori sede.

Ereditarietà delle impostazioni dei criteri

Un criterio viene specificato per un gruppo di amministrazione. Le impostazioni dei criteri possono essere *ereditate*, ovvero ricevute nei sottogruppi (gruppi figlio) del gruppo di amministrazione per cui sono state impostate. Da questo momento in poi, un criterio per un gruppo padre viene denominato anche *criterio principale*.

È possibile abilitare o disabilitare due opzioni di ereditarietà: **Eredita impostazioni dal criterio principale** e **Forza ereditarietà impostazioni nei criteri secondari**:

- Se si abilita l'opzione **Eredita impostazioni dal criterio principale** per un criterio secondario e si bloccano alcune impostazioni nel criterio principale, non è possibile modificare queste impostazioni per il gruppo figlio. Tuttavia, è possibile modificare le impostazioni che non sono bloccate nel criterio principale.

- Se si disabilita l'opzione **Eredita impostazioni dal criterio principale** per un criterio secondario, è possibile modificare tutte le impostazioni nel gruppo figlio, anche se alcune impostazioni sono bloccate nel criterio principale.

- Se si abilita **Forza ereditarietà impostazioni nei criteri secondari** nel gruppo padre, viene abilitata l'opzione **Eredita impostazioni dal criterio principale** per tutti i criteri secondari. In questo caso, non è possibile disabilitare questa opzione per nessun criterio secondario. Tutte le impostazioni bloccate nel criterio principale vengono ereditate forzatamente nei gruppi figlio e non è possibile modificare queste impostazioni nei gruppi figlio.

- Nei criteri per il gruppo **Dispositivi gestiti**, l'opzione **Eredita impostazioni dal criterio principale** non influisce su alcuna impostazione, dal momento che il gruppo **Dispositivi gestiti** non dispone di gruppi upstream e non eredita criteri.

Per impostazione predefinita, l'opzione **Eredita impostazioni dal criterio principale** è abilitata per un nuovo criterio.

Se un criterio dispone di profili, tutti i criteri secondari ereditano tali profili.

Gestione dei criteri

Le applicazioni installate nei dispositivi client sono configurate in modo centralizzato attraverso la definizione di criteri.

I criteri creati per le applicazioni in un gruppo di amministrazione sono visualizzati nell'area di lavoro, nella scheda **Criteri**. Prima del nome di ogni criterio viene visualizzata un'icona con il relativo stato.

Quando un criterio viene eliminato o revocato, l'applicazione continua a funzionare con le impostazioni specificate nel criterio. Successivamente tali impostazioni possono essere modificate manualmente.

L'applicazione di un criterio avviene come segue: se un dispositivo esegue attività residenti (attività di protezione in tempo reale), queste continueranno a essere eseguite con i nuovi valori delle impostazioni. Qualsiasi attività periodica avviata (scansione su richiesta, aggiornamento dei database dell'applicazione) continua a essere eseguita senza che i valori siano modificati. Al successivo avvio, verranno eseguite con i nuovi valori delle impostazioni.

I criteri per le applicazioni con supporto multi-tenancy vengono ereditati sia dai gruppi di amministrazione di livello inferiore che da quelli di livello superiore: il criterio viene propagato a tutti i dispositivi client in cui è installata l'applicazione.

Se gli Administration Server sono strutturati gerarchicamente, gli Administration Server secondari ricevono i criteri dall'Administration Server primario e li distribuiscono ai dispositivi client. Se l'ereditarietà è abilitata, le impostazioni dei criteri possono essere modificate nell'Administration Server primario. In seguito, qualsiasi modifica apportata alle impostazioni del criterio viene propagata ai criteri ereditati negli Administration Server secondari.

Se la connessione tra gli Administration Server primari e secondari si interrompe, il criterio nel server secondario continuerà a utilizzare le impostazioni applicate. Le impostazioni dei criteri modificate nell'Administration Server primario vengono distribuite a un Administration Server secondario una volta ristabilita la connessione.

Se l'eredità è disabilitata, le impostazioni dei criteri possono essere modificate in un Administration Server secondario indipendentemente dall'Administration Server primario.

Se la connessione tra un Administration Server e un dispositivo client si interrompe, il dispositivo client inizia a utilizzare il criterio fuori sede (se è stato definito) o il criterio continua a utilizzare le impostazioni applicate finché non viene ristabilita la connessione.

I risultati della distribuzione dei criteri all'Administration Server secondario sono visualizzati nella finestra delle proprietà del criterio della console nell'Administration Server primario.

I risultati della distribuzione dei criteri ai dispositivi client sono visualizzati nella finestra delle proprietà dei criteri dell'Administration Server a cui sono connessi.

Non utilizzare dati privati nelle impostazioni del criterio. Ad esempio, non specificare la password dell'amministratore del dominio.

Creazione di un criterio

In Administration Console è possibile creare i criteri direttamente nella cartella del gruppo di amministrazione per cui è necessario creare un criterio o nell'area di lavoro della cartella **Criteri**.

Per creare un criterio nella cartella di un gruppo di amministrazione:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui si desidera creare un criterio.
2. Nell'area di lavoro del gruppo selezionare la scheda **Criteri**.
3. Eseguire la Creazione guidata nuovo criterio facendo clic sul pulsante **Nuovo criterio**.

   Verrà avviata la Creazione guidata nuovo criterio. Seguire le istruzioni della procedura guidata.

*Per creare un criterio nell'area di lavoro della cartella **Criteri**:*

1. Nella struttura della console selezionare la cartella **Criteri**.
2. Eseguire la Creazione guidata nuovo criterio facendo clic sul pulsante **Nuovo criterio**.

Verrà avviata la Creazione guidata nuovo criterio. Seguire le istruzioni della procedura guidata.

È possibile creare diversi criteri per un'applicazione di un gruppo, ma può essere attivo un solo criterio alla volta. Quando si crea un nuovo criterio attivo, il criterio attivo precedente diventa inattivo.

Quando si crea un criterio, è possibile specificare un set minimo di parametri necessari per il corretto funzionamento dell'applicazione. Per tutti gli altri valori vengono utilizzati i valori predefiniti applicati durante l'installazione locale dell'applicazione. Dopo avere creato il criterio, è possibile modificarlo.

Non utilizzare dati privati nelle impostazioni del criterio. Ad esempio, non specificare la password dell'amministratore del dominio.

Le impostazioni delle applicazioni Kaspersky modificate in seguito all'applicazione dei criteri sono descritte in dettaglio nelle rispettive Guide.

Dopo la creazione del criterio, le impostazioni per cui non è consentita la modifica (contrassegnate con l'icona del lucchetto ( )) diventano effettive nei dispositivi client indipendentemente dalle impostazioni precedentemente specificate per l'applicazione.

Visualizzazione dei criteri ereditati in un sottogruppo

Per abilitare la visualizzazione dei criteri ereditati per un gruppo di amministrazione nidificato:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui visualizzare i criteri ereditati.
2. Nell'area di lavoro del gruppo selezionato selezionare la scheda **Criteri**.
3. Nel menu di scelta rapida dell'elenco dei criteri selezionare **Visualizza** → **Criteri ereditati**.

I criteri ereditati verranno visualizzati nell'elenco dei criteri con la seguente icona:

- – Se sono stati ereditati da un gruppo creato nell'Administration Server primario.
- – Se sono stati ereditati da un gruppo di livello superiore.

Se è abilitata la modalità di ereditarietà delle impostazioni, i criteri ereditati sono disponibili per la modifica solo nel gruppo in cui sono stati creati. La modifica dei criteri ereditati non è disponibile nel gruppo che li eredita.

Attivazione di un criterio

Per rendere attivo un criterio per il gruppo selezionato:

1. Nell'area di lavoro del gruppo, nella scheda **Criteri**, selezionare il criterio da rendere attivo.
2. Per attivare il criterio, eseguire una delle seguenti azioni:
   - Nel menu di scelta rapida del criterio selezionare **Criterio attivo**.
   - Nella finestra delle proprietà del criterio aprire la sezione **Generale**, quindi selezionare **Criterio attivo** dal gruppo di impostazioni **Stato criterio**.

Il criterio diventerà attivo per il gruppo di amministrazione selezionato.

Quando un criterio è applicato a un numero elevato di dispositivi client, il carico di Administration Server e il traffico di rete aumentano significativamente per un certo periodo di tempo.

Attivazione automatica di un criterio quando si verifica un evento Epidemia di virus

Per attivare automaticamente un criterio quando si verifica un evento Epidemia di virus:

1. Nella finestra delle proprietà di Administration Server aprire la sezione **Epidemia di virus**.
2. Aprire la finestra **Attivazione dei criteri** facendo clic sul collegamento **Configura i criteri da attivare se si verifica un evento di epidemia di virus**, quindi aggiungere il criterio all'elenco selezionato dei criteri attivati quando viene rilevata un'epidemia di virus.

   Se un criterio è stato attivato per l'evento *Epidemia di virus*, è possibile ripristinare il criterio precedente solo utilizzando la modalità manuale.

Applicazione di un criterio fuori sede

Il criterio fuori sede viene applicato a un dispositivo se questo viene disconnesso dalla rete aziendale.

Per applicare un criterio fuori sede:

Nella finestra delle proprietà del criterio aprire la sezione **Generale** e nel gruppo di impostazioni **Stato criterio** selezionare **Criterio fuori sede**.

Il criterio fuori sede verrà applicato ai dispositivi se vengono disconnessi dalla rete aziendale.

Modifica di un criterio. Rollback delle modifiche

Per modificare un criterio:

1. Nella struttura della console selezionare la cartella **Criteri**.
2. Nell'area di lavoro della cartella **Criteri** selezionare un criterio e passare alla finestra delle proprietà del criterio utilizzando il menu di scelta rapida.
3. Apportare le modifiche desiderate.
4. Fare clic su **Applica**.

Le modifiche apportate al criterio saranno salvate nelle proprietà del criterio, nella sezione **Cronologia revisioni**.

È possibile eseguire il rollback delle modifiche apportate al criterio, se necessario.

Per eseguire il rollback delle modifiche apportate al criterio:

1. Nella struttura della console selezionare la cartella **Criteri**.
2. Selezionare il criterio in cui è necessario eseguire il rollback delle modifiche e aprire la finestra delle proprietà del criterio utilizzando il menu di scelta rapida.
3. Nella finestra delle proprietà del criterio selezionare la sezione **Cronologia revisioni**.
4. Nell'elenco delle revisioni del criterio selezionare il numero della revisione a cui eseguire il rollback delle modifiche.
5. Fare clic sul pulsante **Avanzate** e selezionare il valore **Rollback** nell'elenco a discesa.

Confronto dei criteri

È possibile confrontare due criteri per una singola applicazione gestita. Dopo il confronto, è visualizzato un rapporto che indica quali impostazioni dei criteri corrispondono e quali sono diverse. Potrebbe ad esempio essere necessario confrontare i criteri se diversi amministratori hanno creato nelle rispettive sedi più criteri per una singola applicazione gestita oppure se un singolo criterio di primo livello è stato ereditato da tutte le sedi locali e modificato per ciascuna sede. È possibile confrontare i criteri in uno dei seguenti modi: selezionando un criterio e confrontandolo con un altro o confrontando una coppia di criteri dall'elenco dei criteri.

È possibile confrontare solo i criteri con revisioni correnti nella cronologia delle revisioni.

Per confrontare un criterio con un altro:

1. Nella struttura della console selezionare la cartella **Criteri**.
2. Nell'area di lavoro della cartella **Criteri** selezionare il criterio che è necessario confrontare con un altro.
3. Dal menu di scelta rapida del criterio selezionare **Confronta il criterio con un altro criterio**.

4. Nella finestra **Seleziona criterio** selezionare il criterio con cui confrontare il criterio.

5. Fare clic su **OK**.

Per il confronto tra i due criteri per la stessa applicazione viene visualizzato un rapporto in formato HTML.

Per confrontare una coppia di criteri dall'elenco dei criteri:

1. Nella cartella **Criteri**, nell'elenco dei criteri, utilizzare il tasto **MAIUSC** o **CTRL** per selezionare due criteri per una singola applicazione gestita.

2. Nel menu di scelta rapida selezionare **Confronta**.

Per il confronto tra i due criteri per la stessa applicazione viene visualizzato un rapporto in formato HTML.

Il rapporto sul confronto delle impostazioni dei criteri per Kaspersky Endpoint Security for Windows fornisce anche informazioni sul confronto dei profili criterio. È possibile comprimere i risultati del confronto dei profili criterio. Per comprimere la sezione, fare clic sull'icona della freccia ( ) accanto al nome della sezione.

Visualizzazione del grafico dello stato di distribuzione dei criteri

In Kaspersky Security Center, è possibile visualizzare i risultati dell'applicazione dei criteri in ogni dispositivo.

Per visualizzare lo stato di distribuzione dei criteri in ogni dispositivo:

1. Nell'area di lavoro del gruppo, nella scheda **Criteri**, selezionare il criterio di cui si desidera visualizzare lo stato di distribuzione.

   Il grafico nel riquadro di destra mostra una panoramica dell'applicazione dei criteri.

2. Fare clic su **Dettagli**.

   Verrà visualizzata la finestra **Risultati dell'applicazione dei criteri**.

   È possibile esportare i risultati dell'applicazione dei criteri in un file CSV o TXT.

Eliminazione di un criterio

Per eliminare un criterio:

1. Nell'area di lavoro di un gruppo di amministrazione, nella scheda **Criteri**, selezionare il criterio da eliminare.

2. Eliminare il criterio in uno dei seguenti modi:

   - Selezionando **Elimina** nel menu di scelta rapida del criterio.

   - Facendo clic sul collegamento **Elimina criterio** nella finestra di informazioni per il criterio selezionato.

Copia di un criterio

Per copiare un criterio:

1. Nell'area di lavoro del gruppo desiderato, nella scheda **Criteri**, selezionare un criterio.
2. Nel menu di scelta rapida del criterio selezionare **Copia**.
3. Nella struttura della console selezionare un gruppo a cui si desidera aggiungere il criterio.

   È possibile aggiungere un criterio al gruppo da cui è stato copiato.
4. Dal menu di scelta rapida dell'elenco dei criteri per il gruppo selezionato, nella scheda **Criteri** selezionare **Incolla**.

Il criterio verrà copiato con tutte le relative impostazioni e sarà applicato ai dispositivi del gruppo in cui è stato copiato. Se si incolla il criterio nello stesso gruppo da cui è stato copiato, al nome del criterio viene aggiunto automaticamente l'indice **(<numero progressivo successivo>)**, ad esempio **(1)**, **(2)**.

Un criterio attivo diventa inattivo durante la copia. Se necessario, è possibile renderlo attivo.

Esportazione di un criterio

Per esportare un criterio:

1. Esportare un criterio in uno dei seguenti modi:
   - Selezionando **Tutte le attività** → **Esporta** nel menu di scelta rapida del criterio.
   - Facendo clic sul collegamento **Esporta criterio in un file** nella finestra di informazioni del criterio selezionato.
2. Nella finestra **Salva con nome** visualizzata specificare il percorso e il nome del file del criterio. Fare clic sul pulsante **Salva**.

Importazione di un criterio

Per importare un criterio:

1. Nell'area di lavoro del gruppo desiderato, nella scheda **Criteri**, selezionare uno dei seguenti modi per l'importazione dei criteri:
   - Selezionando **Tutte le attività** → **Importa** nel menu di scelta rapida dell'elenco dei criteri.
   - Facendo clic sul pulsante **Importa criteri da file** nella sezione di gestione per l'elenco dei criteri.
2. Nella finestra visualizzata specificare il percorso del file da cui si desidera importare un criterio. Fare clic sul pulsante **Apri**.

Il criterio importato viene visualizzato nell'elenco dei criteri. Vengono importati anche le impostazioni e i profili del criterio. Indipendentemente dallo stato del criterio selezionato durante l'esportazione, il criterio importato è inattivo. È possibile modificare lo stato del criterio nelle proprietà del criterio.

Se il criterio appena importato ha un nome identico a quello di un criterio esistente, il nome del criterio importato viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Conversione di criteri

Kaspersky Security Center è in grado di convertire i criteri delle versioni precedenti delle applicazioni Kaspersky gestite in versioni aggiornate delle stesse applicazioni. I criteri convertiti mantengono le impostazioni dell'amministratore corrente specificate prima dell'aggiornamento, oltre a includere nuove impostazioni dalle versioni aggiornate delle applicazioni. Se un criterio viene convertito in una versione aggiornata di un'applicazione Kaspersky gestita, non è possibile aprire il criterio in un Administration Server in cui è installata una versione precedente del plug-in dell'applicazione. I plug-in di gestione per le applicazioni Kaspersky determinano se la conversione è disponibile per i criteri di queste applicazioni. Per informazioni sulla conversione dei criteri di ciascuna applicazione Kaspersky supportata, fare riferimento alla relativa Guida nel seguente elenco:

- **Applicazioni Kaspersky per workstation:**
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Linux Elbrus Edition
  - Kaspersky Endpoint Security for Mac
  - Kaspersky Endpoint Agent
  - Kaspersky Embedded Systems Security for Windows
- **Kaspersky Industrial CyberSecurity:**
  - Kaspersky Industrial CyberSecurity for Nodes
  - Kaspersky Industrial CyberSecurity for Linux Nodes
  - Kaspersky Industrial CyberSecurity for Networks (la distribuzione centralizzata non è supportata)
- **Applicazioni Kaspersky per dispositivi mobili:**
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS
- **Applicazioni Kaspersky per file server:**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux

- **Applicazioni Kaspersky per macchine virtuali:**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless
- **Applicazioni Kaspersky per sistemi di posta e server SharePoint/di collaborazione**:
  - Kaspersky Security for Linux Mail Server
  - Kaspersky Security for Microsoft Exchange Servers
- **Applicazioni Kaspersky per il rilevamento di attacchi mirati:**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **Applicazioni Kaspersky per dispositivi KasperskyOS:**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (plug-in per Kaspersky Thin Client)

Per convertire i criteri:

1. Nella struttura della console selezionare un Administration Server per cui si desidera convertire i criteri.
2. Nel menu di scelta rapida di Administration Server selezionare **Tutte le attività → Conversione guidata in batch criteri e attività**.

   Verrà avviata la Conversione guidata criteri e attività. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, vengono creati nuovi criteri che utilizzano le impostazioni dei criteri dell'amministratore corrente e le nuove impostazioni delle versioni aggiornate delle applicazioni Kaspersky.

Gestione dei profili criterio

Profilo criterio è una raccolta denominata di impostazioni di un criterio attivato in un dispositivo client (computer o dispositivo mobile) quando il dispositivo soddisfa determinate regole di attivazione. L'attivazione di un profilo determina la modifica delle impostazioni del criterio attivo nel dispositivo prima dell'attivazione del profilo. Tali impostazioni assumono i valori specificati nel profilo.

I profili criterio sono necessari per consentire l'esecuzione dei dispositivi all'interno di un unico gruppo di amministrazione con diverse impostazioni del criterio. Ad esempio, può verificarsi una situazione in cui le impostazioni del criterio devono essere modificate per alcuni dispositivi in un gruppo di amministrazione. In questo caso, è possibile configurare profili criterio per tale criterio, in modo da poter modificare le impostazioni del criterio per determinati dispositivi nel gruppo di amministrazione. Il criterio vieta ad esempio l'esecuzione di un software di navigazione GPS in tutti i dispositivi nel gruppo di amministrazione Utenti. Il software di navigazione GPS è necessario in un solo dispositivo nel gruppo di amministrazione Utenti: quello di proprietà dell'utente che ha il ruolo di corriere. È possibile contrassegnare tale dispositivo semplicemente come "Corriere" e riconfigurare il profilo criterio in modo da consentire l'esecuzione del software di navigazione GPS solo nel dispositivo contrassegnato come "Corriere", mantenendo tutte le altre impostazioni del criterio. In questo caso, se un dispositivo contrassegnato come "Corriere" viene visualizzato nel gruppo di amministrazione Utenti, questo sarà autorizzato a eseguire il software di navigazione GPS. L'esecuzione del software di navigazione GPS continuerà a essere vietata negli altri dispositivi del gruppo di amministrazione Utenti, a meno che anche questi non siano contrassegnati come "Corriere".

I profili sono supportati solo dai seguenti criteri:

- Criteri di Kaspersky Endpoint Security for Windows
- Criteri di Kaspersky Endpoint Security for Mac
- Criteri del plug-in di Kaspersky Mobile Device Management dalla versione 10 Service Pack 1 alla versione 10 Service Pack 3 Maintenance Release 1
- Criteri del plug-in di Kaspersky Device Management for iOS
- Criteri di Kaspersky Security for Virtualization 5.1 Light Agent for Windows
- Criteri di Kaspersky Security for Virtualization 5.1 Light Agent for Linux

I profili criterio semplificano la gestione dei dispositivi client a cui si applicano i criteri:

- Le impostazioni del profilo criterio possono differire dalle impostazioni del criterio.
- Non è necessario gestire e applicare manualmente più istanze di un singolo criterio che variano solo per qualche impostazione.
- Non è necessario allocare un criterio distinto per gli utenti fuori sede.
- È possibile esportare e importare i profili criterio, nonché creare nuovi profili criterio in base a quelli esistenti.
- Un singolo criterio può avere più profili criterio attivi. Solo i profili che soddisfano le regole di attivazione valide nel dispositivo saranno applicati a tale dispositivo.
- I profili sono soggetti alla gerarchia dei criteri. Un criterio ereditato include tutti i profili del criterio di livello più elevato.

Priorità dei profili

I profili creati per un criterio vengono disposti in ordine di priorità decrescente. Ad esempio, se il profilo X si trova più in alto nell'elenco dei profili rispetto al profilo Y, avrà una priorità più alta rispetto a quest'ultimo. A un unico dispositivo possono essere applicati contemporaneamente diversi profili. Se i valori di un'impostazione differiscono in diversi profili, il valore del profilo con priorità più elevata verrà applicato nel dispositivo.

Regole per l'attivazione del profilo

Un profilo criterio viene attivato in un dispositivo client quando viene eseguita una regola di attivazione. Le *regole di attivazione* sono set di condizioni che, se soddisfatte, avviano il profilo criterio in un dispositivo. Una regola di attivazione può contenere le seguenti condizioni:

- Network Agent in un dispositivo client si connette all'Administration Server con un determinato set di impostazioni di connessione, ad esempio indirizzo dell'Administration Server, numero di porta e così via.
- Il dispositivo client è offline.
- Al dispositivo client sono stati assegnati determinati tag.
- Il dispositivo client è collocato in modo esplicito (il dispositivo viene immediatamente collocato nell'unità specificata) o implicito (il dispositivo è collocato in un'unità che si trova nell'unità specificata a qualsiasi livello di annidamento) in un'unità specifica di Active Directory®, il dispositivo o il relativo proprietario si trova in un gruppo di protezione di Active Directory.
- Il dispositivo client appartiene a un determinato proprietario o il proprietario del dispositivo fa parte di un gruppo di protezione interno di Kaspersky Security Center.
- Al proprietario del dispositivo client è stato assegnato un ruolo specificato.

Criteri nella gerarchia dei gruppi di amministrazione

Se si crea un criterio in un gruppo di amministrazione di basso livello, il nuovo criterio eredita tutti i profili del criterio attivo dal gruppo di livello superiore. I profili con nomi identici vengono uniti. I profili criterio per il gruppo di livello superiore hanno una priorità più elevata. Nel gruppo di amministrazione *A*, ad esempio, il criterio *P(A)* dispone dei profili *X1*, *X2* e *X3* (in ordine di priorità decrescente). Nel gruppo di amministrazione *B*, che è un sottogruppo del gruppo *A*, il criterio *P(B)* è stato creato con i profili *X2*, *X4*, *X5*. Il criterio *P(B)* verrà quindi modificato con il criterio *P(A)* affinché l'elenco dei profili nel criterio *P(B)* venga visualizzato nel modo seguente: *X1*, *X2*, *X3*, *X4*, *X5* (in ordine di priorità decrescente). La priorità del profilo *X2* dipenderà dallo stato iniziale del profilo *X2* del criterio *P(B)* e dal profilo *X2* del criterio *P(A)*. Dopo la creazione del criterio *P(B)*, il criterio *P(A)* non verrà più visualizzato nel sottogruppo *B*.

Il criterio attivo viene ricalcolato ogni volta che si avvia Network Agent, si abilita o disabilita la modalità offline o si modifica l'elenco dei tag assegnati al dispositivo client. Ad esempio, le dimensioni della RAM sono state aumentate nel dispositivo che, a sua volta, ha attivato il profilo criterio applicato nei dispositivi con una RAM di grandi dimensioni.

Proprietà e limitazioni dei profili criterio

I profili dispongono delle seguenti proprietà:

- I profili di un criterio inattivo non hanno impatto sui dispositivi client.
- Se un criterio è impostato sullo stato **Criterio fuori sede**, anche i profili del criterio verranno applicati quando un dispositivo viene disconnesso dalla rete aziendale.
- I profili non supportano l'analisi statica dell'accesso ai file eseguibili.
- Un profilo criterio non può contenere impostazioni delle notifiche degli eventi.

- Se la porta UDP 15000 viene utilizzata per la connessione di un dispositivo ad Administration Server, il profilo criterio corrispondente viene attivato entro un minuto dall'assegnazione di un tag al dispositivo.
- È possibile utilizzare le regole per la connessione di Network Agent ad Administration Server quando si creano le regole di attivazione del profilo criterio.

Creazione di un profilo criterio

La creazione del profilo è disponibile solo per i criteri delle seguenti applicazioni:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows e versioni successive
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Plug-in di Kaspersky Mobile Device Management dalla versione 10 Service Pack 1 alla versione 10 Service Pack 3 Maintenance Release 1
- Plug-in di Kaspersky Device Management for iOS
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows and Linux

Per creare un profilo criterio:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui si desidera creare un profilo criterio.
2. Nell'area di lavoro del gruppo di amministrazione selezionare la scheda **Criteri**.
3. Selezionare un criterio e passare alla finestra delle proprietà del criterio utilizzando il menu di scelta rapida.
4. Aprire la sezione **Profili criterio** nella finestra delle proprietà del criterio e fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuovo profilo criterio.
5. Nella finestra **Nome profilo criterio** della procedura guidata specificare quanto segue:

   a. Nome del profilo criterio

      Il nome del profilo non può contenere più di 100 caratteri.

   b. Stato del profilo criterio (*Abilitato* o *Disabilitato*)

      È consigliabile creare e abilitare i profili criterio inattivi solo dopo aver completato la definizione delle impostazioni e delle condizioni di attivazione del profilo criterio.
6. Selezionare la casella di controllo **Dopo aver chiuso la creazione guidata nuovo profilo criterio, passa alla configurazione della regola di attivazione del profilo criterio** per avviare la Creazione guidata nuova regola di attivazione di un profilo criterio. Seguire i passaggi della procedura guidata.
7. Modificare le impostazioni del profilo criterio nella finestra delle proprietà del profilo criterio, in base alle esigenze.
8. Salvare le modifiche facendo clic su **OK**.

   Il profilo verrà salvato. Il profilo verrà attivato nei dispositivi che soddisfano le regole di attivazione.

È possibile creare più profili per un singolo criterio. I profili creati per un criterio vengono visualizzati nelle proprietà del criterio nella sezione **Profili criterio**. È possibile modificare un profilo criterio, modificare la priorità del profilo o rimuovere il profilo.

Modifica di un profilo criterio

Modifica delle impostazioni di un profilo criterio

La possibilità di modificare un profilo criterio è disponibile solo per i criteri di Kaspersky Endpoint Security for Windows.

Per modificare un profilo criterio:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui è necessario modificare il profilo criterio.
2. Nell'area di lavoro del gruppo selezionare la scheda **Criteri**.
3. Selezionare un criterio e passare alla finestra delle proprietà del criterio utilizzando il menu di scelta rapida.
4. Aprire la sezione **Profili criterio** nelle proprietà del criterio.

   Questa sezione contiene un elenco dei profili creati per il criterio. I profili vengono visualizzati nell'elenco in base alle relative priorità.
5. Selezionare un profilo criterio, quindi fare clic sul pulsante **Proprietà**.
6. Configurare il profilo nella finestra delle proprietà:
   - Se necessario, nella sezione **Generale** modificare il nome del profilo e abilitare o disabilitare il profilo utilizzando la casella di controllo **Abilita profilo**.
   - Nella sezione **Regole di attivazione** modificare le regole di attivazione del profilo.
   - Modificare le impostazioni del criterio nelle sezioni corrispondenti.
7. Fare clic su **OK**.

Le impostazioni modificate diventeranno effettive dopo la sincronizzazione del dispositivo con Administration Server (se il profilo criterio è attivo) o dopo l'esecuzione di una regola di attivazione (se il profilo criterio è inattivo).

Modifica della priorità di un profilo criterio

Le priorità dei profili criterio definiscono l'ordine di attivazione dei profili in un dispositivo client. Le priorità vengono utilizzate se sono impostate regole di attivazione identiche per profili criterio differenti.

Ad esempio, sono stati creati due profili criterio: *Profilo 1* e *Profilo 2* che differiscono per i rispettivi valori di un'unica impostazione (*Valore 1* e *Valore 2*). La priorità del *Profilo 1* è più elevata di quella del *Profilo 2*. Sono inoltre disponibili profili con priorità meno elevate di quella del *Profilo 2*. Le regole di attivazione per tali profili sono identiche.

Quando si attiva una regola di attivazione, verrà attivato il *Profilo 1*. L'impostazione nel dispositivo avrà il *Valore 1*. Se si rimuove il *Profilo 1*, il *Profilo 2* avrà la priorità più elevata, pertanto l'impostazione avrà il *Valore 2*.

Nell'elenco dei profili criterio i profili sono visualizzati in base alle rispettive priorità. Il profilo con la priorità più elevata viene posizionato per primo. È possibile modificare la priorità di un profilo utilizzando i pulsanti della freccia verso l'alto  e della freccia verso il basso  .

Eliminazione di un profilo criterio

Per eliminare un profilo criterio:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui si desidera eliminare il profilo criterio.
2. Nell'area di lavoro del gruppo di amministrazione selezionare la scheda **Criteri**.
3. Selezionare un criterio e passare alla finestra delle proprietà del criterio utilizzando il menu di scelta rapida.
4. Aprire la sezione **Profili criterio** nelle proprietà del criterio di Kaspersky Endpoint Security.
5. Selezionare il profilo criterio che si desidera eliminare e fare clic sul pulsante **Elimina**.

Il profilo criterio verrà eliminato. Lo stato attivo passerà a un altro profilo criterio per cui vengono attivate le regole di attivazione nel dispositivo client o al criterio.

Creazione di una regola di attivazione del profilo criterio

Per creare una regola di attivazione per un profilo criterio:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui è necessario creare una regola di attivazione per un profilo criterio.
2. Nell'area di lavoro del gruppo selezionare la scheda **Criteri**.
3. Selezionare un criterio e passare alla finestra delle proprietà del criterio utilizzando il menu di scelta rapida.
4. Selezionare la sezione **Profili criterio** nella finestra delle proprietà del criterio.
5. Selezionare il profilo criterio per cui è necessario creare una regola di attivazione, quindi fare clic sul pulsante **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del profilo criterio.

   Se l'elenco dei profili criterio è vuoto, è possibile creare un profilo criterio.
6. Selezionare la sezione **Regole di attivazione** e fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova regola di attivazione di un profilo criterio.

7. Nella finestra **Regole di attivazione del profilo criterio** selezionare le caselle di controllo accanto alle condizioni che devono determinare l'attivazione del profilo criterio che si sta creando:

- **Regole generali per l'attivazione del profilo criterio**

  Selezionare questa casella di controllo per configurare le regole di attivazione del profilo criterio nel dispositivo in base allo stato della modalità offline del dispositivo, alla regola per la connessione ad Administration Server e ai tag assegnati al dispositivo.

- **Regole per l'utilizzo di Active Directory**

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base alla presenza del dispositivo in un'unità organizzativa di Active Directory o all'appartenenza del dispositivo (o del proprietario) a un gruppo di protezione di Active Directory.

- **Regole per il proprietario di un dispositivo specifico**

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base al proprietario del dispositivo.

- **Regole per le specifiche hardware**

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base al volume della memoria e al numero di processori logici.

Il numero delle pagine aggiuntive della procedura guidata dipende dalle impostazioni selezionate nel primo passaggio. È possibile modificare le regole di attivazione del profilo criterio in un secondo momento.

8. Nella finestra **Condizioni generali** specificare le seguenti impostazioni:

- Nel campo **Il dispositivo è offline** specificare nell'elenco a discesa la condizione per la presenza di un dispositivo nella rete:
  - **Sì**

    Il dispositivo si trova in una rete esterna, pertanto l'Administration Server non è disponibile.
  - **No**

    Il dispositivo è presente nella rete, pertanto Administration Server è disponibile.
  - **Nessun valore selezionato**

    Il criterio non verrà applicato.
- Nella casella **Il dispositivo si trova nel percorso di rete specificato** utilizzare gli elenchi a discesa per configurare l'attivazione dei profili criterio se la regola di connessione di Administration Server viene eseguita/non eseguita nel dispositivo:
  - **Eseguita / Non eseguita**

    Condizione di attivazione del profilo criterio (se la regola viene eseguita o meno).
  - **Nome regola**

    Descrizione del percorso di rete del dispositivo per la connessione ad Administration Server, le cui condizioni devono essere soddisfatte (o non devono essere soddisfatte) per l'attivazione del profilo criterio.

    È possibile creare o configurare una descrizione del percorso di rete dei dispositivi per la connessione a un Administration Server in una regola per il passaggio di Network Agent.

La finestra **Condizioni generali** viene visualizzata se è selezionata la casella di controllo **Regole generali per l'attivazione del profilo criterio**.

9. Nella finestra **Condizioni basate sui tag** specificare le seguenti impostazioni:

- **Elenco di tag**

  Nell'elenco di tag specificare una regola per l'inclusione dei dispositivi nel profilo criterio selezionando le caselle di controllo accanto ai tag appropriati.

  È possibile aggiungere nuovi tag all'elenco immettendoli nel campo sopra l'elenco e facendo clic sul pulsante **Aggiungi**.

  Il profilo criterio include i dispositivi con descrizioni che contengono tutti i tag selezionati. Se le caselle di controllo sono deselezionate, il criterio non viene applicato. Per impostazione predefinita, queste caselle di controllo sono deselezionate.

- **Applica ai dispositivi senza i tag specificati**

  Abilitare questa opzione se è necessario invertire la selezione di tag.

  Se questa opzione è abilitata, il profilo criterio include i dispositivi con descrizioni che non contengono alcuno dei tag selezionati. Se questa opzione è disabilitata, il criterio non viene applicato.

  Per impostazione predefinita, questa opzione è disabilitata.

La finestra **Condizioni basate sui tag** viene visualizzata se la casella di controllo **Regole generali per l'attivazione del profilo criterio** è selezionata.

10. Nella finestra **Condizioni basate su Active Directory** specificare le seguenti impostazioni:

- **Appartenenza del proprietario del dispositivo al gruppo di protezione di Active Directory**

  Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo il cui proprietario appartiene al gruppo di protezione specificato. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Appartenenza del dispositivo al gruppo di protezione di Active Directory**

  Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Allocazione del dispositivo nell'unità organizzativa di Active Directory**

  Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo incluso nell'unità organizzativa di Active Directory specificata. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato.

  Per impostazione predefinita, questa opzione è disabilitata.

La finestra **Condizioni basate su Active Directory** viene visualizzata se è selezionata la casella di controllo **Regole per l'utilizzo di Active Directory**.

11. Nella finestra **Condizioni basate sul proprietario del dispositivo** specificare le seguenti impostazioni:

- **Proprietario dispositivo**

  Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al proprietario. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

  - Il dispositivo appartiene al proprietario specificato (segno "=").
  - Il dispositivo non appartiene al proprietario specificato (segno "#").

    Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il proprietario dispositivo quando l'opzione è abilitata. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Il proprietario del dispositivo fa parte di un gruppo di protezione interno**

  Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base all'appartenenza del proprietario a un gruppo di protezione interno di Kaspersky Security Center. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

  - Il proprietario dispositivo è un membro del gruppo di protezione specificato (segno "=").
  - Il proprietario dispositivo non è un membro del gruppo di protezione specificato (segno "#").

    Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare un gruppo di protezione di Kaspersky Security Center. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Attiva il profilo criterio in base allo specifico ruolo del proprietario del dispositivo**

  Selezionare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo a seconda del ruolo del proprietario. Aggiungere manualmente il ruolo dall'elenco dei ruoli esistenti.

  Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato.

La finestra **Condizioni basate sul proprietario del dispositivo** viene visualizzata se è selezionata la casella di controllo **Regole per il proprietario di un dispositivo specifico**.

12. Nella finestra **Condizioni basate sulle specifiche delle apparecchiature** specificare le seguenti impostazioni:

- **Dimensione RAM (MB)**

  Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al volume della RAM disponibile in tale dispositivo. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

  - Le dimensioni della RAM del dispositivo sono inferiori al valore specificato (segno "<").
  - Le dimensioni della RAM del dispositivo sono superiori al valore specificato (segno ">").

  Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il volume della RAM nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Numero di processori logici**

  Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al numero di processori logici nel dispositivo. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

  - Il numero di processori logici nel dispositivo è inferiore o uguale al valore specificato (segno "<").
  - Il numero di processori logici nel dispositivo è superiore o uguale al valore specificato (segno ">").

  Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il numero di processori logici nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

La finestra **Condizioni basate sulle specifiche delle apparecchiature** viene visualizzata se è selezionata la casella di controllo **Regole per le specifiche hardware**.

13. Nella finestra **Nome della regola di attivazione del profilo criterio**, nel campo **Nome regola**, specificare un nome per la regola.

Il profilo verrà salvato. Il profilo sarà attivato nel dispositivo quando vengono attivate le regole di attivazione.

Le regole di attivazione del profilo criterio create per il profilo sono visualizzate nelle proprietà del profilo criterio nella sezione **Regole di attivazione**. È possibile modificare o rimuovere qualsiasi regola di attivazione del profilo criterio.

È possibile attivare contemporaneamente più regole di attivazione.

Regole di spostamento dei dispositivi

È consigliabile automatizzare l'allocazione dei dispositivi ai gruppi di amministrazione utilizzando le *regole di spostamento dei dispositivi*. Una regola di spostamento dei dispositivi comprende tre elementi principali: nome, condizione di esecuzione (un'espressione logica con gli attributi del dispositivo) e gruppo di amministrazione di destinazione. Una regola sposta un dispositivo nel gruppo di amministrazione di destinazione se gli attributi del dispositivo soddisfano la condizione di esecuzione della regola.

Tutte le regole di spostamento dei dispositivi hanno priorità. L'Administration Server verifica se gli attributi del dispositivo soddisfano la condizione di esecuzione di ogni regola, in ordine di priorità crescente. Se gli attributi del dispositivo soddisfano la condizione di esecuzione di una regola, il dispositivo viene spostato nel gruppo di destinazione, quindi l'elaborazione della regola è completa per questo dispositivo. Se gli attributi del dispositivo soddisfano le condizioni di più regole, il dispositivo viene spostato nel gruppo di destinazione della regola con la priorità più alta (al livello più alto nell'elenco delle regole).

Le regole di spostamento dei dispositivi possono essere create implicitamente. Ad esempio, nelle proprietà di un pacchetto di installazione o di un'attività di installazione remota è possibile specificare il gruppo di amministrazione in cui deve essere spostato il dispositivo dopo l'installazione di Network Agent. Inoltre, le regole di spostamento dei dispositivi possono essere create esplicitamente dall'amministratore di Kaspersky Security Center nell'elenco delle regole di spostamento. L'elenco è disponibile in Administration Console, nelle proprietà del gruppo **Dispositivi non assegnati**.

Per impostazione predefinita, una regola di spostamento dei dispositivi viene utilizzata per l'allocazione iniziale una tantum dei dispositivi ai gruppi di amministrazione. La regola sposta i dispositivi dal gruppo **Dispositivi non assegnati** una sola volta. Se in precedenza un dispositivo era stato spostato da questa regola, la regola non lo sposterà di nuovo, anche se si reinserisce manualmente il dispositivo nel gruppo **Dispositivi non assegnati**. Questo è il modo consigliato per applicare le regole di spostamento.

È possibile spostare i dispositivi che sono già stati assegnati ad alcuni gruppi di amministrazione. A tale scopo, nelle proprietà di una regola deselezionare la casella di controllo **Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione**.

L'applicazione delle regole di spostamento a dispositivi che sono già stati assegnati ad alcuni gruppi di amministrazione aumenta considerevolmente il carico sull'Administration Server.

La casella di controllo **Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione** è bloccata nelle proprietà delle regole di spostamento create automaticamente. Tali regole vengono create quando si aggiunge l'attività *Installa applicazione in remoto* o si crea un pacchetto di installazione indipendente.

È possibile creare una regola di spostamento da applicare ripetutamente a un singolo dispositivo.

È consigliabile evitare di spostare ripetutamente un singolo dispositivo da un gruppo all'altro (ad esempio, per applicare uno speciale criterio al dispositivo, eseguire una speciale attività di gruppo o aggiornare il dispositivo attraverso un punto di distribuzione specifico).

Tali scenari non sono supportati, perché comportano un notevole aumento del carico su Administration Server e del traffico di rete. Questi scenari anche sono in conflitto con i principi operativi di Kaspersky Security Center (in particolare nell'area di diritti di accesso, eventi e rapporti). Un'altra soluzione deve ad esempio essere trovata attraverso l'utilizzo di profili criterio, attività per selezioni dispositivi, l'assegnazione di Network Agent in base allo scenario standard.

Clonazione delle regole di spostamento dei dispositivi

Quando è necessario creare più regole di spostamento dei dispositivi con impostazioni simili, è possibile clonare una regola esistente e quindi modificare le impostazioni della regola clonata. Ad esempio, questo è utile quando è necessario disporre di più regole identiche per lo spostamento dei dispositivi con diversi intervalli IP e gruppi di destinazione.

Per clonare una regola di spostamento dei dispositivi:

1. Aprire la finestra principale dell'applicazione.
2. Nella cartella **Dispositivi non assegnati** fare clic su **Configura regole**.

   Verrà visualizzata la finestra **Proprietà: Dispositivi non assegnati**.
3. Nella sezione **Sposta dispositivi** selezionare la regola di spostamento dei dispositivi che si desidera clonare.
4. Fare clic su **Clona regola**.

Un duplicato della regola di spostamento dei dispositivi selezionata verrà aggiunta alla fine dell'elenco.

Una nuova regola viene creata nello stato disabilitato. È possibile modificare e abilitare la regola in qualsiasi momento.

Classificazione del software

Lo strumento principale per monitorare l'esecuzione delle applicazioni sono le *categorie Kaspersky* (di seguito denominate anche *categorie KL*). Le categorie KL consentono agli amministratori di Kaspersky Security Center di semplificare il supporto della classificazione del software e ridurre al minimo il traffico verso i dispositivi gestiti.

È necessario creare categorie utente per le applicazioni che non possono essere classificate in alcuna delle categorie KL esistenti (ad esempio, per il software personalizzato). Le categorie utente vengono create in base al pacchetto di installazione di un'applicazione (MSI) o a una cartella con pacchetti di installazione.

Se è disponibile una raccolta di software di grandi dimensioni che non è stata classificata tramite le categorie KL, può essere utile creare una categoria aggiornata automaticamente. I checksum dei file eseguibili saranno aggiunti automaticamente a questa categoria a ogni modifica della cartella che contiene i pacchetti di distribuzione.

Non creare categorie di software aggiornate automaticamente per le cartelle Documenti, %windir%, %ProgramFiles% e %ProgramFiles(x86)%. Il pool di file in queste cartelle è soggetto a modifiche frequenti, il che comporta un aumento del carico su Administration Server e del traffico di rete. È necessario creare una cartella dedicata con la raccolta del software e aggiungere periodicamente nuovi elementi a tale raccolta.

Prerequisiti per l'installazione delle applicazioni nei dispositivi di un'organizzazione client

Il processo di installazione remota delle applicazioni nei dispositivi di un'organizzazione client è identico al processo di installazione remota all'interno di un'organizzazione.

Per installare le applicazioni nei dispositivi di un'organizzazione client, è necessario eseguire le seguenti operazioni:

- Prima di installare per la prima volta le applicazioni nei dispositivi dell'organizzazione client, installare Network Agent in tali dispositivi.

  Durante la configurazione del pacchetto di installazione di Network Agent da parte del provider di servizi, in Kaspersky Security Center definire le seguenti impostazioni nella finestra delle proprietà del pacchetto di installazione:

  - Nella stringa **Administration Server** della sezione **Connessione** specificare l'indirizzo dello stesso Administration Server virtuale specificato durante l'installazione locale di Network Agent nel punto di distribuzione.

  - Nella sezione **Avanzate** selezionare la casella di controllo **Esegui la connessione ad Administration Server utilizzando un gateway di connessione**. Nella stringa **Indirizzo gateway connessione** specificare l'indirizzo del punto di distribuzione. È possibile utilizzare sia l'indirizzo IP che il nome del dispositivo nella rete Windows.

- Selezionare **Utilizzo delle risorse del sistema operativo tramite punti di distribuzione** come metodo di download del pacchetto di installazione di Network Agent. È possibile selezionare il metodo di download come segue:

  - Se si installa l'applicazione utilizzando l'attività di installazione remota, è possibile specificare il metodo di download in uno dei seguenti modi:

    - Durante la creazione dell'attività di installazione remota, nella finestra **Impostazioni**

    - Nella finestra delle proprietà dell'attività di installazione remota, nella sezione **Impostazioni**

  - Se si installano le applicazioni utilizzando l'Installazione remota guidata, è possibile selezionare un metodo di download nella finestra **Impostazioni** della procedura guidata.

- L'account utilizzato dal punto di distribuzione per l'autorizzazione deve avere accesso alla risorsa Admin$ in tutti i dispositivi client.

Visualizzazione e modifica delle impostazioni locali delle applicazioni

Il sistema di amministrazione Kaspersky Security Center consente di gestire in remoto le impostazioni locali delle applicazioni nei dispositivi tramite Administration Console.

Le *impostazioni locali delle applicazioni* sono le impostazioni di un'applicazione specifiche per un dispositivo. È possibile utilizzare Kaspersky Security Center per impostare le impostazioni locali delle applicazioni per i dispositivi inclusi nei gruppi di amministrazione.

Le descrizioni dettagliate delle impostazioni delle applicazioni Kaspersky sono disponibili nelle rispettive Guide.

Per visualizzare o modificare le impostazioni locali di un'applicazione:

1. Nell'area di lavoro del gruppo a cui appartiene il dispositivo attinente selezionare la scheda **Dispositivi**.

2. Nella finestra delle proprietà del dispositivo, nella sezione **Applicazioni**, selezionare l'applicazione desiderata.

3. Aprire la finestra delle proprietà dell'applicazione facendo doppio clic sul nome dell'applicazione oppure facendo clic sul pulsante **Proprietà**.

Verrà visualizzata la finestra delle impostazioni locali dell'applicazione selezionata, in cui è possibile visualizzare e modificare tali impostazioni.

È possibile modificare i valori delle impostazioni le cui modifiche non sono state bloccate da un criterio di gruppo (ovvero, quelle non contrassegnate dall'icona del lucchetto (🔒) in un criterio).

Aggiornamento di Kaspersky Security Center e delle applicazioni gestite

Questa sezione descrive le operazioni che è necessario eseguire per aggiornare Kaspersky Security Center e le applicazioni gestite.

Scenario: Aggiornamento periodico di database e applicazioni Kaspersky

Questa sezione fornisce uno scenario per l'aggiornamento periodico dei database, dei moduli software e delle applicazioni Kaspersky. Dopo aver completato lo scenario Configurazione della protezione di rete, è necessario mantenere l'affidabilità del sistema di protezione per assicurarsi che gli Administration Server e i dispositivi gestiti siano protetti da varie minacce, inclusi virus, attacchi di rete e attacchi di phishing.

La protezione della rete viene mantenuta aggiornata tramite aggiornamenti periodici dei seguenti elementi:

- Database e moduli del software Kaspersky
- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center e le applicazioni di protezione

Completando questo scenario, è possibile avere la certezza di quanto segue:

- La rete è protetta dal software Kaspersky più recente, inclusi i componenti di Kaspersky Security Center e le applicazioni di protezione.
- I database anti-virus e gli altri database Kaspersky di importanza critica per la sicurezza della rete sono sempre aggiornati.

Prerequisiti

I dispositivi gestiti devono disporre di una connessione ad Administration Server. Se non dispongono di una connessione, valutare se eseguire l'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky manualmente o direttamente dai server degli aggiornamenti Kaspersky.

Administration Server deve disporre di una connessione a Internet.

Prima di iniziare, verificare di avere:

1. Distribuito le applicazioni di protezione Kaspersky nei dispositivi gestiti in base allo scenario di distribuzione delle applicazioni Kaspersky tramite Kaspersky Security Center Web Console.
2. Creato e configurato tutti i criteri, i profili criterio e le attività richiesti in base allo scenario di configurazione della protezione di rete.
3. Assegnato un numero appropriato di punti di distribuzione in base al numero di dispositivi gestiti e alla topologia della rete.

L'aggiornamento dei database e delle applicazioni Kaspersky prevede diversi passaggi:

1 Scelta di uno schema di aggiornamento

Esistono diversi schemi che è possibile utilizzare per installare gli aggiornamenti dei componenti di Kaspersky Security Center e delle applicazioni di protezione. Scegliere lo schema o gli schemi più appropriati per i requisiti della rete.

2 Creazione dell'attività per il download degli aggiornamenti nell'archivio di Administration Server

Questa attività viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. Se la procedura guidata non è stata eseguita, creare l'attività ora.

Questa attività è necessaria per scaricare gli aggiornamenti dai server di aggiornamento Kaspersky nell'archivio di Administration Server, nonché per aggiornare i database e i moduli software Kaspersky per Kaspersky Security Center. Dopo aver scaricato gli aggiornamenti, questi possono essere propagati ai dispositivi gestiti.

Se nella rete sono stati assegnati punti di distribuzione, gli aggiornamenti vengono scaricati automaticamente dall'archivio di Administration Server agli archivi dei punti di distribuzione. In questo caso, i dispositivi gestiti inclusi nell'ambito di un punto di distribuzione scaricano gli aggiornamenti dall'archivio del punto di distribuzione anziché dall'archivio di Administration Server.

Istruzioni dettagliate:

- Administration Console: Creazione dell'attività per il download degli aggiornamenti nell'archivio dell'Administration Server
- Kaspersky Security Center Web Console: Creazione dell'attività per il download degli aggiornamenti nell'archivio dell'Administration Server

3 Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione (facoltativo)

Per impostazione predefinita, gli aggiornamenti vengono scaricati nei punti di distribuzione dall'Administration Server. È possibile configurare Kaspersky Security Center per scaricare gli aggiornamenti nei punti di distribuzione direttamente dai server di aggiornamento Kaspersky. Il download negli archivi dei punti di distribuzione è preferibile se il traffico tra Administration Server e punti di distribuzione è superiore rispetto a quello del traffico tra i punti di distribuzione e i server di aggiornamento Kaspersky oppure se Administration Server non dispone di accesso a Internet.

Quando nella rete sono stati assegnati punti di distribuzione ed è stata creata l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, i punti di distribuzione scaricano gli aggiornamenti dai server di aggiornamento Kaspersky e non dall'archivio dell'Administration Server.

Istruzioni dettagliate:

- Administration Console: Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione
- Kaspersky Security Center Web Console: Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione

4. **Configurazione dei punti di distribuzione**

   Quando nella rete sono stati assegnati punti di distribuzione, verificare che l'opzione **Distribuisci aggiornamenti** sia abilitata nelle proprietà di tutti i punti di distribuzione richiesti. Quando questa opzione è disabilitata per un punto di distribuzione, i dispositivi inclusi nell'ambito del punto di distribuzione scaricano gli aggiornamenti dall'archivio di Administration Server.

   Se si desidera che i dispositivi gestiti ricevano gli aggiornamenti solo dai punti di distribuzione, abilitare l'opzione **Distribuisci i file solo tramite punti di distribuzione** nel criterio di Network Agent.

5. **Ottimizzazione del processo di aggiornamento utilizzando il modello offline di download degli aggiornamenti o i file diff (facoltativo)**

   È possibile ottimizzare il processo di aggiornamento utilizzando il modello offline di download degli aggiornamenti (abilitato per impostazione predefinita) oppure i file diff. Per ogni segmento di rete, è necessario scegliere quale di queste due funzionalità abilitare, perché non possono funzionare contemporaneamente.

   Quando il modello offline di download degli aggiornamenti è abilitato, Network Agent scarica gli aggiornamenti richiesti nel dispositivo gestito una volta che gli aggiornamenti sono stati scaricati nell'archivio di Administration Server, prima che l'applicazione di protezione li richieda. Questo migliora l'affidabilità del processo di aggiornamento. Per utilizzare questa funzionalità, abilitare l'opzione **Scarica aggiornamenti e database anti-virus da Administration Server anticipatamente (scelta consigliata)** nel criterio di Network Agent.

   Se non si utilizza il modello offline di download degli aggiornamenti, è possibile ottimizzare il traffico tra Administration Server e i dispositivi gestiti tramite i file diff. Quando questa funzionalità è abilitata, Administration Server o un punto di distribuzione scarica file diff anziché interi file di database o moduli software Kaspersky. Un file diff descrive le differenze tra due versioni di un file di un database o un modulo software. Pertanto, un file diff occupa meno spazio di un intero file. Questo comporta una riduzione del traffico tra Administration Server o i punti di distribuzione e i dispositivi gestiti. Per utilizzare questa funzionalità, abilitare l'opzione **Scarica file diff** nelle proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* e/o dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

   Istruzioni dettagliate:

   - Utilizzo dei file diff per l'aggiornamento dei database e dei moduli del software Kaspersky
   - Administration Console: Abilitazione e disabilitazione del modello offline per il download degli aggiornamenti
   - Kaspersky Security Center Web Console: Abilitazione e disabilitazione del modello offline per il download degli aggiornamenti

6. **Verifica degli aggiornamenti scaricati (facoltativo)**

   Prima di installare gli aggiornamenti scaricati, è possibile verificare gli aggiornamenti tramite l'attività di *Verifica aggiornamenti*. Questa attività esegue in sequenza le attività di aggiornamento dei dispositivi e le attività di scansione malware configurate tramite le impostazioni per il gruppo specificato di dispositivi di test. Una volta ottenuti i risultati delle attività, Administration Server avvia o blocca la propagazione degli aggiornamenti ai dispositivi rimanenti.

   L'attività *Verifica aggiornamenti* può essere eseguita durante l'esecuzione dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Nelle proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* abilitare l'opzione **Verifica gli aggiornamenti prima della distribuzione** in Administration Console o l'opzione **Esegui la verifica degli aggiornamenti** in Kaspersky Security Center Web Console.

   Istruzioni dettagliate:

   - Administration Console: Verifica degli aggiornamenti scaricati
   - Kaspersky Security Center Web Console: Verifica degli aggiornamenti scaricati

7. **Approvazione e rifiuto degli aggiornamenti software**

Per impostazione predefinita, gli aggiornamenti software scaricati hanno lo stato *Indefinito*. È possibile modificare lo stato in *Approvato* o *Rifiutato*. Gli aggiornamenti approvati vengono sempre installati. Se un aggiornamento richiede la visualizzazione e l'accettazione dei termini del Contratto di licenza con l'utente finale, è prima necessario accettare i termini. Successivamente, l'aggiornamento può essere propagato ai dispositivi gestiti. Gli aggiornamenti indefiniti possono essere installati solo in Network Agent e negli altri componenti di Kaspersky Security Center in conformità con le impostazioni del criterio di Network Agent. Gli aggiornamenti per cui è stato impostato lo stato *Rifiutato* non verranno installati nei dispositivi. Se in precedenza era stato installato un aggiornamento rifiutato per un'applicazione di protezione, Kaspersky Security Center tenterà di disinstallare l'aggiornamento da tutti i dispositivi.

L'approvazione e il rifiuto degli aggiornamenti sono disponibili solo per Network Agent e le applicazioni Kaspersky gestite installate nei dispositivi client basati su Windows e basatu su Linux. L'aggiornamento continuo di Administration Server, Kaspersky Security Center Web Console e plug-in Web di gestione non è supportato.

Istruzioni dettagliate:

- Administration Console: Approvazione e rifiuto degli aggiornamenti software
- Kaspersky Security Center Web Console: Approvazione e rifiuto degli aggiornamenti software

8. **Configurazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center**

   Gli aggiornamenti scaricati e le patch scaricate per Network Agent e altri componenti di Kaspersky Security Center vengono installati automaticamente. Se l'opzione **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito** è stata mantenuta abilitata nelle proprietà di Network Agent, tutti gli aggiornamenti verranno installati automaticamente dopo essere stati scaricati nell'archivio (o in diversi archivi). Se questa opzione è disabilitata, le patch di Kaspersky che sono state scaricate e contrassegnate con lo stato *Indefinito* saranno installate solo dopo che si modifica il relativo stato in *Approvato*.

   Istruzioni dettagliate:

   - Administration Console: Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center
   - Kaspersky Security Center Web Console: Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center

9. **Installazione degli aggiornamenti per Administration Server**

   Gli aggiornamenti software per Administration Server non dipendono dagli stati degli aggiornamenti. Non vengono installati automaticamente e devono prima essere approvati dall'amministratore nella scheda **Monitoraggio** di Administration Console (**Administration Server** `<nome server>` → **Monitoraggio**) o nella sezione **Notifiche** di Kaspersky Security Center Web Console (**Monitoraggio e generazione dei rapporti** → **Notifiche**). Successivamente, l'amministratore deve eseguire esplicitamente l'installazione degli aggiornamenti.

10. **Configurazione dell'installazione automatica degli aggiornamenti per le applicazioni di protezione**

    Creare le *Attività* di aggiornamento per le applicazioni gestite per garantire aggiornamenti tempestivi alle applicazioni, ai moduli software e ai database Kaspersky, inclusi i database anti-virus. Per garantire aggiornamenti tempestivi, è consigliabile selezionare l'opzione **Quando vengono scaricati nuovi aggiornamenti nell'archivio** durante la configurazione della pianificazione dell'attività.

    Se la rete include dispositivi solo IPv6 e si desidera aggiornare regolarmente le applicazioni di protezione installate in tali dispositivi, assicurarsi che Administration Server (versione non precedente alla 13.2) e Network Agent (versione non precedente alla 13.2) siano installati nei dispositivi gestiti.

    Per impostazione predefinita, gli aggiornamenti per Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Security for Linux vengono installati solo dopo aver modificato lo stato degli aggiornamenti in *Approvato*. È possibile modificare le impostazioni di aggiornamento nell'*attività* di aggiornamento.

Se un aggiornamento richiede la visualizzazione e l'accettazione dei termini del Contratto di licenza con l'utente finale, è prima necessario accettare i termini. Successivamente, l'aggiornamento può essere propagato ai dispositivi gestiti.

Istruzioni dettagliate:

- Administration Console: Installazione automatica degli aggiornamenti di Kaspersky Endpoint Security nei dispositivi
- Kaspersky Security Center Web Console: Installazione automatica degli aggiornamenti di Kaspersky Endpoint Security nei dispositivi

Risultati

Al termine dello scenario, Kaspersky Security Center è configurato per aggiornare i database Kaspersky e le applicazioni Kaspersky installate dopo che gli aggiornamenti vengono scaricati nell'archivio di Administration Server o negli archivi dei punti di distribuzione. È quindi possibile procedere al monitoraggio dello stato della rete.

Informazioni sull'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky

Per assicurarsi che la protezione dei propri Administration Server e dispositivi gestiti sia aggiornata, è necessario garantire aggiornamenti tempestivi dei seguenti componenti:

- Database e moduli del software Kaspersky

  Prima di scaricare i database e i moduli software di Kaspersky, Kaspersky Security Center verifica se i server Kaspersky sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. Ciò è necessario per garantire che i database anti-virus siano aggiornati e per mantenere il livello di sicurezza per i dispositivi gestiti.

- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center e le applicazioni di protezione

  Kaspersky Security Center consente di aggiornare automaticamente Network Agent e le applicazioni Kaspersky installate nei dispositivi client basati su Windows e basati su Linux. L'aggiornamento continuo di Administration Server, Kaspersky Security Center Web Console e plug-in Web di gestione non è supportato. Per aggiornare questi componenti è necessario scaricare le versioni più recenti delle applicazioni dal sito Web di Kaspersky, quindi installarle manualmente.

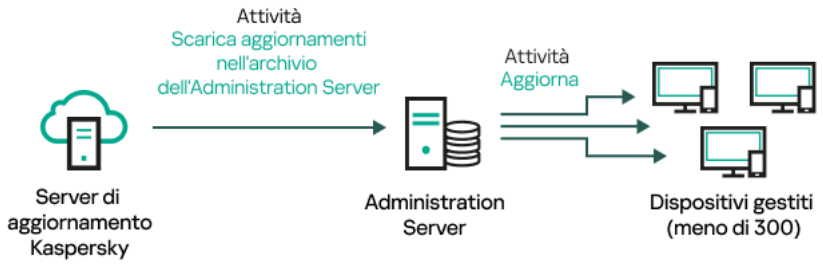
In base alla configurazione della propria rete è possibile utilizzare i seguenti schemi di download e distribuzione degli aggiornamenti richiesti ai dispositivi gestiti:

- Utilizzando un'unica attività: *Scarica aggiornamenti nell'archivio dell'Administration Server*
- Utilizzando due attività:
  - L'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*
  - L'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*
- Manualmente attraverso una cartella locale, una cartella condivisa o un server FTP

- Direttamente dai server di aggiornamento Kaspersky a Kaspersky Endpoint Security nei dispositivi gestiti
- Tramite una cartella locale o di rete se Administration Server non dispone della connessione a Internet

Utilizzo dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server

In questo schema Kaspersky Security Center scarica gli aggiornamenti tramite l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Nelle reti piccole che contengono meno di 300 dispositivi gestiti in un singolo segmento di rete o meno di 10 dispositivi gestiti in ciascun segmento di rete, gli aggiornamenti vengono distribuiti nei dispositivi gestiti direttamente dall'archivio di Administration Server (vedere la figura di seguito).

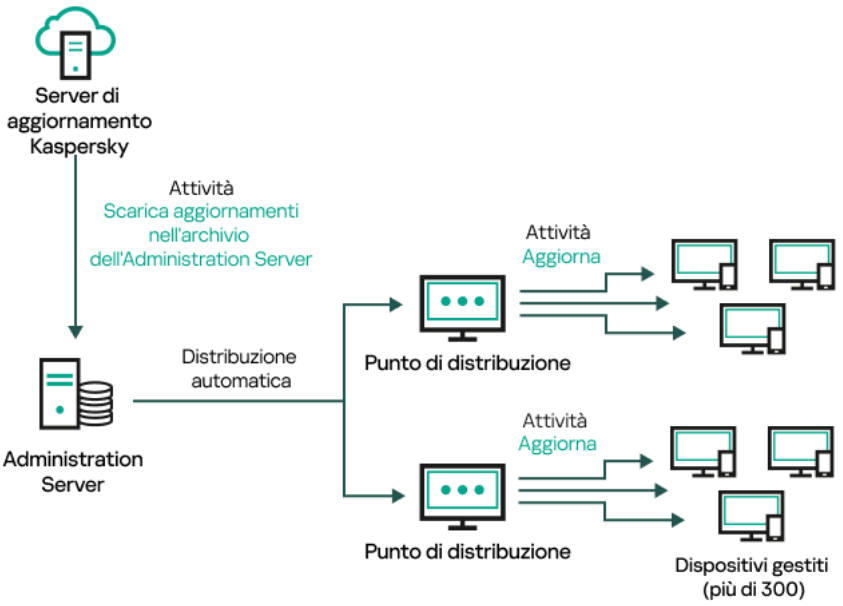


Aggiornamento tramite l'attività Scarica aggiornamenti nell'archivio dell'Administration Server senza punti di distribuzione

Per impostazione predefinita, Administration Server comunica con i server di aggiornamento Kaspersky e scarica gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server per fare in modo che utilizzi il protocollo HTTP anziché HTTPS.

Se la rete contiene più di 300 dispositivi gestiti in un singolo segmento di rete o se la rete è composta da più segmenti di rete con più di 9 dispositivi gestiti in ciascun segmento di rete, è consigliabile utilizzare i punti di distribuzione per propagare gli aggiornamenti ai dispositivi gestiti (vedere la figura di seguito). I punti di distribuzione riducono il carico per Administration Server e ottimizzano il traffico tra Administration Server e dispositivi gestiti. È possibile calcolare il numero e la configurazione dei punti di distribuzione richiesti per la rete.

In questo schema gli aggiornamenti vengono scaricati automaticamente dall'archivio di Administration Server agli archivi dei punti di distribuzione. I dispositivi gestiti inclusi nell'ambito di un punto di distribuzione scaricano gli aggiornamenti dall'archivio del punto di distribuzione anziché dall'archivio di Administration Server.



Aggiornamento tramite l'attività Scarica aggiornamenti nell'archivio dell'Administration Server con punti di distribuzione

Al completamento dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, i seguenti aggiornamenti vengono scaricati nell'archivio dell'Administration Server:

- Moduli del software e database Kaspersky per Kaspersky Security Center

  Questi aggiornamenti vengono installati automaticamente.

- Moduli del software e database Kaspersky per le applicazioni di protezione nei dispositivi gestiti

  Questi aggiornamenti vengono installati tramite l'attività di aggiornamento per Kaspersky Endpoint Security for Windows.

- Aggiornamenti per Administration Server

  Questi aggiornamenti non vengono installati automaticamente. L'amministratore deve approvare esplicitamente ed eseguire l'installazione degli aggiornamenti.

  > Sono necessari i diritti di amministratore locale per l'installazione delle patch nell'Administration Server.

- Aggiornamenti per i componenti di Kaspersky Security Center

  Per impostazione predefinita, questi aggiornamenti vengono installati automaticamente. È possibile modificare le impostazioni nel criterio di Network Agent.

- Aggiornamenti per le applicazioni di protezione

  Per impostazione predefinita, Kaspersky Endpoint Security for Windows installa solo gli aggiornamenti approvati. È possibile approvare gli aggiornamenti tramite Administration Console o tramite Kaspersky Security Center Web Console. Gli aggiornamenti vengono installati attraverso l'attività di *aggiornamento* e possono essere configurati nelle proprietà di questa attività.

> L'attività *Scarica aggiornamenti nell'archivio di Administration Server* non è disponibile negli Administration Server virtuali. L'archivio dell'Administration Server virtuale visualizza gli aggiornamenti scaricati nell'Administration Server primario.

È possibile configurare la verifica della possibilità di utilizzare gli aggiornamenti e degli eventuali errori in un set di dispositivi di test. Se la verifica ha esito positivo, gli aggiornamenti vengono distribuiti agli altri dispositivi gestiti.

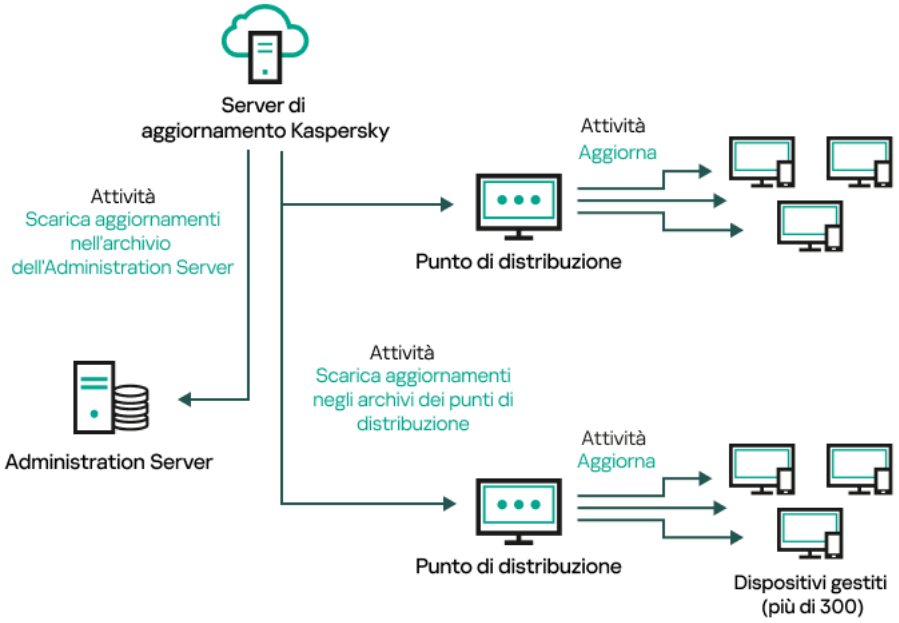
Ogni applicazione Kaspersky richiede gli aggiornamenti necessari da Administration Server. Administration Server aggrega tali richieste e scarica solo gli aggiornamenti che sono richiesti da un'applicazione. Questo garantisce che gli stessi aggiornamenti non vengano scaricati più volte e che gli aggiornamenti non necessari non vengano scaricati affatto. Durante l'esecuzione dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, Administration Server invia automaticamente le seguenti informazioni ai server di aggiornamento Kaspersky per garantire il download delle versioni appropriate dei moduli software e dei database Kaspersky:

- Versione e ID applicazione
- ID di installazione dell'applicazione
- ID chiave attiva
- ID di esecuzione dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*

Le informazioni trasmesse non contengono dati personali o altri dati riservati. AO Kaspersky Lab protegge le informazioni in base ai requisiti previsti dalla legge.

Tramite due attività: l'attività Scarica aggiornamenti nell'archivio dell'Administration Server e l'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

È possibile scaricare gli aggiornamenti negli archivi dei punti di distribuzione direttamente dai server di aggiornamento Kaspersky anziché dall'archivio di Administration Server, quindi distribuire gli aggiornamenti ai dispositivi gestiti (vedere la figura di seguito). Il download negli archivi dei punti di distribuzione è preferibile se il traffico tra Administration Server e punti di distribuzione è superiore rispetto a quello del traffico tra i punti di distribuzione e i server di aggiornamento Kaspersky oppure se Administration Server non dispone di accesso a Internet.



Aggiornamento tramite l'attività Scarica aggiornamenti nell'archivio dell'Administration Server e l'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

Per impostazione predefinita, Administration Server e i punti di distribuzione comunicano con i server di aggiornamento Kaspersky e scaricano gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server e/o i punti di distribuzione per fare in modo che utilizzino il protocollo HTTP anziché HTTPS.

Per implementare questo schema, creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* oltre all'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. In seguito, i punti di distribuzione scaricheranno gli aggiornamenti dai server di aggiornamento Kaspersky e non dall'archivio di Admnistration Server.

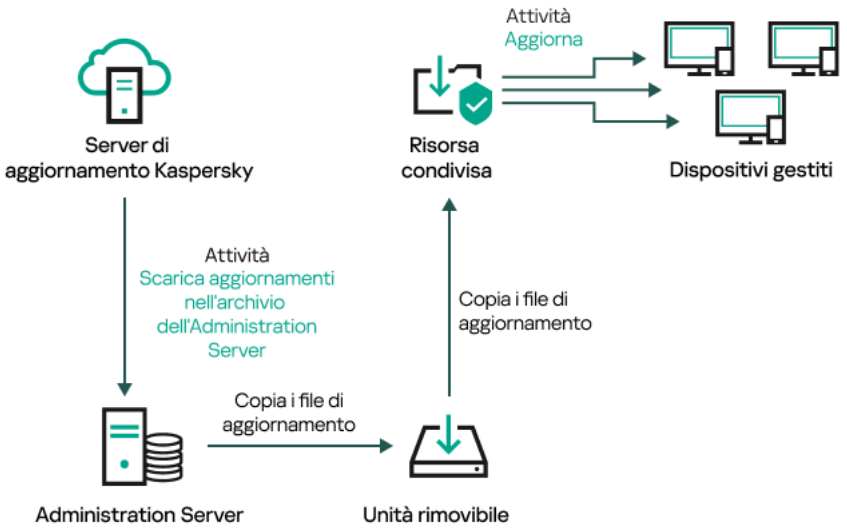
I dispositivi dei punti di distribuzione che eseguono macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky.

Se uno o più dispositivi che eseguono macOS rientrano nell'ambito dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'attività viene completata con lo stato *Non riuscito*, anche se è stata completata correttamente in tutti i dispositivi Windows.

Anche l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* è richiesta per questo schema, poiché questa attività è utilizzata per scaricare i moduli software e i database Kaspersky per Kaspersky Security Center.

Manualmente attraverso una cartella locale, una cartella condivisa o un server FTP

Se i dispositivi client non hanno una connessione ad Administration Server, è possibile utilizzare una cartella locale o una risorsa condivisa come sorgente per l'aggiornamento di database, moduli software e applicazioni Kaspersky. In questo schema è necessario copiare gli aggiornamenti richiesti dall'archivio di Administration Server in un'unità rimovibile, quindi copiare gli aggiornamenti nella cartella locale o nella risorsa condivisa specificata come sorgente degli aggiornamenti nelle impostazioni di Kaspersky Endpoint Security (vedere la figura di seguito).



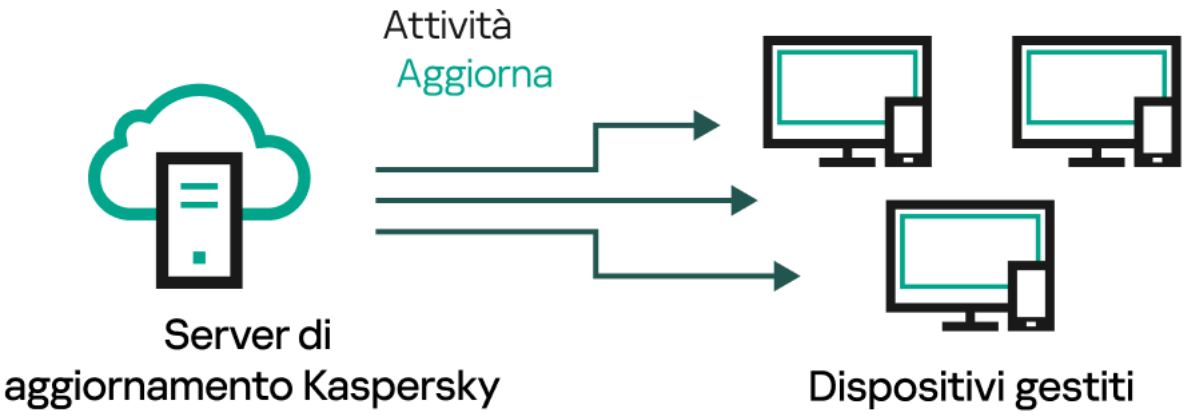
Aggiornamento tramite una cartella locale, una cartella condivisa o un server FTP

Per ulteriori informazioni sulle sorgenti degli aggiornamenti in Kaspersky Endpoint Security, consultare le seguenti Guide:

- Guida di Kaspersky Endpoint Security for Windows
- Guida di Kaspersky Endpoint Security for Linux

Direttamente dai server di aggiornamento Kaspersky a Kaspersky Endpoint Security nei dispositivi gestiti

Nei dispositivi gestiti, è possibile configurare Kaspersky Endpoint Security per ricevere gli aggiornamenti direttamente dai server di aggiornamento Kaspersky (vedere la figura di seguito).



Aggiornamento delle applicazioni di protezione direttamente dai server di aggiornamento Kaspersky

In questo schema, l'applicazione di protezione non utilizza gli archivi forniti da Kaspersky Security Center. Per ricevere gli aggiornamenti direttamente dai server di aggiornamento Kaspersky, specificare i server di aggiornamento Kaspersky come sorgente degli aggiornamenti nell'interfaccia dell'applicazione di protezione. Per ulteriori informazioni su queste impostazioni, consultare le seguenti Guide:

- Guida di Kaspersky Endpoint Security for Windows
- Guida di Kaspersky Endpoint Security for Linux

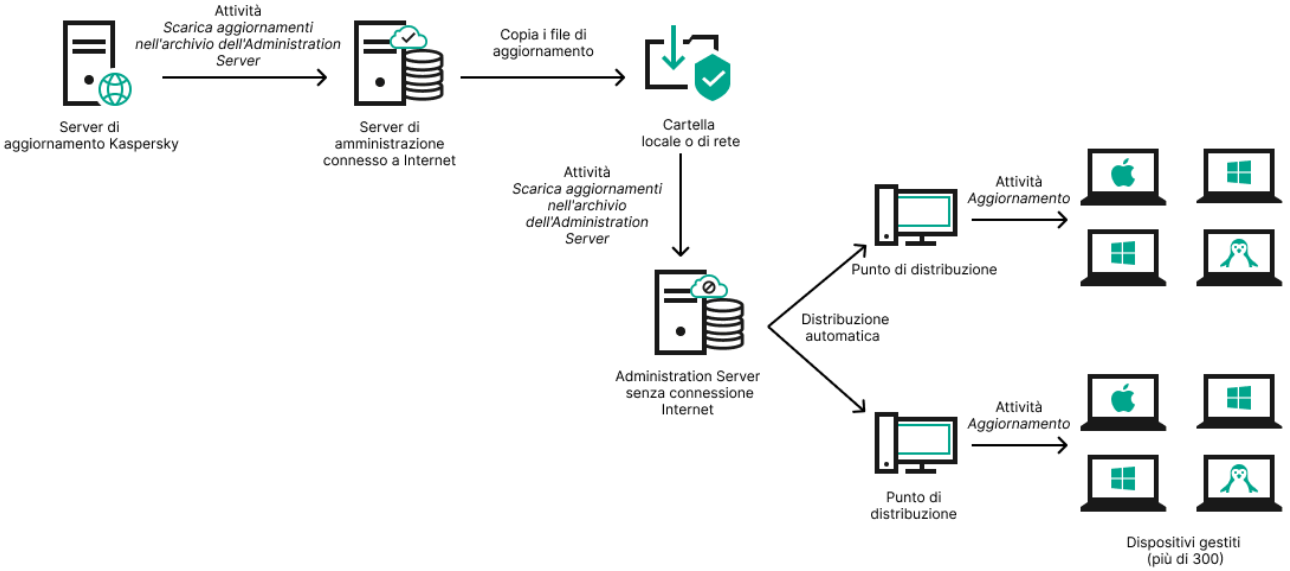
Tramite una cartella locale o di rete se Administration Server non dispone della connessione a Internet

Se Administration Server non dispone della connessione a Internet, è possibile configurare l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* per scaricare gli aggiornamenti da una cartella locale o di rete. In questo caso, di tanto in tanto è necessario copiare i file di aggiornamento necessari nella cartella specificata. È ad esempio possibile copiare i file di aggiornamento necessari da una delle seguenti origini:

- Administration Server con una connessione Internet (vedere la figura seguente)

  Poiché un Administration Server scarica solo gli aggiornamenti richiesti dalle applicazioni di protezione, i set di applicazioni di protezione gestiti dagli Administration Server (quello con una connessione Internet e quello senza connessione), devono corrispondere.

  Se l'Administration Server utilizzato per scaricare gli aggiornamenti dispone della versione 13.2 o precedente, aprire le proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, quindi abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**.



Aggiornamento tramite una cartella locale o di rete se Administration Server non dispone di una connessione Internet

- Kaspersky Update Utility

  Poiché questa utilità utilizza il vecchio schema per scaricare gli aggiornamenti, aprire le proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, quindi abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**.

Informazioni sull'utilizzo dei file diff per l'aggiornamento dei database e dei moduli del software Kaspersky

Quando Kaspersky Security Center scarica gli aggiornamenti dai server di aggiornamento Kaspersky, ottimizza il traffico utilizzando file diff. È anche possibile abilitare l'utilizzo dei file diff da parte dei dispositivi (Administration Server, punti di distribuzione e dispositivi client) che recuperano gli aggiornamenti da altri dispositivi della rete.

Informazioni sulla funzionalità Download dei file diff

Un file diff descrive le differenze tra due versioni di un file di un database o un modulo software. L'utilizzo dei file diff riduce il traffico all'interno della rete aziendale, poiché i file diff occupano meno spazio rispetto ai file completi di database e moduli software. Se è abilitata la funzionalità *Download dei file diff* in un Administration Server o un punto di distribuzione, i file diff vengono salvati in questo Administration Server o punto di distribuzione. Come risultato, i dispositivi che recuperano gli aggiornamenti da questo Administration Server o punto di distribuzione possono utilizzare i file diff salvati per l'aggiornamento dei database e dei moduli software.

Per ottimizzare l'utilizzo dei file diff, è consigliabile sincronizzare la pianificazione di aggiornamento dei dispositivi con la pianificazione di aggiornamento dell'Administration Server o del punto di distribuzione da cui i dispositivi recuperano gli aggiornamenti. Il traffico può comunque essere ridotto anche se i dispositivi vengono aggiornati con una frequenza notevolmente inferiore a quella dell'Administration Server o del punto di distribuzione da cui i dispositivi recuperano gli aggiornamenti.

La funzionalità Download dei file diff può essere abilitata solo negli Administration Server e nei punti di distribuzione versione 11 e successive. Per salvare i file diff in Administration Server e punti di distribuzione di versioni precedenti, eseguirne l'upgrade alla versione 11 o successiva.

La funzionalità Download dei file diff è incompatibile con il modello offline per il download degli aggiornamenti. In altre parole, i Network Agent che utilizzano il modello offline di download degli aggiornamenti non scaricano i file diff anche se la funzionalità Download dei file diff è stata attivata nell'Administration Server o nel punto di distribuzione che fornisce gli aggiornamenti a questi Network Agent.

I punti di distribuzione non utilizzano la modalità IP multicast per la distribuzione automatica dei file diff.

Abilitazione della funzionalità Download dei file diff

Prerequisiti

I prerequisiti per lo scenario sono i seguenti:

- È stato eseguito l'upgrade di Administration Server e punti di distribuzione alla versione 11 o successiva.
- Il modello offline per il download degli aggiornamenti è disabilitato nelle impostazioni del criterio di Network Agent.

Passaggi

1. **Abilitazione della funzionalità in Administration Server**

   Abilitare la funzionalità nelle impostazioni di un'attività Scarica aggiornamenti nell'archivio dell'Administration Server.

2. **Abilitazione della funzionalità per un punto di distribuzione**

   Abilitare la funzionalità per un punto di distribuzione che riceve gli aggiornamenti tramite un'attività Scarica aggiornamenti negli archivi dei punti di distribuzione.

   Successivamente abilitare la funzionalità per un punto di distribuzione che riceve gli aggiornamenti da Administration Server.

   La funzionalità è abilitata nelle impostazioni del criterio di Network Agent e, se sono stati assegnati manualmente punti di distribuzione e se si desidera sostituire le impostazioni del criterio, nella sezione **Punti di distribuzione**.

Per verificare che la funzionalità Download dei file diff sia abilitata correttamente, è possibile misurare il traffico interno prima e dopo l'esecuzione dello scenario.

Creazione dell'attività per il download degli aggiornamenti nell'archivio di Administration Server

L'attività *Scarica aggiornamenti nell'archivio di Administration Server* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. È possibile creare una sola attività *Scarica aggiornamenti nell'archivio di Administration Server*. Di conseguenza, è possibile creare un'attività *Scarica aggiornamenti nell'archivio di Administration Server* solo se tale attività è stata rimossa dall'elenco di attività di Administration Server.

Per creare un'attività Scarica aggiornamenti nell'archivio di Administration Server:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Avviare la creazione dell'attività in uno dei seguenti modi:
   - Nel menu di scelta rapida della cartella **Attività** nella struttura della console selezionare **Nuovo** → **Attività**.
   - Nell'area di lavoro della cartella **Attività** fare clic sul pulsante **Crea attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Nella pagina **Selezionare il tipo di attività** della procedura guidata selezionare **Scarica aggiornamenti nell'archivio dell'Administration Server**.

4. Nella pagina **Impostazioni** della procedura guidata specificare le impostazioni dell'attività nel modo seguente:

- **Sorgenti degli aggiornamenti**

  È possibile utilizzare le seguenti risorse come sorgenti degli aggiornamenti per l'Administration Server:

  - Server degli aggiornamenti Kaspersky

    I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni. Per impostazione predefinita, Administration Server comunica con i server di aggiornamento Kaspersky e scarica gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server per fare in modo che utilizzi il protocollo HTTP anziché HTTPS.

    Opzione selezionata per impostazione predefinita.

  - Administration Server primario

    Questa risorsa si applica alle attività create per un Administration Server secondario o virtuale.

  - Cartella locale o di rete

    Un'unità locale o una cartella di rete che contiene gli aggiornamenti più recenti. Una cartella di rete può essere un server FTP o HTTP oppure una condivisione SMB. Se una cartella di rete richiede l'autenticazione, è supportato solo il protocollo SMB. Quando si seleziona una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server.

    Una cartella di rete o un server FTP o HTTP utilizzato da una sorgente degli aggiornamenti deve contenere una struttura di cartelle (con gli aggiornamenti) che corrisponde alla struttura creata durante l'utilizzo dei server di aggiornamento Kaspersky.

- **Altre impostazioni**:

  - **Forza aggiornamento degli Administration Server secondari**

    Se questa opzione è abilitata, Administration Server avvia le attività di aggiornamento negli Administration Server secondari non appena vengono scaricati nuovi aggiornamenti. Le attività di aggiornamento vengono avviate utilizzando la sorgente dell'aggiornamento configurata nelle proprietà dell'attività negli Administration Server secondari.

    Se questa opzione è disabilitata, le attività di aggiornamento negli Administration Server secondari vengono avviate in base alla relativa pianificazione.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Copia gli aggiornamenti scaricati in cartelle aggiuntive**

Dopo avere ricevuto gli aggiornamenti, l'Administration Server li copia nelle cartelle specificate. Utilizzare questa opzione se si desidera gestire manualmente la distribuzione degli aggiornamenti nella rete.

Questa opzione può ad esempio essere utilizzata nella seguente situazione: la rete dell'organizzazione è composta da diverse subnet indipendenti e i dispositivi in ciascuna subnet non hanno accesso ad altre subnet. I dispositivi in tutte le subnet hanno tuttavia accesso a una condivisione di rete comune. In questo caso, è possibile impostare Administration Server in una delle subnet per il download degli aggiornamenti dai server di aggiornamento Kaspersky, abilitare questa opzione e quindi specificare la condivisione di rete. Nelle attività di download degli aggiornamenti nell'archivio per gli altri Administration Server specificare la stessa condivisione di rete come sorgente degli aggiornamenti.

Se si seleziona di copiare gli aggiornamenti scaricati in una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server. Il percorso della cartella dipende dal sistema operativo del dispositivo. Poiché la cartella locale si trova in Administration Server basato su Linux, è necessario specificare il percorso POSIX, ad esempio /path/to/dir.

Quando si seleziona una cartella di rete che si trova in Administration Server basato su Linux, è necessario garantire preventivamente l'accesso alla cartella di rete dal dispositivo in cui è installato Administration Server montando la cartella. L'accesso alla cartella viene eseguito utilizzando il protocollo SMB.

Per impostazione predefinita, questa opzione è disabilitata.

- **Non forzare l'aggiornamento dei dispositivi e degli Administration Server secondari prima del completamento della copia**

  Le attività di download degli aggiornamenti nei dispositivi client e negli Administration Server secondari vengono avviate solo una volta che gli aggiornamenti sono stati copiati dalla cartella degli aggiornamenti principale nelle cartelle degli aggiornamenti aggiuntive.

  Questa opzione deve essere abilitata se i dispositivi client e gli Administration Server secondari scaricano gli aggiornamenti da cartelle di rete aggiuntive.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica gli aggiornamenti utilizzando lo schema precedente**

A partire dalla versione 14, Kaspersky Security Center scarica gli aggiornamenti dei database e dei moduli software utilizzando il nuovo schema. Affinché l'applicazione possa scaricare gli aggiornamenti utilizzando il nuovo schema, la sorgente degli aggiornamenti deve contenere i file di aggiornamento con i metadati compatibili con il nuovo schema. Se la sorgente degli aggiornamenti contiene i file di aggiornamento con i metadati compatibili solo con lo schema precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**. In caso contrario, l'attività di download degli aggiornamenti avrà esito negativo.

È ad esempio necessario abilitare questa opzione quando una cartella locale o di rete è specificata come sorgente degli aggiornamenti e i file di aggiornamento in questa cartella sono stati scaricati da una delle seguenti applicazioni:

- Kaspersky Update Utility

  Questa utilità scarica gli aggiornamenti utilizzando lo schema precedente.

- Kaspersky Security Center 13.2 o versione precedente

  Ad esempio, Administration Server 1 non dispone di una connessione Internet. In questo caso, è possibile scaricare gli aggiornamenti utilizzando un Administration Server 2 dotato di una connessione Internet, quindi posizionare gli aggiornamenti in una cartella locale o di rete per utilizzarlo come sorgente degli aggiornamenti per Administration Server 1. Se Administration Server 2 dispone della versione 13.2 ò precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente** nell'attività per Administration Server 1.

Per impostazione predefinita, questa opzione è disabilitata.

5. Nella pagina **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N settimane**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

  - **Settimanale**

    L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  > Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- **Durante un'epidemia di virus**

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

- Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
- Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

  Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
- Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

6. Nella pagina **Definire il nome dell'attività** della procedura guidata specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

7. Nella pagina **Completare la creazione dell'attività** della procedura guidata fare clic sul pulsante **Fine** per chiudere la procedura guidata.

   Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Al termine della procedura guidata, l'attività **Scarica aggiornamenti nell'archivio di Administration Server** viene visualizzata nell'elenco delle attività di Administration Server nell'area di lavoro.

Oltre alle impostazioni specificate durante la creazione dell'attività, è possibile modificare altre proprietà di un'attività creata.

Quando Administration Server esegue l'attività *Scarica aggiornamenti nell'archivio di Administration Server*, gli aggiornamenti dei database e dei moduli software vengono scaricati dalla sorgente degli aggiornamenti e archiviati nella cartella condivisa di Administration Server. Se questa attività viene creata per un gruppo di amministrazione, verrà applicata solo ai Network Agent inclusi nel gruppo di amministrazione specificato.

Gli aggiornamenti vengono distribuiti nei dispositivi client e negli Administration Server secondari dalla cartella condivisa di Administration Server.

Creazione dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

I dispositivi dei punti di distribuzione che eseguono macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky.

Se uno o più dispositivi che eseguono macOS rientrano nell'ambito dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'attività viene completata con lo stato *Non riuscito*, anche se è stata completata correttamente in tutti i dispositivi Windows.

È possibile creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per un gruppo di amministrazione. L'attività verrà eseguita per i punti di distribuzione inclusi nel gruppo di amministrazione specificato.

È ad esempio possibile utilizzare questa attività se il costo del traffico tra l'Administration Server e i punti di distribuzione è superiore rispetto a quello del traffico tra i punti di distribuzione e i server di aggiornamento Kaspersky oppure se l'Administration Server non dispone di accesso a Internet. Se il punto di distribuzione si connette a Internet utilizzando un server proxy, è necessario specificare le impostazioni corrispondenti nel criterio di Network Agent.

Per creare l'attività Scarica aggiornamenti negli archivi dei punti di distribuzione per un gruppo di amministrazione selezionato:

1. Nella struttura della console selezionare la cartella **Attività**.

2. Nell'area di lavoro di questa cartella fare clic sul pulsante **Nuova attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

3. Nella pagina **Selezionare il tipo di attività** della procedura guidata selezionare il nodo **Kaspersky Security Center Administration Server**, espandere la cartella **Avanzate**, quindi selezionare l'attività **Scarica aggiornamenti negli archivi dei punti di distribuzione**.

4. Nella pagina **Impostazioni** della procedura guidata specificare le impostazioni dell'attività nel modo seguente:

- **Sorgenti degli aggiornamenti**

  È possibile utilizzare le seguenti risorse come sorgenti degli aggiornamenti per il punto di distribuzione:

  - Server degli aggiornamenti Kaspersky

    I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.

    Questa opzione è selezionata per impostazione predefinita.

  - Cartella locale o di rete

    Un'unità locale o una cartella di rete che contiene gli aggiornamenti più recenti. Una cartella di rete può essere un server FTP o HTTP oppure una condivisione SMB. Se una cartella di rete richiede l'autenticazione, è supportato solo il protocollo SMB. Quando si seleziona una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server.

    > Una cartella di rete o un server FTP o HTTP utilizzato da una sorgente degli aggiornamenti deve contenere una struttura di cartelle (con gli aggiornamenti) che corrisponde alla struttura creata durante l'utilizzo dei server di aggiornamento Kaspersky.

- **Cartella per l'archiviazione degli aggiornamenti**

  Il percorso della cartella specificata per l'archiviazione degli aggiornamenti salvati. È possibile copiare il percorso della cartella specificata negli appunti. Non è possibile modificare il percorso di una cartella specificata per un'attività di gruppo.

- **Scarica gli aggiornamenti utilizzando lo schema precedente**

  A partire dalla versione 14, Kaspersky Security Center scarica gli aggiornamenti dei database e dei moduli software utilizzando il nuovo schema. Affinché l'applicazione possa scaricare gli aggiornamenti utilizzando il nuovo schema, la sorgente degli aggiornamenti deve contenere i file di aggiornamento con i metadati compatibili con il nuovo schema. Se la sorgente degli aggiornamenti contiene i file di aggiornamento con i metadati compatibili solo con lo schema precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**. In caso contrario, l'attività di download degli aggiornamenti avrà esito negativo.

  È ad esempio necessario abilitare questa opzione quando una cartella locale o di rete è specificata come sorgente degli aggiornamenti e i file di aggiornamento in questa cartella sono stati scaricati da una delle seguenti applicazioni:

  - Kaspersky Update Utility

    Questa utilità scarica gli aggiornamenti utilizzando lo schema precedente.

  - Kaspersky Security Center 13.2 o versione precedente

    Un punto di distribuzione è ad esempio configurato per acquisire gli aggiornamenti da una cartella locale o di rete. In questo caso, è possibile scaricare gli aggiornamenti utilizzando un Administration Server dotato di una connessione Internet, quindi posizionare gli aggiornamenti nella cartella locale nel punto di distribuzione. Se la versione di Administration Server è la 13.2 o precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente** nell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

  Per impostazione predefinita, questa opzione è disabilitata.

5. Nella pagina **Selezionare un gruppo di amministrazione** della procedura guidata fare clic su **Sfoglia** e selezionare il gruppo di amministrazione a cui si applica l'attività.

6. Nella pagina **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N settimane**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

  - **Settimanale**

    L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- **Durante un'epidemia di virus**

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

- Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
- Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

  Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
- Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

7. Nella pagina **Definire il nome dell'attività** della procedura guidata specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

8. Nella pagina **Completare la creazione dell'attività** della procedura guidata fare clic sul pulsante **Fine** per chiudere la procedura guidata.

   Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Al termine della procedura guidata, **Scarica aggiornamenti negli archivi dei punti di distribuzione** compare nell'elenco delle attività di Network Agent nel gruppo di amministrazione di destinazione e nell'area di lavoro **Attività** della console.

Oltre alle impostazioni specificate durante la creazione dell'attività, è possibile modificare altre proprietà di un'attività creata.

Quando si esegue l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, gli aggiornamenti dei database e dei moduli software vengono scaricati dalla sorgente degli aggiornamenti e archiviati nella cartella condivisa. Gli aggiornamenti scaricati verranno utilizzati solo dai punti di distribuzione inclusi nel gruppo di amministrazione specificato e che non hanno alcuna attività di download degli aggiornamenti esplicitamente configurata.

Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni** selezionare **Punti di distribuzione**. Nelle proprietà di ciascun punto di distribuzione, nella sezione **Sorgente degli aggiornamenti** è possibile specificare la sorgente degli aggiornamenti (**Recupera da Administration Server** o **Usa attività per il download forzato degli aggiornamenti**). Per impostazione predefinita, è selezionata l'opzione **Recupera da Administration Server** per un punto di distribuzione assegnato automaticamente o manualmente. Tali punti di distribuzione utilizzeranno i risultati dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

Le proprietà di ogni punto di distribuzione specificano la cartella di rete che è stata configurata per tale punto di distribuzione singolarmente. I nomi delle cartelle possono variare per diversi punti di distribuzione. Per questo motivo, non è consigliabile modificare la cartella di rete nelle proprietà dell'attività se l'attività viene creata per un gruppo di dispositivi.

Se si sta creando un'attività locale per un dispositivo, è possibile modificare la cartella di rete con gli aggiornamenti nelle proprietà dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

Configurazione dell'attività Scarica aggiornamenti nell'archivio di Administration Server

Per configurare l'attività Scarica aggiornamenti nell'archivio di Administration Server:

1. Nell'area di lavoro della cartella **Attività** della struttura della console selezionare **Scarica aggiornamenti nell'archivio dell'Administration Server** nell'elenco delle attività.

2. Aprire la finestra delle proprietà dell'attività in uno dei seguenti modi:

   - Selezionando **Proprietà** nel menu di scelta rapida dell'attività.

   - Facendo clic sul collegamento **Configura attività** nella finestra di informazioni dell'attività selezionata.

   Verrà visualizzata la finestra delle proprietà dell'attività *Scarica aggiornamenti nell'archivio di Administration Server*. In questa finestra è possibile configurare il modo in cui gli aggiornamenti vengono scaricati nell'archivio di Administration Server.

Verifica degli aggiornamenti scaricati

Prima di installare gli aggiornamenti nei dispositivi gestiti, è possibile verificare la possibilità di utilizzare gli aggiornamenti e gli eventuali errori tramite l'attività *Verifica aggiornamenti*. L'attività di *Verifica aggiornamentii* viene eseguita automaticamente nell'ambito dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Administration Server scarica gli aggiornamenti dalla sorgente, li salva nell'archivio temporaneo ed esegue l'attività *Verifica aggiornamenti*. Se l'attività viene completata correttamente, gli aggiornamenti sono copiati dall'archivio temporaneo nella cartella condivisa di Administration Server (<cartella di installazione di Kaspersky Security Center>\Share\Updates). Vengono distribuiti a tutti i dispositivi client per cui l'Administration Server opera come sorgente degli aggiornamenti.

Se i risultati dell'attività *Verifica aggiornamenti* mostrano che gli aggiornamenti presenti nell'archivio temporaneo non sono corretti o se l'attività *Verifica aggiornamenti* viene completata con un errore, gli aggiornamenti non vengono copiati nella cartella condivisa. L'Administration Server mantiene il set di aggiornamenti precedente. Inoltre, le attività con il tipo di pianificazione **Quando vengono scaricati nuovi aggiornamenti nell'archivio** non vengono avviate. Tali operazioni vengono eseguite al successivo avvio dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, se la scansione dei nuovi aggiornamenti viene completata correttamente.

Un set di aggiornamenti è considerato non valido se viene soddisfatta una delle seguenti condizioni in almeno un dispositivo di test:

- Si è verificato un errore dell'attività di aggiornamento.

- Lo stato della protezione in tempo reale dell'applicazione di protezione è cambiato dopo l'applicazione degli aggiornamenti.

- È stato rilevato un oggetto infetto durante l'esecuzione dell'attività di scansione su richiesta.

- Si è verificato un errore di runtime di un'applicazione Kaspersky.

Se nei dispositivi di test non si verifica alcuna delle condizioni elencate, il set di aggiornamenti viene considerato valido e l'attività *Verifica aggiornamenti* viene considerata completata correttamente.

Prima di iniziare a creare l'attività *Verifica aggiornamenti*, eseguire i prerequisiti:

1. Creare un gruppo di amministrazione con diversi dispositivi di test. Sarà necessario questo gruppo per verificare i relativi aggiornamenti.

   È consigliabile utilizzare dispositivi con il livello di protezione più affidabile e con la configurazione delle applicazioni più diffusa nella rete. Questo approccio aumenta la qualità e la probabilità di rilevamento dei virus durante le scansioni e riduce al minimo il rischio di falsi positivi. Se vengono rilevati virus nei dispositivi di test, l'attività *Verifica aggiornamenti* viene considerata non riuscita.

2. Creare le attività *Aggiorna* e *Scansione malware* per un'applicazione supportata da Kaspersky Security Center, ad esempio Kaspersky Endpoint Security for Windows o Kaspersky Security for Windows Server. Quando si creano le attività *Aggiorna* e *Scansione malware*, specificare il gruppo di amministrazione con i dispositivi di test.

   L'attività *Verifica aggiornamenti* esegue in sequenza le attività *Aggiorna* e *Scansione malware* nei dispositivi di test per verificare che tutti gli aggiornamenti siano validi. Inoltre, durante la creazione dell'attività *Verifica aggiornamenti*, è necessario specificare le attività *Aggiorna* e *Scansione malware*.

3. Creare l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*.

Per fare in modo che Kaspersky Security Center verifichi gli aggiornamenti scaricati prima di distribuirli ai dispositivi client:

1. Nell'area di lavoro della cartella **Attività** selezionare l'attività Scarica aggiornamenti nell'*Scarica aggiornamenti nell'archivio dell'Administration Server* nell'elenco delle attività.

2. Aprire la finestra delle proprietà dell'attività in uno dei seguenti modi:

   - Selezionando **Proprietà** nel menu di scelta rapida dell'attività.

   - Facendo clic sul collegamento **Configura attività** nella finestra di informazioni dell'attività selezionata.

3. Se l'attività di *Verifica aggiornamenti* esiste, fare clic sul pulsante **Sfoglia**. Nella finestra visualizzata selezionare l'attività *Verifica aggiornamenti* nel gruppo di amministrazione con dispositivi di test.

4. Se non è stata creata l'attività di *Verifica aggiornamenti* in precedenza, fare clic sul pulsante **Crea**.

   Verrà avviata la Creazione guidata attività di *Verifica aggiornamenti*. Seguire le istruzioni della procedura guidata.

5. Fare clic su **OK** per chiudere la finestra delle proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*.

La verifica automatica degli aggiornamenti è abilitata. Adesso è possibile eseguire l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, che inizierà dalla verifica degli aggiornamenti.

Configurazione di criteri di test e attività ausiliarie

Durante la creazione di un'attività *Verifica aggiornamenti*, Administration Server genera criteri di test, attività ausiliarie di aggiornamento di gruppo e attività di scansione su richiesta.

Le attività ausiliarie di aggiornamento di gruppo e le attività di scansione su richiesta richiedono alcuni minuti. Queste attività vengono eseguite durante l'esecuzione dell'attività *Verifica aggiornamenti*. L'attività *Verifica aggiornamenti* viene eseguita durante l'esecuzione dell'attività *Scarica aggiornamenti nell'archivio*. La durata dell'attività *Scarica aggiornamenti nell'archivio* comprende anche le attività ausiliarie di aggiornamento di gruppo e le attività di scansione su richiesta.

È possibile modificare le impostazioni dei criteri di testo e delle attività ausiliarie.

Per modificare le impostazioni di un criterio di testo o di un'attività ausiliaria:

1. Nella struttura della console selezionare un gruppo per cui è stata creata l'attività *Verifica aggiornamenti*.
2. Nell'area di lavoro del gruppo selezionare una delle seguenti schede:
   - **Criteri**, se si desidera modificare le impostazioni dei criteri di test.
   - **Attività**, se si desidera modificare le impostazioni delle attività ausiliarie.
3. Nell'area di lavoro della scheda selezionare un criterio o un'attività di cui si desidera modificare le impostazioni.
4. Aprire la finestra delle proprietà del criterio (attività) in uno dei seguenti modi:
   - Selezionando **Proprietà** nel menu di scelta rapida del criterio (attività).
   - Facendo clic sul collegamento **Configura criterio** (**Configura attività**) nella finestra di informazioni per il criterio selezionato (attività).

Per verificare correttamente gli aggiornamenti, impostare le seguenti limitazioni alla modifica dei criteri di test e delle attività ausiliarie:

- Nelle impostazioni delle attività ausiliarie:
  - Salvare tutte le attività con livelli di importanza **Evento critico** ed **Errore funzionale** in Administration Server. Utilizzando questo tipo di eventi, Administration Server analizza l'esecuzione delle applicazioni.
  - Utilizzare Administration Server come sorgente degli aggiornamenti.
  - Specificare il tipo di pianificazione dell'attività: **Manualmente**.
- Nelle impostazioni dei criteri di test:
  - Disabilitare le tecnologie di accelerazione della scansione iChecker e iSwift (**Protezione minacce essenziale → Protezione minacce file → Impostazioni → Avanzate → Tecnologie di scansione**).
  - Selezionare le azioni da eseguire sugli oggetti infetti: **Disinfetta; elimina se la disinfezione fallisce** / **Disinfetta; blocca se la disinfezione fallisce** / **Blocca**. (**Protezione minacce essenziale → Protezione minacce file → Azione se viene rilevata una minaccia**).
- Nelle impostazioni dei criteri di test e delle attività ausiliarie:

  Se è necessario il riavvio del dispositivo dopo l'installazione degli aggiornamenti dei moduli software, questo deve essere eseguito immediatamente. Se il dispositivo non viene riavviato, non è possibile testare questo tipo di aggiornamenti. Per alcune applicazioni, l'installazione di aggiornamenti che richiedono un riavvio potrebbe essere proibita o configurata in modo da richiedere la conferma dell'utente. Queste limitazioni dovrebbero essere disabilitate nelle impostazioni dei criteri di test e delle attività ausiliarie.

Visualizzazione degli aggiornamenti scaricati

Per visualizzare l'elenco degli aggiornamenti scaricati:

Nella struttura della console selezionare la sottocartella **Aggiornamenti per database e moduli software Kaspersky** nella cartella **Archivi**.

L'area di lavoro della cartella **Aggiornamenti per database e moduli software Kaspersky** mostra l'elenco degli aggiornamenti salvati in Administration Server.

Installazione automatica degli aggiornamenti di Kaspersky Endpoint Security nei dispositivi

È possibile configurare gli aggiornamenti automatici dei database e dei moduli software di Kaspersky Endpoint Security nei dispositivi client.

Per configurare il download e l'installazione automatica degli aggiornamenti di Kaspersky Endpoint Security nei dispositivi client:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Creare un'attività **Aggiornamento** in uno dei seguenti modi:
   - Selezionando **Nuovo → Attività** nel menu di scelta rapida della cartella **Attività** nella struttura della console.
   - Facendo clic sul pulsante **Nuova attività** nell'area di lavoro della cartella **Attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Nella pagina **Selezionare il tipo di attività** della procedura guidata selezionare **Kaspersky Endpoint Security** come tipo di attività, quindi selezionare **Aggiornamento** come sottotipo di attività.
4. Seguire le rimanenti istruzioni della procedura guidata.

   Al termine della procedura guidata, verrà creata un'attività di aggiornamento per Kaspersky Endpoint Security. L'attività creata viene visualizzata nell'elenco di attività nell'area di lavoro della cartella **Attività**.
5. Nell'area di lavoro della cartella **Attività** selezionare un'attività di aggiornamento creata.
6. Dal menu di scelta rapida dell'attività selezionare **Proprietà**.
7. Nella finestra delle proprietà dell'attività visualizzata, nel riquadro **Sezioni**, selezionare **Opzioni**.

   Nella sezione **Opzioni** è possibile definire le impostazioni dell'attività di aggiornamento in modalità locale o mobile:
   - **Impostazioni di aggiornamento per la modalità locale**: viene stabilita la connessione tra il dispositivo e Administration Server.
   - **Impostazioni di aggiornamento per la modalità mobile**: non viene stabilita alcuna connessione tra Kaspersky Security Center e il dispositivo (ad esempio, quando il dispositivo non è connesso a Internet).
8. Fare clic sul pulsante **Impostazioni** per selezionare la sorgente degli aggiornamenti.
9. Selezionare l'opzione **Scarica gli aggiornamenti dei moduli dell'applicazione** per scaricare e installare gli aggiornamenti dei moduli software oltre ai database dell'applicazione.

   Se la casella di controllo è selezionata, Kaspersky Endpoint Security invia una notifica all'utente per informarlo degli aggiornamenti dei moduli software disponibili e include gli aggiornamenti dei moduli software nel pacchetto di aggiornamento durante l'esecuzione dell'attività di aggiornamento. Configurare l'utilizzo dei moduli di aggiornamento:
   - **Installa gli aggiornamenti critici e approvati**. Se sono disponibili aggiornamenti per i moduli software, Kaspersky Endpoint Security li installa automaticamente con lo stato *Critico*. Gli aggiornamenti rimanenti saranno installati dopo essere stati approvati dall'amministratore.
   - **Installa solo gli aggiornamenti approvati**. Se sono disponibili aggiornamenti per i moduli software, Kaspersky Endpoint Security li installa una volta che la relativa installazione è stata approvata. Saranno installati in locale tramite l'interfaccia dell'applicazione o mediante Kaspersky Security Center.

   Se l'aggiornamento dei moduli software richiede la visualizzazione e l'accettazione delle condizioni del Contratto di licenza e dell'Informativa sulla privacy, l'applicazione installa gli aggiornamenti dopo che le condizioni del Contratto di licenza e dell'Informativa sulla privacy sono state accettate dall'utente.

10. Selezionare l'opzione **Copia aggiornamenti nella cartella** per fare in modo che l'applicazione salvi gli aggiornamenti scaricati in una cartella, quindi fare clic sul pulsante **Sfoglia** per specificare la cartella.

11. Fare clic su **OK**.

Quando è in esecuzione l'attività **Aggiornamento**, l'applicazione invia richieste ai server di aggiornamento Kaspersky.

Alcuni aggiornamenti richiedono l'installazione delle versioni più recenti dei plug-in di gestione.

Modello offline per il download degli aggiornamenti

Network Agent nei dispositivi gestiti talvolta potrebbero non connettersi ad Administration Server per ricevere gli aggiornamenti. Ad esempio, un Network Agent potrebbe essere stato installato in un computer portatile che a volte non dispone di una connessione Internet e dell'accesso alla rete locale. Inoltre, l'amministratore può limitare il tempo per la connessione dei dispositivi alla rete. In questi casi, Network Agent non possono ricevere gli aggiornamenti dall'Administration Server in base alla pianificazione esistente. Se è stato configurato l'aggiornamento di applicazioni gestite (ad esempio, Kaspersky Endpoint Security) tramite Network Agent, ogni aggiornamento richiede una connessione all'Administration Server. Quando non viene stabilita la connessione tra Network Agent e l'Administration Server, l'aggiornamento non è possibile. È possibile configurare la connessione tra Network Agent e l'Administration Server in modo che Network Agent si connetta all'Administration Server a intervalli di tempo specificati. Nel caso peggiore, se gli intervalli di connessione specificati corrispondono a periodi in cui la connessione non è disponibile, i database non saranno mai aggiornati. Inoltre, possono verificarsi problemi quando più applicazioni gestite tentano di accedere contemporaneamente all'Administration Server per ricevere gli aggiornamenti. In questo caso, l'Administration Server può smettere di rispondere alle richieste (in modo simile a un attacco DDoS).

Per evitare problemi di questo tipo, in Kaspersky Security Center è implementato un modello offline per il download degli aggiornamenti e dei moduli delle applicazioni gestite. Questo modello offre un meccanismo per la distribuzione degli aggiornamenti, indipendentemente dai problemi temporanei causati dall'inaccessibilità dei canali di comunicazione di Administration Server. Il modello consente inoltre di ridurre il carico sull'Administration Server.

Funzionamento del modello offline per il download degli aggiornamenti

Quando Administration Server riceve gli aggiornamenti, segnala a Network Agent (nei dispositivi in cui è installato) gli aggiornamenti che saranno necessari per le applicazioni gestite. Quando Network Agent riceve le informazioni su questi aggiornamenti, scarica anticipatamente i file appropriati da Administration Server. Alla prima connessione con Network Agent, Administration Server avvia un download degli aggiornamenti. Una volta che Network Agent ha scaricato tutti gli aggiornamenti in un dispositivo client, tali aggiornamenti diventano disponibili per le applicazioni nel dispositivo.

Quando un'applicazione gestita in un dispositivo client tenta di accedere a Network Agent per gli aggiornamenti, questo Network Agent verifica se dispone di tutti gli aggiornamenti richiesti. Se gli aggiornamenti sono stati ricevuti da Administration Server non più di 25 ore prima del momento in cui vengono richiesti dall'applicazione gestita, il Network Agent non si connette ad Administration Server, ma fornisce all'applicazione gestita gli aggiornamenti dalla cache locale. La connessione con Administration Server potrebbe non essere stabilita quando Network Agent fornisce gli aggiornamenti alle applicazioni nei dispositivi client, ma la connessione non è necessaria per l'aggiornamento.

Per distribuire il carico sull'Administration Server, Network Agent si connette all'Administration Server e scarica gli aggiornamenti in ordine casuale durante l'intervallo di tempo specificato dall'Administration Server. Questo intervallo di tempo dipende dal numero di dispositivi con Network Agent installato che scaricano aggiornamenti e dalle dimensioni di tali aggiornamenti. Per ridurre il carico sull'Administration Server, è possibile utilizzare Network Agent come punti di distribuzione.

Se il modello offline di download degli aggiornamenti è disabilitato, gli aggiornamenti vengono distribuiti in base alla pianificazione dell'attività di download degli aggiornamenti.

Per impostazione predefinita, il modello offline per il download degli aggiornamenti è abilitato.

Il modello offline per il download degli aggiornamenti viene utilizzato solo con i dispositivi gestiti in cui per l'attività di recupero degli aggiornamenti da parte delle applicazioni gestite è selezionato il tipo di pianificazione **Quando vengono scaricati nuovi aggiornamenti nell'archivio**. Per altri dispositivi gestiti, viene utilizzato lo schema standard per il recupero degli aggiornamenti da Administration Server in tempo reale.

È consigliabile disabilitare il modello offline per il download degli aggiornamenti utilizzando le impostazioni dei criteri di Network Agent per i gruppi di amministrazione appropriati nei seguenti casi: qualora per le applicazioni gestite sia impostato il recupero degli aggiornamenti dai server di Kaspersky o da una cartella di rete (invece che da Administration Server) e se per l'attività di download degli aggiornamenti è selezionato il tipo di pianificazione **Quando vengono scaricati nuovi aggiornamenti nell'archivio**.

Abilitazione e disabilitazione del modello offline per il download degli aggiornamenti

È consigliabile evitare di disabilitare il modello offline per il download degli aggiornamenti. Se viene disabilitato possono verificarsi errori durante l'invio degli aggiornamenti ai dispositivi. In alcuni casi è possibile che uno specialista del Servizio di assistenza tecnica di Kaspersky consigli di deselezionare la casella di controllo **Scarica aggiornamenti e database anti-virus da Administration Server anticipatamente**. Sarà quindi necessario accertarsi che l'attività per la ricezione degli aggiornamenti per le applicazioni Kaspersky sia stata configurata.

Per abilitare o disabilitare il modello offline per il download degli aggiornamenti per un gruppo di amministrazione:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui è necessario abilitare il modello offline per il download degli aggiornamenti.
2. Nell'area di lavoro del gruppo aprire la scheda **Criteri**.
3. Nella scheda **Criteri** selezionare il criterio di Network Agent.
4. Nel menu di scelta rapida del criterio selezionare **Proprietà**.

   Aprire la finestra delle proprietà del criterio di Network Agent.
5. Nella finestra delle proprietà del criterio selezionare la sezione **Gestire patch e aggiornamenti**.
6. Selezionare o deselezionare la casella di controllo **Scarica aggiornamenti e database anti-virus da Administration Server anticipatamente (scelta consigliata)** per abilitare o disabilitare, rispettivamente, il modello offline di download degli aggiornamenti.

   Per impostazione predefinita, il modello offline per il download degli aggiornamenti è abilitato.

Il modello offline per il download degli aggiornamenti verrà abilitato o disabilitato.

Installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center

Per impostazione predefinita, gli aggiornamenti e le patch scaricati e installati automaticamente per i seguenti componenti dell'applicazione:

- Network Agent per Windows
- Administration Console
- Server per dispositivi mobili MDM iOS

L'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center è disponibile solo per i dispositivi che eseguono Windows. È possibile disabilitare l'installazione automatica di aggiornamenti e patch per questi componenti. In questo caso, tutti gli aggiornamenti e le patch scaricati verranno installati solo dopo l'impostazione dello stato su *Approvato*. Gli aggiornamenti e le patch con lo stato *Indefinito* non verranno installati.

Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center

L'installazione automatica degli aggiornamenti e delle patch per i componenti di Kaspersky Security Center è abilitata per impostazione predefinita durante l'installazione di Network Agent nel dispositivo. È possibile disabilitarla durante l'installazione di Network Agent o disabilitarla in un secondo momento utilizzando un criterio.

Per disabilitare l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center durante l'installazione locale di Network Agent in un dispositivo:

1. Avviare l'installazione locale di Network Agent nel dispositivo.
2. Durante il passaggio **Impostazioni avanzate** deselezionare la casella di controllo **Installa automaticamente gli aggiornamenti applicabili e le patch per i componenti con stato Indefinito**.
3. Seguire le istruzioni della procedura guidata.

Nel dispositivo verrà installato Network Agent con l'installazione automatica di aggiornamenti e patch disabilitata per i componenti di Kaspersky Security Center. È possibile abilitare l'installazione automatica di aggiornamenti e patch in un secondo momento utilizzando un criterio.

Per disabilitare l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center durante l'installazione di Network Agent nel dispositivo tramite un pacchetto di installazione:

1. Nella struttura della console selezionare la cartella **Installazione remota → Pacchetti di installazione**.
2. Nel menu di scelta rapida del pacchetto **Kaspersky Security Center Network Agent <numero di versione>** selezionare **Proprietà**.
3. Nelle proprietà del pacchetto di installazione, nella sezione **Impostazioni** deselezionare la casella di controllo **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito**.

Network Agent con l'installazione automatica di aggiornamenti e patch disabilitata per i componenti di Kaspersky Security Center verrà installato da questo pacchetto. È possibile abilitare l'installazione automatica di aggiornamenti e patch in un secondo momento utilizzando un criterio.

Se questa casella di controllo è stata selezionata o deselezionata durante l'installazione di Network Agent nel dispositivo, successivamente è possibile abilitare (o disabilitare) l'aggiornamento automatico utilizzando il criterio di Network Agent.

Per abilitare o disabilitare l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center utilizzando il criterio di Network Agent:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui è necessario abilitare o disabilitare l'installazione automatica di aggiornamenti e patch.
2. Nell'area di lavoro del gruppo aprire la scheda **Criteri**.
3. Nella scheda **Criteri** selezionare il criterio di Network Agent.
4. Nel menu di scelta rapida del criterio selezionare **Proprietà**.

   Aprire la finestra delle proprietà del criterio di Network Agent.
5. Nella finestra delle proprietà del criterio selezionare la sezione **Gestire patch e aggiornamenti**.
6. Selezionare o deselezionare la casella di controllo **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito** per abilitare o disabilitare, rispettivamente, l'applicazione automatica di patch e aggiornamenti.
7. Impostare il lucchetto per questa casella di controllo.

Il criterio verrà applicato ai dispositivi selezionati e l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center verrà abilitata (o disabilitata) in tali dispositivi.

Distribuzione automatica degli aggiornamenti

Kaspersky Security Center consente la distribuzione e l'installazione automatica degli aggiornamenti nei dispositivi client e negli Administration Server secondari.

Distribuzione automatica degli aggiornamenti ai dispositivi client

Per distribuire automaticamente gli aggiornamenti dell'applicazione selezionata ai dispositivi client subito dopo che vengono scaricati nell'archivio di Administration Server:

1. Eseguire la connessione ad Administration Server che gestisce i dispositivi client.
2. Creare un'attività di distribuzione degli aggiornamenti per i dispositivi client selezionati in uno dei seguenti modi:
   - Se è necessario distribuire gli aggiornamenti ai dispositivi client che appartengono a un gruppo di amministrazione selezionato, creare un'attività per il gruppo selezionato.
   - Se è necessario distribuire gli aggiornamenti ai dispositivi client che appartengono ad altri gruppi di amministrazione o che non appartengono ad alcun gruppo, creare un'attività per dispositivi specifici.

   Verrà avviata la Creazione guidata nuova attività. Seguire le relative istruzioni ed eseguire le azioni seguenti:

   a. Nella finestra della procedura guidata **Tipo di attività**, nel nodo dell'applicazione desiderata, selezionare l'attività di distribuzione degli aggiornamenti.

      Il nome dell'attività di distribuzione degli aggiornamenti visualizzato nella finestra **Tipo di attività** dipende dall'applicazione per cui si crea tale attività. Per informazioni dettagliate sui nomi delle attività di aggiornamento per le applicazioni Kaspersky selezionate, vedere la Guida corrispondente.

   b. Nella finestra della procedura guidata **Pianificazione**, nel campo **Avvio pianificato**, selezionare **Quando vengono scaricati nuovi aggiornamenti nell'archivio**.

   La nuova attività di distribuzione degli aggiornamenti creata verrà avviata per i dispositivi selezionati ogni volta che gli aggiornamenti vengono scaricati nell'archivio di Administration Server.

Se è già stata creata un'attività di distribuzione degli aggiornamenti per l'applicazione desiderata per dispositivi selezionati, per distribuire automaticamente gli aggiornamenti ai dispositivi client, nella sezione **Pianificazione** della finestra delle proprietà dell'attività selezionare l'opzione di avvio **Quando vengono scaricati nuovi aggiornamenti nell'archivio** nel campo **Avvio pianificato**.

Distribuzione automatica degli aggiornamenti agli Administration Server secondari

Per distribuire gli aggiornamenti dell'applicazione selezionata agli Administration Server secondari subito dopo che questi vengono scaricati nell'archivio dell'Administration Server primario:

1. Nella struttura della console, nel nodo dell'Administration Server primario, selezionare la cartella **Attività**.
2. Nell'elenco delle attività nell'area di lavoro selezionare l'attività di Administration Server Scarica aggiornamenti nell'archivio di Administration Server.

3. Aprire la sezione **Impostazioni** dell'attività selezionata in uno dei seguenti modi:

   - Selezionando **Proprietà** nel menu di scelta rapida dell'attività.
   - Facendo clic sul collegamento **Modifica impostazioni** nella finestra di informazioni dell'attività selezionata.

4. Nella sezione **Impostazioni** della finestra delle proprietà dell'attività selezionare **Altre impostazioni**, quindi fare clic sul collegamento **Configura**.

5. Nella finestra **Altre impostazioni** visualizzata selezionare la casella di controllo **Forza aggiornamento degli Administration Server secondari**.

6. Nelle impostazioni dell'attività di download degli aggiornamenti di Administration Server, nella scheda **Impostazioni** della finestra delle proprietà dell'attività, selezionare la casella di controllo **Forza aggiornamento degli Administration Server secondari**.

Dopo che l'Administration Server primario recupera gli aggiornamenti, le attività di download degli aggiornamenti verranno avviate automaticamente negli Administration Server secondari, indipendentemente dalla relativa pianificazione.

L'Administration Server primario aggiorna i database anti-virus in base alle applicazioni installate negli Administration Server secondari. Non è richiesta l'installazione di plug-in aggiuntivi né la creazione di pacchetti di installazione nell'Administration Server primario.

Assegnazione automatica di punti di distribuzione

È consigliabile assegnare automaticamente i punti di distribuzione. Kaspersky Security Center selezionerà autonomamente a quali dispositivi assegnare i punti di distribuzione.

Per assegnare automaticamente i punti di distribuzione:

1. Aprire la finestra principale dell'applicazione.

2. Nella struttura della console selezionare il nodo con il nome dell'Administration Server per cui si desidera assegnare automaticamente i punti di distribuzione.

3. Dal menu di scelta rapida di Administration Server fare clic su **Proprietà**.

4. Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni** selezionare **Punti di distribuzione**.

5. Nella parte destra della finestra selezionare l'opzione **Assegna i punti di distribuzione automaticamente**.

   Se è abilitata l'assegnazione automatica dei dispositivi come punti di distribuzione, non è possibile configurare i punti di distribuzione manualmente, né modificare l'elenco dei punti di distribuzione.

6. Fare clic su **OK**.

Administration Server assegna e configura i punti di distribuzione automaticamente.

Assegnazione manuale di un punto di distribuzione a un dispositivo

Kaspersky Security Center consente di assegnare ai dispositivi il ruolo di punti di distribuzione.

È consigliabile assegnare automaticamente i punti di distribuzione. In questo caso, Kaspersky Security Center selezionerà autonomamente a quali dispositivi assegnare i punti di distribuzione. Tuttavia, se per qualche motivo non è possibile assegnare automaticamente i punti di distribuzione (se ad esempio si desidera utilizzare i server assegnati in modo esclusivo), è possibile assegnare i punti di distribuzione manualmente dopo averne calcolato il numero ed eseguito la configurazione.

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Per assegnare manualmente a un dispositivo il ruolo di punto di distribuzione:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server selezionare la sezione **Punti di distribuzione** e fare clic sul pulsante **Aggiungi**. Questo pulsante è disponibile se è stata selezionata l'opzione **Assegna i punti di distribuzione manualmente**.

   Verrà visualizzata la finestra **Aggiungi punto di distribuzione**.
4. Nella finestra **Aggiungi punto di distribuzione** eseguire le seguenti azioni:

   a. Selezionare un dispositivo che opererà come punto di distribuzione (selezionarne uno in un gruppo di amministrazione o specificare l'Indirizzo IP di un dispositivo). Quando si seleziona un dispositivo, tenere presenti le funzionalità operative dei punti di distribuzione e i requisiti definiti per il dispositivo che opera come punto di distribuzione.

   b. Indicare i dispositivi specifici a cui il punto di distribuzione distribuirà gli aggiornamenti. È possibile specificare un gruppo di amministrazione o una descrizione del percorso di rete.
5. Fare clic su **OK**.

   Il punto di distribuzione aggiunto sarà visualizzato nell'elenco dei punti di distribuzione, nella sezione **Punti di distribuzione**.

6. Selezionare il nuovo punto di distribuzione aggiunto nell'elenco e fare clic sul pulsante **Proprietà** per aprire la relativa finestra delle proprietà.

7. Configurare il punto di distribuzione nella finestra delle proprietà:

   - La sezione **Generale** contiene le impostazioni per l'interazione tra il punto di distribuzione e i dispositivi client.

     - **Porta SSL**

       Numero della porta SSL per la connessione criptata tra i dispositivi client e il punto di distribuzione tramite SSL.

       Per impostazione predefinita, viene utilizzata la porta 13000.

     - **Usa multicast**

       Se questa opzione è abilitata, verrà utilizzata la modalità IP multicast per la distribuzione automatica dei pacchetti di installazione ai dispositivi client del gruppo.

       Il multicast IP riduce il tempo necessario per installare un'applicazione da un pacchetto di installazione in un gruppo di dispositivi client, ma aumenta il tempo di installazione quando si installa un'applicazione in un singolo dispositivo client.

     - **Indirizzo IP multicast**

       Indirizzo IP che verrà utilizzato per la modalità multicast. È possibile definire un indirizzo IP nell'intervallo da 224.0.0.0 a 239.255.255.255

       Per impostazione predefinita Kaspersky Security Center assegna automaticamente un indirizzo IP multicast univoco all'interno dell'intervallo specificato.

     - **Numero di porta IP multicast**

       Numero di porta per la modalità IP multicast.

       Il numero di porta predefinito è 15001. Se il dispositivo in cui è installato Administration Server è specificato come punto di distribuzione, per impostazione predefinita viene utilizzata la porta 13001 per la connessione SSL.

     - **Distribuisci aggiornamenti**

Gli aggiornamenti vengono distribuiti ai dispositivi gestiti dalle seguenti sorgenti:

- Questo punto di distribuzione se l'opzione è abilitata.
- Altri punti di distribuzione, Administration Server o server degli aggiornamenti Kaspersky se l'opzione è disabilitata.

Se si utilizzano i punti di distribuzione per distribuire gli aggiornamenti, è possibile risparmiare traffico riducendo il numero di download. È inoltre possibile alleggerire il carico su Administration Server e ridistribuirlo tra i punti di distribuzione. È possibile calcolare il numero di punti di distribuzione per la propria rete in modo da ottimizzare il traffico e il carico.

Se si disabilita questa opzione, il numero di download degli aggiornamenti e il carico su Administration Server potrebbero aumentare. Per impostazione predefinita, questa opzione è abilitata.

- **Distribuisci pacchetti di installazione**

I pacchetti di installazione vengono distribuiti ai dispositivi gestiti dalle seguenti sorgenti:

- Questo punto di distribuzione se l'opzione è abilitata.
- Altri punti di distribuzione, Administration Server o server degli aggiornamenti Kaspersky se l'opzione è disabilitata.

Se si utilizzano i punti di distribuzione per distribuire i pacchetti di installazione, è possibile risparmiare traffico riducendo il numero di download. È inoltre possibile alleggerire il carico su Administration Server e ridistribuirlo tra i punti di distribuzione. È possibile calcolare il numero di punti di distribuzione per la propria rete in modo da ottimizzare il traffico e il carico.

Se si disabilita questa opzione, il numero di download dei pacchetti di installazione e il carico su Administration Server potrebbero aumentare. Per impostazione predefinita, questa opzione è abilitata.

- **Utilizzare questo punto di distribuzione come server push**

In Kaspersky Security Center un punto di distribuzione può fungere da server push per i dispositivi gestiti tramite il protocollo mobile. È ad esempio necessario abilitare un server push se si desidera forzare la sincronizzazione dei dispositivi KasperskyOS con Administration Server. Un server push ha lo stesso ambito dei dispositivi gestiti del punto di distribuzione in cui è abilitato il server push. Se sono stati assegnati più punti di distribuzione per lo stesso gruppo di amministrazione, è possibile abilitare il server push in ciascuno dei punti di distribuzione. In questo caso, Administration Server bilancia il carico tra i punti di distribuzione.

Se si gestiscono dispositivi in cui è installato KasperskyOS o si prevede di farlo, è necessario utilizzare un punto di distribuzione come server push. È inoltre possibile utilizzare un punto di distribuzione come server push se si desidera inviare notifiche push ai dispositivi client.

- **Porta server push**

La porta nel punto di distribuzione che i dispositivi client utilizzeranno per la connessione. Per impostazione predefinita, viene utilizzata la porta 13295.

- Nella sezione **Ambito** specificare l'ambito in cui il punto di distribuzione distribuirà gli aggiornamenti (gruppi di amministrazione e/o percorso di rete).

- Nella sezione **Proxy KSN** è possibile configurare l'applicazione per l'utilizzo del punto di distribuzione per l'inoltro delle richieste KSN dai dispositivi gestiti.

  - **Abilita proxy KSN da parte del punto di distribuzione**

    Il servizio proxy KSN viene eseguito nel dispositivo utilizzato come punto di distribuzione. Utilizzare questa funzionalità per ridistribuire e ottimizzare il traffico nella rete.

    Il punto di distribuzione invia le statistiche KSN, elencate nell'informativa di Kaspersky Security Network, a Kaspersky. Per impostazione predefinita, l'informativa KSN è disponibile in %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    Per impostazione predefinita, questa opzione è disabilitata. L'attivazione di questa opzione ha effetto solo se le opzioni **Usa Administration Server come server proxy** e **Accetto di utilizzare Kaspersky Security Network** sono abilitate nella finestra delle proprietà di Administration Server.

    È possibile assegnare il nodo di un cluster attivo-passivo a un punto di distribuzione e abilitare il proxy KSN in tale nodo.

  - **Inoltra richieste KSN ad Administration Server**

    Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti ad Administration Server.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Accedi a KSN Cloud/KPSN direttamente tramite Internet**

    Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti a KSN Cloud o KPSN. Anche le richieste KSN generate nello stesso punto di distribuzione vengono inviate direttamente a KSN Cloud o KPSN.

    I punti di distribuzione in cui è installato Network Agent versione 11 (o precedente) non possono accedere direttamente a KPSN. Se si desidera riconfigurare i punti di distribuzione per inviare richieste KSN a KPSN, abilitare l'opzione **Inoltra richieste KSN ad Administration Server** per ciascun punto di distribuzione.

    I punti di distribuzione in cui è installato Network Agent versione 12 (o successive) possono accedere direttamente a KPSN.

  - **Ignora impostazioni del server proxy durante la connessione a KPSN**

    Abilitare questa opzione se le impostazioni del server proxy sono configurate nelle proprietà del punto di distribuzione o nel criterio di Network Agent ma l'architettura di rete richiede l'utilizzo diretto di KPSN. In caso contrario, le richieste dalle applicazioni gestite non possono raggiungere KPSN.

    Questa opzione è disponibile se si seleziona l'opzione **Accedi a KSN Cloud/KPSN direttamente tramite Internet**.

  - **Porta TCP**

    Numero della porta TCP utilizzata dai dispositivi gestiti per la connessione al server proxy KSN. Il numero di porta predefinito è 13111.

  - **Porta UDP**

Se è necessario che Network Agent si connetta ad Administration server attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in **Porta UDP**. Per impostazione predefinita, questa opzione è abilitata. La porta UDP predefinita per la connessione ad Administration Server è 15000.

- **Porta HTTPS**

  Se è necessario che i dispositivi gestiti si connettano al server proxy KSN attraverso una porta HTTPS, abilitare l'opzione **Usa HTTPS** tramite porta e specificare il numero in **HTTPS tramite porta**. La porta HTTPS predefinita per la connessione al server proxy KSN è la 17111.

- Nella sezione **Device discovery** configurare il polling dei domini Windows, di Active Directory e degli intervalli IP da parte del punto di distribuzione.

  - **Domini Windows**

    È possibile abilitare la device discovery per i domini Windows e impostare la pianificazione per l'individuazione.

  - **Active Directory**

    È possibile abilitare il polling della rete per Active Directory e impostare la pianificazione per il polling.

    Se si utilizza un punto di distribuzione Windows, è possibile selezionare una delle seguenti opzioni:

    - **Esegui il polling del dominio Active Directory corrente**.
    - **Esegui il polling della foresta di dominio Active Directory**.
    - **Esegui il polling dei domini Active Directory selezionati**. Se si seleziona questa opzione, aggiungere uno o più domini Active Directory all'elenco.

    Se si utilizza un punto di distribuzione Linux con Network Agent versione 15 installato, è possibile eseguire il polling solo dei domini Active Directory per i quali si specificano l'indirizzo e le credenziali utente. Il polling del dominio Active Directory corrente e della foresta di domini Active Directory non è disponibile.

  - **Intervalli IP**

    Adesso è possibile abilitare Device discovery per gli intervalli IPv4 e le reti IPv6.

    Se si abilita l'opzione **Abilita polling intervallo**, è possibile aggiungere gli intervalli esaminati e impostare la relativa pianificazione. È possibile aggiungere intervalli IP all'elenco degli intervalli esaminati.

    Se si abilita l'opzione **Usa Zeroconf per il polling delle reti IPv6**, il punto di distribuzione esegue automaticamente il polling della rete IPv6 utilizzando le reti zero-configuration (definite anche *Zeroconf*). In questo caso, gli intervalli IP specificati vengono ignorati perché il punto di distribuzione esegue il polling dell'intera rete. L'opzione **Usa Zeroconf per il polling delle reti IPv6** è disponibile se nel punto di distribuzione viene eseguito Linux. Per utilizzare il polling ipv6 Zeroconf, è necessario installare l'utilità avahi-browse nel punto di distribuzione.

- Nella sezione **Avanzate** specificare la cartella che il punto di distribuzione deve utilizzare per archiviare i dati distribuiti.

- **Usa cartella predefinita**

  Se questa opzione è selezionata, l'applicazione utilizza la cartella di installazione di Network Agent nel punto di distribuzione.

- **Usa cartella specificata**

  Se questa opzione è selezionata, nel campo sottostante è possibile specificare il percorso della cartella. È possibile specificare una cartella locale nel punto di distribuzione oppure una cartella in qualsiasi dispositivo nella rete aziendale.

  L'account utente utilizzato nel punto di distribuzione per eseguire Network Agent deve disporre di accesso in lettura e scrittura alla cartella specificata.

I dispositivi selezionati opereranno come punti di distribuzione.

Solo i dispositivi con un sistema operativo Windows possono determinare il percorso di rete. Non è possibile determinare il percorso di rete per i dispositivi che eseguono altri sistemi operativi.

Rimozione di un dispositivo dall'elenco dei punti di distribuzione

Per rimuovere un dispositivo dall'elenco dei punti di distribuzione:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server, nella sezione **Punti di distribuzione**, selezionare il dispositivo che opera come punto di distribuzione e fare clic sul pulsante **Rimuovi**.

Il dispositivo verrà rimosso dall'elenco dei punti di distribuzione e smetterà di operare come punto di distribuzione.

Non è possibile rimuovere un dispositivo dall'elenco dei punti di distribuzione se è stato assegnato automaticamente da Administration Server.

Download degli aggiornamenti tramite punti di distribuzione

Kaspersky Security Center consente ai punti di distribuzione di ricevere aggiornamenti dall'Administration Server, dai server di Kaspersky o da una cartella locale o di rete.

Se non è necessario specificare una sorgente degli aggiornamenti, è consigliabile utilizzare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per un gruppo di amministrazione. Per informazioni dettagliate, fare riferimento al seguente argomento: Creazione dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione.

Per configurare il download degli aggiornamenti per un punto di distribuzione:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server, nella sezione **Punti di distribuzione** selezionare il punto di distribuzione tramite il quale verranno inviati gli aggiornamenti ai dispositivi client nel gruppo.
4. Fare clic sul pulsante **Proprietà** per aprire la finestra delle proprietà del punto di distribuzione selezionato.
5. Nella finestra delle proprietà del punto di distribuzione selezionare la sezione **Sorgenti degli aggiornamenti**.
6. Selezionare una sorgente degli aggiornamenti per il punto di distribuzione:
   - Per consentire al punto di distribuzione di ricevere gli aggiornamenti da Administration Server, selezionare **Recupera da Administration Server**:
     - Scarica file diff

       Questa opzione consente di abilitare la funzionalità di download dei file diff.

       Per impostazione predefinita, questa opzione è abilitata.
   - Per consentire al punto di distribuzione di ricevere aggiornamenti utilizzando un'attività, selezionare **Usa attività per il download forzato degli aggiornamenti**:
     - Se l'attività è già presente nel dispositivo, fare clic sul pulsante **Sfoglia**, quindi selezionare l'attività nell'elenco visualizzato.
     - Se l'attività non è ancora presente nel dispositivo, fare clic sul pulsante **Nuova attività** per creare un'attività. Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

   L'attività Scarica aggiornamenti negli archivi dei punti di distribuzione è un'attività locale. È necessario creare una nuova attività per ogni dispositivo che opera come punto di distribuzione.

Il punto di distribuzione riceverà gli aggiornamenti dalla sorgente specificata.

Eliminazione di aggiornamenti software dall'archivio

Per eliminare gli aggiornamenti software dall'archivio di Administration Server:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Aggiornamenti software**.
2. Nell'area di lavoro della cartella **Aggiornamenti software** selezionare l'aggiornamento che si desidera eliminare.
3. Dal menu di scelta rapida dell'aggiornamento selezionare **Elimina file di aggiornamento**.

Gli aggiornamenti software verranno eliminati dall'archivio di Administration Server.

Installazione patch per un'applicazione Kaspersky in modalità cluster

Kaspersky Security Center supporta solo l'installazione manuale delle patch per le applicazioni Kaspersky in modalità cluster.

Per installare una patch per un'applicazione Kaspersky:

1. Scaricare la patch in ogni nodo del cluster.
2. Eseguire l'installazione della patch nel nodo attivo.
3. Attendere il completamento dell'installazione della patch.
4. Eseguire la patch in tutti i sottonodi del cluster consecutivamente.

   Se si esegue la patch dalla riga di comando, utilizzare il parametro `--CLUSTER_SECONDARY_NODE`.

   A questo punto, la patch è installata in tutti i nodi del cluster.
5. Eseguire manualmente i servizi cluster di Kaspersky.

Ogni nodo del cluster è visualizzato in Administration Console come un dispositivo con Network Agent installato.

Per informazioni sulle patch installate, controllare la cartella **Aggiornamenti software** o il rapporto sulle versioni degli aggiornamenti per i moduli software delle applicazioni Kaspersky.

Gestione delle applicazioni di terzi nei dispositivi client

Kaspersky Security Center consente di gestire le applicazioni sviluppate da Kaspersky e altri produttori e installate nei dispositivi client.

L'amministratore può eseguire le seguenti azioni:

- Creare categorie di applicazioni in base ai criteri specificati.
- Gestire categorie di applicazioni utilizzando regole create appositamente.
- Gestire le applicazioni in esecuzione nei dispositivi.
- Eseguire l'inventario e mantenere un registro del software installato nei dispositivi.
- Correggere le vulnerabilità del software installato nei dispositivi.
- Installare aggiornamenti da Windows Update e altri produttori di software nei dispositivi.
- Monitorare l'utilizzo delle chiavi di licenza per i gruppi di applicazioni concesse in licenza.

Informazioni sulle applicazioni di terze parti

Kaspersky Security Center può aiutare ad aggiornare il software di terze parti installato nei dispositivi client e a correggere le vulnerabilità del software di terze parti. Kaspersky Security Center può aggiornare il software di terze parti solo dalla versione corrente alla versione più recente.

L'elenco del software di terze parti può essere modificato e viene aggiornato in modo dinamico. È possibile verificare se il software di terze parti (installato nei dispositivi degli utenti) può essere aggiornato con Kaspersky Security Center visualizzando l'elenco degli aggiornamenti disponibili in Administration Console (basata su MMC) e Kaspersky Security Center Web Console.

La procedura descritta di seguito è destinata esclusivamente alla visualizzazione dell'elenco dei software di terze parti che possono essere aggiornati con Kaspersky Security Center. Per accedere alle informazioni pertinenti senza avviare alcuna attività, è necessario seguire i passaggi indicati.

Per visualizzare l'elenco dei software di terze parti che è possibile aggiornare con Kaspersky Security Center in Kaspersky Security Center Web Console:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nel passaggio **Impostazioni nuova attività**, specificare le seguenti impostazioni:
   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Security Center**.
   b. Nel campo **Tipo di attività**, selezionare **Installa aggiornamenti richiesti e correggi vulnerabilità**.
4. Nel passaggio **Ambito dell'attività** della procedura guidata, selezionare l'opzione **Dispositivi gestiti**.
5. Nel passaggio **Specificare le regole per l'installazione degli aggiornamenti** del programma di installazione, fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
6. Nel passaggio **Selezionare il tipo di regola** della procedura guidata, selezionare l'opzione **Regola per gli aggiornamenti di terze parti**.
7. Nella fase **Criteri generali** della procedura guidata, selezionare l'opzione **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**, quindi fare clic su **Avanti**.

Viene visualizzato l'elenco dei software di terze parti.

Per visualizzare l'elenco del software di terze parti che è possibile aggiornare con Kaspersky Security Center nella console basata su MMC, è necessaria la licenza di Vulnerability e patch management. In caso contrario, l'attività **Installa aggiornamenti richiesti e correggi vulnerabilità** non è disponibile.

1. Nella struttura della console selezionare la cartella **Dispositivi gestiti**.
2. Nell'area di lavoro selezionare la scheda **Attività**.

3. Fare clic sul pulsante **Crea attività** per eseguire la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

4. Nella pagina **Selezionare il tipo di attività** della procedura guidata selezionare **Installa aggiornamenti richiesti e correggi vulnerabilità**.

5. Nel passaggio **Specificare le regole per l'installazione degli aggiornamenti** del programma di installazione, fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

6. Nel passaggio **Selezionare il tipo di regola** della procedura guidata, selezionare l'opzione **Regola per gli aggiornamenti di terze parti**.

7. Nella fase **Criteri generali** della procedura guidata, selezionare l'opzione **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**, quindi fare clic su **Avanti**.

Viene visualizzato l'elenco dei software di terze parti.

Installazione degli aggiornamenti software di terze parti

Kaspersky Security Center consente di gestire gli aggiornamenti del software installato nei dispositivi client e di correggere le vulnerabilità delle applicazioni Microsoft e di altri produttori di software tramite l'installazione degli aggiornamenti richiesti.

Kaspersky Security Center cerca gli aggiornamenti tramite l'attività di ricerca degli aggiornamenti e li scarica nell'archivio degli aggiornamenti. Al termine della ricerca degli aggiornamenti, l'applicazione fornisce all'amministratore informazioni sugli aggiornamenti disponibili e sulle vulnerabilità delle applicazioni che possono essere corrette tramite tali aggiornamenti.

Le informazioni sugli aggiornamenti disponibili per Microsoft Windows sono fornite dal servizio Windows Update. Administration Server può essere utilizzato come server WSUS (Windows Server Update Services). Per utilizzare Administration Server come server WSUS, è necessario configurare la sincronizzazione degli aggiornamenti con Windows Update. Dopo avere configurato la sincronizzazione dei dati con Windows Update, Administration Server fornisce gli aggiornamenti ai servizi Windows Update nei dispositivi in modalità centralizzata e in base alla frequenza impostata.

È inoltre possibile gestire gli aggiornamenti software tramite un criterio di Network Agent. A tale scopo, è necessario creare un criterio di Network Agent e configurare l'aggiornamento del software nelle finestre corrispondenti della Creazione guidata nuovo criterio.

L'amministratore può visualizzare un elenco degli aggiornamenti disponibili nella sottocartella **Aggiornamenti software** inclusa nella cartella **Gestione applicazioni**. Questa cartella contiene un elenco degli aggiornamenti per le applicazioni Microsoft e di altri produttori di software recuperati da Administration Server che possono essere distribuiti ai dispositivi. Dopo avere visualizzato le informazioni sugli aggiornamenti disponibili, l'amministratore può installarli nei dispositivi.

Kaspersky Security Center aggiorna alcune applicazioni rimuovendo la versione precedente dell'applicazione e installando la nuova.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Verificare che l'opzione **Visualizza Vulnerability e patch management** sia abilitata nella finestra **Configura interfaccia** per gli Administration Server primari e secondari. In caso contrario, l'attività di ricerca degli aggiornamenti gestisce solo gli aggiornamenti WSUS.

Per motivi di sicurezza, tutti gli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management vengono automaticamente analizzati alla ricerca di malware dalle tecnologie Kaspersky. Queste tecnologie vengono utilizzate per il controllo automatico dei file e includono la scansione virus, l'analisi statica, l'analisi dinamica, l'analisi del comportamento nell'ambiente sandbox e il machine learning.

Gli esperti Kaspersky non eseguono l'analisi manuale degli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management. Inoltre, gli esperti di Kaspersky non ricercano vulnerabilità (note o sconosciute) o funzionalità non documentate in tali aggiornamenti, né eseguono altri tipi di analisi degli aggiornamenti diversi da quelli specificati nel paragrafo precedente.

Prima di installare gli aggiornamenti in tutti i dispositivi, è possibile eseguire un'installazione di test per verificare che gli aggiornamenti installati non causino problemi di funzionamento delle applicazioni nei dispositivi.

Scenario: Aggiornamento di software di terze parti

Questa sezione fornisce uno scenario per l'aggiornamento del software di terze parti installato nei dispositivi client. Il software di terze parti include le applicazioni Microsoft e di altri fornitori di software. Gli aggiornamenti per le applicazioni Microsoft sono forniti dal servizio Windows Update.

Prerequisiti

Administration Server deve disporre di una connessione a Internet per installare gli aggiornamenti di software di terze parti diverso dal software Microsoft.

Per impostazione predefinita, non è richiesta la connessione Internet per l'installazione degli aggiornamenti software Microsoft nei dispositivi gestiti da parte di Administration Server. I dispositivi gestiti possono ad esempio scaricare gli aggiornamenti software Microsoft direttamente dai server Microsoft Update o da Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione. Administration Server deve essere connesso a Internet quando si utilizza Administration Server come server WSUS.

Passaggi

L'aggiornamento del software di terze parti prevede diversi passaggi:

1. **Ricerca degli aggiornamenti richiesti**

   Per trovare gli aggiornamenti software di terze parti richiesti per i dispositivi gestiti, eseguire l'attività *Trova vulnerabilità e aggiornamenti richiesti*. Al termine di questa attività, Kaspersky Security Center riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi specificati nelle proprietà dell'attività.

   L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Se non è stata eseguita la procedura guidata, creare l'attività o eseguire l'Avvio rapido guidato.

   Istruzioni dettagliate:

   - Administration Console: Scansione delle applicazioni per rilevare la presenza di vulnerabilità, Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
   - Kaspersky Security Center Web Console: Creazione dell'attività Trova vulnerabilità e aggiornamenti richiesti, Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

2. **Analisi dell'elenco degli aggiornamenti rilevati**

   Visualizzare l'elenco **Aggiornamenti software** e decidere quali aggiornamenti si desidera installare. Per visualizzare informazioni dettagliate su ciascun aggiornamento, fare clic sul nome dell'aggiornamento nell'elenco. Per ogni aggiornamento nell'elenco, è anche possibile visualizzare le statistiche sull'installazione dell'aggiornamento nei dispositivi client.

   Istruzioni dettagliate:

   - Administration Console: Visualizzazione delle informazioni sugli aggiornamenti disponibili
   - Kaspersky Security Center Web Console: Visualizzazione delle informazioni sugli aggiornamenti software di terze parti disponibili

3. **Configurazione dell'installazione degli aggiornamenti**

   Quando Kaspersky Security Center ha ricevuto l'elenco degli aggiornamenti software di terze parti, è possibile installarli nei dispositivi client utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Installa aggiornamenti di Windows Update*. Creare una di queste attività. È possibile creare queste attività nella scheda **Attività** o utilizzando l'elenco **Aggiornamenti software**.

   L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per installare gli aggiornamenti per le applicazioni Microsoft, inclusi gli aggiornamenti forniti dal servizio Windows Update, e gli aggiornamenti del software di altri produttori. Questa attività può essere creata solo se si dispone della licenza per la funzionalità Vulnerability e patch management.

   L'attività *Installa aggiornamenti di Windows Update* non richiede una licenza, ma può essere utilizzata per installare solo gli aggiornamenti di Windows Update.

   Per installare alcuni aggiornamenti software, è necessario accettare il Contratto di licenza con l'utente finale (EULA) per il software da installare. Se non si accetta il Contratto di licenza con l'utente finale, l'aggiornamento software non verrà installato.

   È possibile avviare un'attività di installazione degli aggiornamenti in base a una pianificazione. Quando si specifica la pianificazione dell'attività, assicurarsi che l'attività di installazione degli aggiornamenti venga avviata dopo il completamento dell'attività *Trova vulnerabilità e aggiornamenti richiesti*.

   Istruzioni dettagliate:

- Administration Console: Correzione delle vulnerabilità delle applicazioni, Visualizzazione delle informazioni sugli aggiornamenti disponibili
- Kaspersky Security Center Web Console: Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità, Creazione dell'attività Installa aggiornamenti di Windows Update, Visualizzazione delle informazioni sugli aggiornamenti software di terze parti disponibili

4. **Pianificazione delle attività**

   Per assicurarsi che l'elenco degli aggiornamenti sia sempre aggiornato, pianificare l'attività *Trova vulnerabilità e aggiornamenti richiesti* affinché venga eseguita periodicamente in modo automatico. Per impostazione predefinita, l'attività *Trova vulnerabilità e aggiornamenti richiesti* è impostata per l'avvio manuale.

   Se è stata creata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile pianificarla in modo che venga eseguita con la stessa frequenza dell'attività *Trova vulnerabilità e aggiornamenti richiesti* o con una frequenza inferiore. Quando si pianifica l'attività *Installa aggiornamenti di Windows Update*, tenere presente che per questa attività è necessario definire l'elenco degli aggiornamenti ogni volta prima di avviare l'attività.

   Durante la pianificazione delle attività, assicurarsi che un'attività di installazione degli aggiornamenti venga avviata dopo il completamento dell'attività *Trova vulnerabilità e aggiornamenti richiesti*.

5. **Approvazione e rifiuto degli aggiornamenti software (facoltativo)**

   Se è stata creata l'attività Installa aggiornamenti richiesti e correggi vulnerabilità, è possibile specificare le regole per l'installazione degli aggiornamenti nelle proprietà dell'attività. Se è stata creata l'attività Installa aggiornamenti di Windows Update, ignorare questo passaggio.

   Per ciascuna regola, è possibile definire gli aggiornamenti da installare in base allo stato dell'aggiornamento: *Indefinito*, *Approvato* o *Rifiutato*. Ad esempio, è possibile creare un'attività specifica per i server e impostare una regola per questa attività in modo da consentire l'installazione solo degli aggiornamenti di Windows Update e solo di quelli con stato *Approvato*. Successivamente, si imposta manualmente lo stato *Approvato* per gli aggiornamenti da installare. In questo caso, gli aggiornamenti di Windows Update con stato *Indefinito* o *Rifiutato* non verranno installati nei server specificati nell'attività.

   L'utilizzo dello stato *Approvato* per gestire l'installazione degli aggiornamenti è efficace per una piccola quantità di aggiornamenti. Per installare più aggiornamenti, utilizzare le regole che è possibile configurare nell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. È consigliabile impostare lo stato *Approvato* solo per gli aggiornamenti specifici che non soddisfano i criteri specificati nelle regole. Quando si approva manualmente una grande quantità di aggiornamenti, le prestazioni di Administration Server si riducono e questo può causare un sovraccarico di Administration Server.

   Per impostazione predefinita, gli aggiornamenti software scaricati hanno lo stato *Indefinito*. È possibile modificare lo stato in *Approvato* o *Rifiutato* nell'elenco **Aggiornamenti software** (**Operazioni** → **Gestione patch** → **Aggiornamenti software**).

   Istruzioni dettagliate:

   - Administration Console: Approvazione e rifiuto degli aggiornamenti software
   - Kaspersky Security Center Web Console: Approvazione e rifiuto degli aggiornamenti software di terze parti

6. **Configurazione di Administration Server per operare come server WSUS (Windows Server Update Services) (facoltativo)**

   Per impostazione predefinita, gli aggiornamenti di Windows Update vengono scaricati nei dispositivi gestiti dai server Microsoft. È possibile modificare questa impostazione per utilizzare Administration Server come server WSUS. In questo caso, Administration Server sincronizza i dati sugli aggiornamenti con Windows Update con la frequenza specificata e fornisce gli aggiornamenti in modalità centralizzata a Windows Update nei dispositivi nella rete.

   Per utilizzare Administration Server come server WSUS, creare l'attività Esegui sincronizzazione di Windows Update e selezionare la casella di controllo **Usa Administration Server come server WSUS** nel criterio di Network Agent.

Istruzioni dettagliate:

- Administration Console: Sincronizzazione degli aggiornamenti da Windows Update con Administration Server, Configurazione degli aggiornamenti di Windows in un criterio di Network Agent
- Kaspersky Security Center Web Console: Creazione dell'attività Esegui sincronizzazione di Windows Update

7. **Esecuzione di un'attività di installazione degli aggiornamenti**

   Avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Installa aggiornamenti di Windows Update*. Quando si avviano queste attività, gli aggiornamenti vengono scaricati e installati nei dispositivi gestiti. Al termine dell'attività, assicurarsi che questa abbia lo stato *Completato* nell'elenco attività.

8. **Creare il rapporto sui risultati dell'installazione degli aggiornamenti del software di terze parti (facoltativo)**

   Per visualizzare le statistiche dettagliate sull'installazione degli aggiornamenti, creare il **Rapporto sui risultati dell'installazione degli aggiornamenti software di terze parti**.

   Istruzioni dettagliate:

   - Administration Console: Creazione e visualizzazione di un rapporto
   - Kaspersky Security Center Web Console: Generazione e visualizzazione di un rapporto

Risultati

Se è stata creata e configurata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, gli aggiornamenti vengono installati automaticamente nei dispositivi gestiti. Quando i nuovi aggiornamenti vengono scaricati nell'archivio dell'Administration Server, Kaspersky Security Center verifica se soddisfano i criteri specificati nelle regole per gli aggiornamenti. Tutti i nuovi aggiornamenti che soddisfano i criteri verranno installati automaticamente alla successiva esecuzione dell'attività.

Se è stata creata l'attività *Installa aggiornamenti di Windows Update*, vengono installati solo gli aggiornamenti specificati nelle proprietà dell'attività *Installa aggiornamenti di Windows Update*. Se in seguito si desidera installare i nuovi aggiornamenti scaricati nell'archivio dell'Administration Server, è necessario aggiungere gli aggiornamenti richiesti all'elenco degli aggiornamenti nell'attività esistente o creare una nuova attività *Installa aggiornamenti di Windows Update*.

Visualizzazione delle informazioni sugli aggiornamenti disponibili per le applicazioni di terze parti

Per visualizzare un elenco degli aggiornamenti disponibili per le applicazioni di terze parti installate nei dispositivi client:

Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Aggiornamenti software**.

Nell'area di lavoro della cartella è possibile visualizzare un elenco degli aggiornamenti disponibili per le applicazioni installate nei dispositivi.

Per visualizzare le proprietà di un aggiornamento:

nell'area di lavoro della cartella **Aggiornamenti software** selezionare **Proprietà** nel menu di scelta rapida dell'aggiornamento.

Nella finestra delle proprietà dell'aggiornamento è possibile visualizzare le seguenti informazioni:

- Nella sezione **Generale** è possibile visualizzare lo **Stato di approvazione dell'aggiornamento**:
  - **Indefinito**: l'aggiornamento è disponibile nell'elenco degli aggiornamenti, ma non è approvato per l'installazione.
  - **Approvato**: l'aggiornamento è disponibile nell'elenco degli aggiornamenti e approvato per l'installazione.
  - **Rifiutato**: l'aggiornamento viene rifiutato per l'installazione.
- Nella sezione **Attributi** è possibile visualizzare i valori del campo **Installazione automatica**:
  - Il valore **Automaticamente** viene visualizzato se l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* può installare gli aggiornamenti per l'applicazione. L'attività installa automaticamente i nuovi aggiornamenti dall'indirizzo Web fornito dal produttore del software di terze parti.
  - Il valore **Manualmente** viene visualizzato se Kaspersky Security Center non riesce a installare automaticamente gli aggiornamenti per l'applicazione. È possibile installare gli aggiornamenti manualmente.

  Il campo **Installazione automatica** non viene visualizzato per gli aggiornamenti delle applicazioni Windows.
- Elenco dei dispositivi client a cui è destinato l'aggiornamento.
- Elenco degli eventuali componenti di sistema (prerequisiti) che devono essere installati prima dell'aggiornamento.
- Vulnerabilità del software che l'aggiornamento consente di correggere.

Approvazione e rifiuto degli aggiornamenti software

Le impostazioni di un'attività di installazione degli aggiornamenti possono richiedere l'approvazione degli aggiornamenti da installare. È possibile approvare gli aggiornamenti da installare e rifiutare quelli che non devono essere installati.

Ad esempio, potrebbe essere utile controllare prima l'installazione degli aggiornamenti in un ambiente di test e verificare che non interferiscano con l'utilizzo dei dispositivi e solo successivamente consentire l'installazione degli aggiornamenti nei dispositivi client.

L'utilizzo dello stato *Approvato* per gestire l'installazione degli aggiornamenti di terze parti è efficace per una piccola quantità di aggiornamenti. Per installare più aggiornamenti di terze parti, utilizzare le regole che è possibile configurare nell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. È consigliabile impostare lo stato *Approvato* solo per gli aggiornamenti specifici che non soddisfano i criteri specificati nelle regole. Quando si approva manualmente una grande quantità di aggiornamenti, le prestazioni di Administration Server si riducono e questo può causare un sovraccarico di Administration Server.

Per approvare o rifiutare uno o più aggiornamenti:

1. Nella struttura della console selezionare il nodo **Avanzate** → **Gestione applicazioni** → **Aggiornamenti software**.
2. Nell'area di lavoro della cartella **Aggiornamenti software** fare clic sul pulsante **Aggiorna** nell'angolo superiore destro. Viene visualizzato un elenco degli aggiornamenti.

3. Selezionare gli aggiornamenti che si desidera accettare o rifiutare.

   Nella parte destra dell'area di lavoro verrà visualizzata la finestra di informazioni relativa agli oggetti selezionati.

4. Nell'elenco a discesa **Stato di approvazione dell'aggiornamento** selezionare **Approvato** per approvare gli aggiornamenti selezionati o **Rifiutato** per rifiutare gli aggiornamenti selezionati.

   Il valore predefinito è **Indefinito**.

Gli aggiornamenti per cui si imposta lo stato **Approvato** verranno inseriti in una coda per l'installazione.

Gli aggiornamenti per cui si imposta lo stato **Rifiutato** verranno disinstallati (se possibile) da tutti i dispositivi in cui erano installati in precedenza. Inoltre, non verranno installati in altri dispositivi in futuro.

Alcuni aggiornamenti per le applicazioni Kaspersky non possono essere disinstallati. Se si imposta lo stato **Rifiutato** per tali aggiornamenti, Kaspersky Security Center non li disinstallerà dai dispositivi in cui erano installati in precedenza. Tuttavia, tali aggiornamenti non verranno installati in altri dispositivi in futuro. Se un aggiornamento per le applicazioni Kaspersky non può essere disinstallato, questa proprietà è visualizzata nella finestra delle proprietà dell'aggiornamento: nel riquadro **Sezioni** selezionare **Generale** e nell'area di lavoro verrà visualizzata la proprietà in **Requisiti per l'installazione**. Se si imposta lo stato **Rifiutato** per gli aggiornamenti software di terze parti, tali aggiornamenti non verranno installati nei dispositivi in cui l'installazione era stata pianificata ma non ancora eseguita. Gli aggiornamenti rimarranno nei dispositivi in cui erano già installati. Se è necessario eliminarli, è possibile eliminarli manualmente in locale.

Sincronizzazione degli aggiornamenti da Windows Update con Administration Server

Se è stata selezionata l'opzione **Usa Administration Server come server WSUS** nella finestra **Impostazioni per la gestione degli aggiornamenti** dell'Avvio rapido guidato, l'attività di sincronizzazione di Windows Update viene creata automaticamente. È possibile eseguire l'attività nella cartella **Attività**. La funzionalità di aggiornamento del software Microsoft è disponibile solo dopo il completamento dell'attività **Esegui sincronizzazione di Windows Update**.

Gli aggiornamenti software Microsoft possono superare i 10 GB. Assicurarsi che il database di Administration Server sia in grado di ospitare tali volumi; in caso contrario, l'attività **Esegui sincronizzazione di Windows Update** non riuscirà. Il database Microsoft SQL Express non è supportato per l'attività **Esegui sincronizzazione di Windows Update**.

L'attività **Esegui sincronizzazione di Windows Update** scarica solo metadati dai server Microsoft. Se la rete non utilizza un server WSUS, ogni dispositivo client scarica gli aggiornamenti Microsoft da server esterni in modo indipendente.

Per creare un'attività per la sincronizzazione di Windows Update con Administration Server:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Aggiornamenti software**.

2. Fare clic sul pulsante **Azioni aggiuntive** e selezionare **Configura sincronizzazione di Windows Update** nell'elenco a discesa.

   La procedura guidata crea l'attività **Esegui sincronizzazione di Windows Update** visualizzata nella cartella **Attività**.

   Viene avviata la Creazione guidata attività di recupero dati da Windows Update Center. Seguire le istruzioni della procedura guidata.

È inoltre possibile creare l'attività di sincronizzazione di Windows Update nella cartella **Attività** facendo clic su **Crea attività**.

Microsoft elimina periodicamente gli aggiornamenti obsoleti dai server dell'azienda in modo che il numero degli aggiornamenti correnti sia sempre compreso tra 200.000 e 300.000. Per ridurre l'utilizzo dello spazio su disco e le dimensioni del database, Kaspersky Security Center elimina gli aggiornamenti obsoleti che non sono più presenti nei server di aggiornamento di Microsoft.

Durante l'esecuzione dell'attività **Esegui sincronizzazione di Windows Update** l'applicazione riceve un elenco degli aggiornamenti correnti da un server di aggiornamento Microsoft. Kaspersky Security Center compila quindi un elenco degli aggiornamenti che sono diventati obsoleti. Al successivo avvio dell'attività **Trova vulnerabilità e aggiornamenti richiesti**, Kaspersky Security Center contrassegna tutti gli aggiornamenti obsoleti e ne imposta l'ora di eliminazione. Al successivo avvio dell'attività **Esegui sincronizzazione di Windows Update**, vengono eliminati tutti gli aggiornamenti contrassegnati per l'eliminazione 30 giorni prima. Kaspersky Security Center verifica inoltre se sono presenti aggiornamenti obsoleti contrassegnati per l'eliminazione più di 180 giorni prima ed elimina gli aggiornamenti meno recenti.

Quando viene completata l'attività **Esegui sincronizzazione di Windows Update** e gli aggiornamenti obsoleti vengono eliminati, il database può ancora salvare i codici hash relativi ai file degli aggiornamenti eliminati, nonché i file corrispondenti nei file %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles files (se sono stati scaricati in precedenza). È possibile eseguire l'attività Manutenzione di Administration Server per eliminare i record obsoleti dal database e dai file corrispondenti.

Passaggio 1. Stabilire se ridurre o meno il traffico

Quando Kaspersky Security Center sincronizza gli aggiornamenti con i server di Microsoft Windows Update, le informazioni su tutti i file vengono salvate nel database di Administration Server. Anche tutti i file richiesti per un aggiornamento vengono scaricati nell'unità durante l'interazione con l'Agente di Windows Update. In particolare, Kaspersky Security Center salva le informazioni sui file per l'aggiornamento rapido nel database e li scarica se necessario. Il download dei file per l'aggiornamento rapido comporta una riduzione dello spazio su disco.

Per evitare la diminuzione dello spazio su disco e ridurre il traffico, è possibile disabilitare l'opzione **Scarica i file di installazione rapida**.

Se l'opzione è selezionata, i file degli aggiornamenti rapidi vengono scaricati durante l'esecuzione dell'attività. Per impostazione predefinita, questa opzione non è selezionata.

Passaggio 2. Applicazioni

In questa sezione è possibile selezionare le applicazioni per cui saranno scaricati gli aggiornamenti.

Se la casella di controllo **Tutte le applicazioni** è selezionata, verranno scaricati gli aggiornamenti per tutte le applicazioni esistenti e per tutte le applicazioni che potrebbero essere rilasciate in futuro.

Per impostazione predefinita, la casella di controllo **Tutte le applicazioni** è selezionata.

Passaggio 3. Categorie di aggiornamenti

In questa sezione è possibile selezionare le categorie di aggiornamenti che verranno scaricati in Administration Server.

Se la casella di controllo **Tutte le categorie** è selezionata, gli aggiornamenti verranno scaricati per tutte le categorie di aggiornamenti esistenti e per tutte le categorie che possono presentarsi in futuro.

Per impostazione predefinita, la casella di controllo **Tutte le categorie** è selezionata.

Passaggio 4. Lingue degli aggiornamenti

In questa finestra è possibile selezionare le lingue di localizzazione degli aggiornamenti che verranno scaricati in Administration Server. Selezionare una delle seguenti opzioni per il download delle lingue di localizzazione degli aggiornamenti:

- **Scarica tutte le lingue, incluse quelle nuove**

  Se questa opzione è selezionata, tutte le lingue di localizzazione disponibili degli aggiornamenti verranno scaricate in Administration Server. Per impostazione predefinita, questa opzione è selezionata.

- **Scarica le lingue selezionate**

  Se questa opzione è selezionata, è possibile selezionare dall'elenco le lingue di localizzazione degli aggiornamenti da scaricare in Administration Server.

Passaggio 5. Selezione dell'account per l'avvio dell'attività

Nella finestra **Selezione di un account per l'esecuzione dell'attività** è possibile specificare l'account da utilizzare durante l'esecuzione dell'attività. Selezionare una delle seguenti opzioni:

- **Account predefinito**

  L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

  Per impostazione predefinita, questa opzione è selezionata.

- **Specifica account**

  Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

  - **Account**

    Account tramite il quale viene eseguita l'attività.

  - **Password**

    Password dell'account con cui verrà eseguita l'attività.

Passaggio 6. Configurazione di una pianificazione di avvio delle attività

Nella pagina **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio delle attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N settimane**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

- **Settimanale**

  L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Una sola volta**

  L'attività viene eseguita una volta, nella data e nell'ora specificate (per impostazione predefinita, il giorno in cui è stata creata l'attività).

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  > Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- **Durante un'epidemia di virus**

L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

- Anti-virus per workstation e file server
- Anti-virus per la difesa perimetrale
- Anti-virus per i sistemi di posta

Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- Al completamento di un'altra attività

  L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

  È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

  Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

  - Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
  - Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

    Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
  - Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- Esegui attività non effettuate

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

Passaggio 7. Definizione del nome dell'attività

Nella finestra **Definire il nome dell'attività** specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali (`"*<>?\:|`). Il valore predefinito è *Esegui sincronizzazione di Windows Update*.

Passaggio 8. Completamento della creazione dell'attività

Nella finestra **Completare la creazione dell'attività** fare clic sul pulsante **Fine** per completare la procedura guidata.

Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

La nuova attività di sincronizzazione di Windows Update creata verrà visualizzata nell'elenco delle attività nella cartella **Attività** della struttura della console.

Installazione manuale degli aggiornamenti nei dispositivi

Se è stato selezionato **Cerca e installa gli aggiornamenti richiesti** nella pagina **Impostazioni per la gestione degli aggiornamenti** dell'Avvio rapido guidato, verrà creata automaticamente l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. È possibile eseguire o interrompere l'attività nella cartella **Dispositivi gestiti**, nella scheda **Attività**.

Se è stato selezionato **Cerca gli aggiornamenti richiesti** nell'Avvio rapido guidato, è possibile installare gli aggiornamenti software nei dispositivi client tramite l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.

È possibile eseguire qualsiasi delle seguenti operazioni:

- Creare un'attività per l'installazione degli aggiornamenti.
- Aggiungere una regola per l'installazione di un aggiornamento a un'attività per l'installazione di aggiornamenti.
- Configurare un'installazione di test degli aggiornamenti, nelle impostazioni di un'attività per l'installazione di aggiornamenti.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Installazione degli aggiornamenti tramite la creazione di un'attività di installazione

È possibile eseguire qualsiasi delle seguenti operazioni:

- Creare un'attività per l'installazione di determinati aggiornamenti.
- Selezionare un aggiornamento e creare un'attività per l'installazione di tale aggiornamento e degli aggiornamenti analoghi.

Per installare specifici aggiornamenti:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Aggiornamenti software**.
2. Nell'area di lavoro selezionare gli aggiornamenti che si desidera installare.
3. Eseguire una delle seguenti operazioni:
   - Fare clic con il pulsante destro del mouse su uno degli aggiornamenti selezionati nell'elenco e quindi scegliere **Installa aggiornamento** → **Nuova attività**.
   - Fare clic sul collegamento **Installa aggiornamento (crea attività)** nella finestra di informazioni degli aggiornamenti selezionati.
4. Scegliere l'operazione da eseguire quando viene richiesto se installare tutti gli aggiornamenti precedenti dell'applicazione. Fare clic su **Sì** se si desidera installare in modo incrementale le versioni successive dell'applicazione, se questo è necessario per l'installazione degli aggiornamenti selezionati. Fare clic su **No** se si desidera eseguire l'aggiornamento delle applicazioni in modo diretto, senza installare le versioni successive. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

   Viene avviata la Creazione guidata attività di installazione aggiornamenti e correzione vulnerabilità. Seguire le istruzioni della procedura guidata.

5. Nella pagina **Selezione dell'opzione per il riavvio del sistema operativo** della procedura guidata selezionare l'azione da eseguire quando il sistema operativo nei dispositivi client deve essere riavviato dopo l'operazione:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

6. Nella pagina **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N settimane**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

  - **Settimanale**

    L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- In base ai giorni della settimana

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- Mensile

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- Manualmente

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- Ogni mese nei giorni specificati delle settimane selezionate

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- Durante un'epidemia di virus

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- Al completamento di un'altra attività

L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

- Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
- Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

  Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
- Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

7. Nella pagina **Definire il nome dell'attività** della procedura guidata specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

8. Nella pagina **Completare la creazione dell'attività** della procedura guidata fare clic sul pulsante **Fine** per chiudere la procedura guidata.

   Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Al termine della procedura guidata, l'attività **Installa aggiornamenti richiesti e correggi vulnerabilità** verrà visualizzata nella cartella **Attività**.

È possibile abilitare l'installazione automatica dei componenti di sistema (prerequisiti) prima dell'installazione di un aggiornamento nelle proprietà dell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. Quando si abilita questa opzione, tutti i componenti di sistema vengono installati prima dell'aggiornamento. Nelle proprietà dell'aggiornamento è disponibile un elenco dei componenti necessari.

Nelle proprietà dell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile consentire l'installazione di aggiornamenti che eseguono l'upgrade a una nuova versione dell'applicazione.

Se le impostazioni dell'attività specificano regole per l'installazione di aggiornamenti di terze parti, Administration Server scarica tutti gli aggiornamenti appropriati dai siti Web dei relativi produttori. Gli aggiornamenti vengono salvati nell'archivio di Administration Server e quindi sono distribuiti e installati nei dispositivi a cui sono applicabili.

Se le impostazioni dell'attività specificano regole per l'installazione di aggiornamenti Microsoft e Administration Server opera come server WSUS, Administration Server scarica tutti gli aggiornamenti appropriati nell'archivio e quindi li distribuisce ai dispositivi gestiti. Se la rete non utilizza un server WSUS, ogni dispositivo client scarica gli aggiornamenti Microsoft da server esterni in modo indipendente.

Per installare uno specifico aggiornamento e quelli analoghi:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Aggiornamenti software**.

2. Nell'area di lavoro selezionare l'aggiornamento che si desidera installare.

3. Fare clic sul pulsante **Esegui Installazione guidata aggiornamenti**.

   Verrà avviata l'Installazione guidata aggiornamenti.

   Le funzionalità dell'Installazione guidata aggiornamenti sono disponibili solo con la licenza Vulnerability e patch management.

   Seguire le istruzioni della procedura guidata.

4. Nella pagina **Cerca attività di installazione degli aggiornamenti esistenti** specificare le seguenti impostazioni:

   - **Cerca attività per l'installazione dell'aggiornamento**

     Se questa opzione è abilitata, l'Installazione guidata aggiornamenti cerca le attività esistenti per l'installazione dell'aggiornamento selezionato.

     Se questa opzione è disabilitata o se la ricerca non recupera attività applicabili, l'Installazione guidata aggiornamenti richiede di creare una regola o un'attività per l'installazione dell'aggiornamento.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Approva installazione dell'aggiornamento**

     L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

     Per impostazione predefinita, questa opzione è disabilitata.

5. Se si sceglie di eseguire la ricerca delle attività esistenti di installazione degli aggiornamenti e la ricerca recupera alcune attività, è possibile visualizzare le proprietà di queste attività o avviarle manualmente. Non sono necessarie ulteriori operazioni.

   Altrimenti, fare clic sul pulsante **Nuova attività di installazione degli aggiornamenti**.

6. Selezionare il tipo di regola di installazione da aggiungere alla nuova attività e fare clic sul pulsante **Fine**.

7. Scegliere l'operazione da eseguire quando viene richiesto se installare tutti gli aggiornamenti precedenti dell'applicazione. Fare clic su **Sì** se si desidera installare in modo incrementale le versioni successive dell'applicazione, se questo è necessario per l'installazione degli aggiornamenti selezionati. Fare clic su **No** se si desidera eseguire l'aggiornamento delle applicazioni in modo diretto, senza installare le versioni successive. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

   Viene avviata la Creazione guidata attività di installazione aggiornamenti e correzione vulnerabilità. Seguire le istruzioni della procedura guidata.

8. Nella pagina **Selezione dell'opzione per il riavvio del sistema operativo** della procedura guidata selezionare l'azione da eseguire quando il sistema operativo nei dispositivi client deve essere riavviato dopo l'operazione:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

9. Nella pagina **Selezionare i dispositivi a cui assegnare l'attività** della procedura guidata selezionare una delle seguenti opzioni:

- **Seleziona i dispositivi della rete rilevati da Administration Server**

  L'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

  Questa opzione può ad esempio essere utilizzata in un'attività per l'installazione di Network Agent nei dispositivi non assegnati.

- **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**

  È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

  Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

- **Assegna un'attività a una selezione dispositivi**

  L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

- **Assegna un'attività a un gruppo di amministrazione**

  L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

  Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

10. Nella pagina **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N settimane**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

  - **Settimanale**

    L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- In base ai giorni della settimana

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- Mensile

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- Manualmente (opzione selezionata per impostazione predefinita)

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- Ogni mese nei giorni specificati delle settimane selezionate

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  > Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- Durante un'epidemia di virus

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- Al completamento di un'altra attività

L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

- Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
- Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

  Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
- Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

11. Nella pagina **Definire il nome dell'attività** della procedura guidata specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

12. Nella pagina **Completare la creazione dell'attività** della procedura guidata fare clic sul pulsante **Fine** per chiudere la procedura guidata.

    Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Al termine della procedura guidata, verrà creata l'attività **Installa aggiornamenti richiesti e correggi vulnerabilità**, che sarà visualizzata nella cartella **Attività**.

Oltre alle impostazioni specificate durante la creazione dell'attività, è possibile modificare altre proprietà di un'attività creata.

L'upgrade a una nuova versione dell'applicazione può causare un malfunzionamento delle applicazioni dipendenti nei dispositivi.

Installazione di un aggiornamento tramite l'aggiunta di una regola a un'attività di installazione esistente

Per installare un aggiornamento tramite l'aggiunta di una regola a un'attività di installazione esistente:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Aggiornamenti software**.

2. Nell'area di lavoro selezionare l'aggiornamento che si desidera installare.

3. Fare clic sul pulsante **Esegui Installazione guidata aggiornamenti**.

   Verrà avviata l'Installazione guidata aggiornamenti.

   Le funzionalità dell'Installazione guidata aggiornamenti sono disponibili solo con la licenza Vulnerability e patch management.

   Seguire le istruzioni della procedura guidata.

4. Nella pagina **Cerca attività di installazione degli aggiornamenti esistenti** specificare le seguenti impostazioni:

   - **Cerca attività per l'installazione dell'aggiornamento**

     Se questa opzione è abilitata, l'Installazione guidata aggiornamenti cerca le attività esistenti per l'installazione dell'aggiornamento selezionato.

     Se questa opzione è disabilitata o se la ricerca non recupera attività applicabili, l'Installazione guidata aggiornamenti richiede di creare una regola o un'attività per l'installazione dell'aggiornamento.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Approva installazione dell'aggiornamento**

     L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

     Per impostazione predefinita, questa opzione è disabilitata.

5. Se si sceglie di eseguire la ricerca delle attività esistenti di installazione degli aggiornamenti e la ricerca recupera alcune attività, è possibile visualizzare le proprietà di queste attività o avviarle manualmente. Non sono necessarie ulteriori operazioni.

   In caso contrario, fare clic sul pulsante **Aggiungi una regola di installazione degli aggiornamenti**.

6. Selezionare l'attività a cui aggiungere una regola, quindi fare clic sul pulsante **Aggiungi regola**.

   È inoltre possibile visualizzare le proprietà delle attività esistenti, avviarle manualmente o creare una nuova attività.

7. Selezionare il tipo di regola da aggiungere all'attività selezionata e fare clic sul pulsante **Fine**.

8. Scegliere l'operazione da eseguire quando viene richiesto se installare tutti gli aggiornamenti precedenti dell'applicazione. Fare clic su **Sì** se si desidera installare in modo incrementale le versioni successive dell'applicazione, se questo è necessario per l'installazione degli aggiornamenti selezionati. Fare clic su **No** se si desidera eseguire l'aggiornamento delle applicazioni in modo diretto, senza installare le versioni successive. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

Una nuova regola per l'installazione dell'aggiornamento viene aggiunta all'attività **Installa aggiornamenti richiesti e correggi vulnerabilità** esistente.

Configurazione di un'installazione di test degli aggiornamenti

Per configurare un'installazione di test degli aggiornamenti:

1. Nella struttura della console selezionare l'attività **Installa aggiornamenti richiesti e correggi vulnerabilità** nella cartella **Dispositivi gestiti**, nella scheda **Attività**.

2. Dal menu di scelta rapida dell'attività selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà dell'attività **Installa aggiornamenti richiesti e correggi vulnerabilità**.

3. Nella finestra delle proprietà dell'attività, nella sezione **Installazione di test**, selezionare una delle opzioni disponibili per l'installazione di test:

   - **Non eseguire scansione**. Selezionare questa opzione se non si desidera eseguire un'installazione di test degli aggiornamenti.

   - **Esegui scansione nei dispositivi selezionati**. Selezionare questa opzione se si desidera testare l'installazione degli aggiornamenti nei dispositivi selezionati. Fare clic sul pulsante **Aggiungi** e selezionare i dispositivi in cui si desidera eseguire l'installazione di test degli aggiornamenti.

   - **Esegui scansione nei dispositivi del gruppo specificato**. Selezionare questa opzione se si desidera testare l'installazione degli aggiornamenti in un gruppo di dispositivi. Nel campo **Specificare un gruppo di test** specificare un gruppo di dispositivi in cui si desidera eseguire un'installazione di test.

   - **Esegui scansione nella percentuale di dispositivi specificata**. Selezionare questa opzione se si desidera testare l'installazione solo su una parte dei dispositivi di destinazione. Nel campo **Percentuale di dispositivi di test su tutti i dispositivi di destinazione** specificare la percentuale dei dispositivi in cui si desidera eseguire un'installazione di test degli aggiornamenti.

4. Dopo avere selezionato qualsiasi opzione tranne **Non eseguire scansione**, nel campo **Tempo disponibile per decidere se continuare l'installazione, in ore** specificare il numero di ore tra l'installazione di test degli aggiornamenti e l'avvio dell'installazione degli aggiornamenti in tutti i dispositivi.

Configurazione degli aggiornamenti di Windows in un criterio di Network Agent

Per configurare gli aggiornamenti di Windows in un criterio di Network Agent:

1. Nella struttura della console selezionare **Dispositivi gestiti**.

2. Nell'area di lavoro selezionare la scheda **Criteri**.

3. Selezionare un criterio di Network Agent.

4. Nel menu di scelta rapida del criterio selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del criterio di Network Agent.

5. Nel riquadro **Sezioni** selezionare **Vulnerabilità e aggiornamenti software**.

6. Selezionare l'opzione **Usa Administration Server come server WSUS** server per scaricare gli aggiornamenti di Windows in Administration Server e quindi distribuirli nei dispositivi client tramite Network Agent.

   Se questa opzione non è selezionata, gli aggiornamenti di Windows vengono scaricati in Administration Server. In questo caso, i dispositivi client ricevono gli aggiornamenti di Windows direttamente dai server Microsoft.

7. Selezionare il set di aggiornamenti che gli utenti possono installare manualmente nei propri dispositivi tramite Windows Update.

Nei dispositivi che eseguono Windows 10, se Windows Update ha già rilevato aggiornamenti per il dispositivo, la nuova opzione selezionata in **Consentire agli utenti di gestire l'installazione degli aggiornamenti Windows Update** verrà applicata solo dopo l'installazione degli aggiornamenti rilevati.

Selezionare un elemento nell'elenco a discesa:

- **Consentire agli utenti di installare tutti gli aggiornamenti Windows Update applicabili**

  Gli utenti possono installare nei propri dispositivi tutti gli aggiornamenti di Microsoft Windows Update applicabili.

  Selezionare questa opzione se non si desidera interferire nell'installazione degli aggiornamenti.

  Quando l'utente installa manualmente gli aggiornamenti di Microsoft Windows Update, gli aggiornamenti possono essere scaricati dai server Microsoft anziché da Administration Server. Questo è possibile se Administration Server non ha ancora scaricato gli aggiornamenti. Il download degli aggiornamenti dai server Microsoft comporta un traffico aggiuntivo.

- **Consentire agli utenti di installare solo gli aggiornamenti Windows Update approvati**

  Gli utenti possono installare nei propri dispositivi tutti gli aggiornamenti di Microsoft Windows Update applicabili e approvati dall'amministratore.

  Ad esempio, potrebbe essere utile controllare prima l'installazione degli aggiornamenti in un ambiente di test e verificare che non interferiscano con l'utilizzo dei dispositivi e solo successivamente consentire l'installazione degli aggiornamenti approvati nei dispositivi client.

  Quando l'utente installa manualmente gli aggiornamenti di Microsoft Windows Update, gli aggiornamenti possono essere scaricati dai server Microsoft anziché da Administration Server. Questo è possibile se Administration Server non ha ancora scaricato gli aggiornamenti. Il download degli aggiornamenti dai server Microsoft comporta un traffico aggiuntivo.

- **Non consentire agli utenti di installare gli aggiornamenti Windows Update**

  Gli utenti non possono installare manualmente gli aggiornamenti di Microsoft Windows Update nei propri dispositivi. Tutti gli aggiornamenti applicabili vengono installati in base alla configurazione specificata dall'amministratore.

  Selezionare questa opzione se si desidera gestire l'installazione degli aggiornamenti in modo centralizzato.

  È ad esempio possibile ottimizzare la pianificazione degli aggiornamenti in modo da evitare di sovraccaricare la rete. È possibile pianificare le installazioni degli aggiornamenti in orario non lavorativo, in modo che non interferiscano con la produttività degli utenti.

8. Selezionare la modalità di ricerca degli aggiornamenti di Windows:

- **Attiva**

  Se questa opzione è selezionata, Administration Server con il supporto di Network Agent avvia una richiesta da un Windows Update Agent nel dispositivo client alla sorgente degli aggiornamenti: server Windows Update o WSUS. Successivamente, Network Agent trasmette le informazioni ricevute da Windows Update Agent ad Administration Server.

  L'opzione è valida solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** dell'attività *Trova vulnerabilità e aggiornamenti richiesti* è selezionata.

  Per impostazione predefinita, questa opzione è selezionata.

- **Passiva**

  Se questa opzione è selezionata, Network Agent trasmette periodicamente ad Administration Server le informazioni sugli aggiornamenti recuperati durante l'ultima sincronizzazione di Windows Update Agent con la sorgente degli aggiornamenti. Se non viene eseguita la sincronizzazione di Windows Update Agent con una sorgente degli aggiornamenti, le informazioni sugli aggiornamenti in Administration Server diventano obsolete.

  Selezionare questa opzione se si desidera ottenere gli aggiornamenti dalla cache della memoria della sorgente degli aggiornamenti.

- **Disabilitata**

  Se questa opzione è selezionata, Administration Server non richiede informazioni sugli aggiornamenti.

  Selezionare questa opzione se, ad esempio, si desidera prima testare gli aggiornamenti nel dispositivo locale.

9. Selezionare l'opzione **Esegui la scansione dei file eseguibili per rilevarne le vulnerabilità al momento dell'esecuzione** se si desidera sottoporre a scansione i file eseguibili alla ricerca di vulnerabilità durante la loro esecuzione.

10. Assicurarsi che la modifica sia bloccata per tutte le impostazioni modificate. In caso contrario, le modifiche non verranno applicate.

11. Fare clic su **Applica**.

Correzione delle vulnerabilità del software di terze parti

Questa sezione descrive le funzionalità di Kaspersky Security Center relative alla correzione delle vulnerabilità del software installato nei dispositivi gestiti.

Scenario: Individuazione e correzione delle vulnerabilità del software di terze parti

Questa sezione fornisce uno scenario per individuare e correggere le vulnerabilità nei dispositivi gestiti che eseguono Windows. È possibile individuare e correggere le vulnerabilità del software nel sistema operativo e nel software di terze parti, incluso il software Microsoft.

Prerequisiti

- Kaspersky Security Center viene distribuito nell'organizzazione.
- Nell'organizzazione sono presenti dispositivi gestiti che eseguono Windows.
- È necessaria una connessione Internet affinché Administration Server esegua le seguenti attività:
  - Per creare un elenco di correzioni consigliate per le vulnerabilità del software Microsoft. L'elenco viene creato e aggiornato regolarmente dagli specialisti Kaspersky.
  - Per correggere le vulnerabilità in software di terze parti diverso dal software Microsoft.

Passaggi

L'individuazione e la correzione delle vulnerabilità del software prevede diversi passaggi:

1. **Ricerca delle vulnerabilità del software installato nei dispositivi gestiti**

   Per individuare le vulnerabilità del software installato nei dispositivi gestiti, eseguire l'attività *Trova vulnerabilità e aggiornamenti richiesti*. Al termine di questa attività, Kaspersky Security Center riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi specificati nelle proprietà dell'attività.

   L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. Se la procedura guidata non è stata eseguita, avviarla ora o creare l'attività manualmente.

   Istruzioni dettagliate:

   - Administration Console: Scansione delle applicazioni per rilevare la presenza di vulnerabilità, Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
   - Kaspersky Security Center Web Console: Creazione dell'attività Trova vulnerabilità e aggiornamenti richiesti, Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

2. **Analisi dell'elenco delle vulnerabilità del software rilevate**

   Visualizzare l'elenco **Vulnerabilità del software** e decidere quali vulnerabilità devono essere corrette. Per visualizzare informazioni dettagliate su ciascuna vulnerabilità, fare clic sul nome della vulnerabilità nell'elenco. Per ogni vulnerabilità nell'elenco, è anche possibile visualizzare le statistiche sulla vulnerabilità nei dispositivi gestiti.

   Istruzioni dettagliate:

   - Administration Console: Visualizzazione delle informazioni sulle vulnerabilità del software, Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti

- Kaspersky Security Center Web Console: Visualizzazione delle informazioni sulle vulnerabilità del software, Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti

3. **Configurazione della correzione delle vulnerabilità**

   Quando vengono rilevate le vulnerabilità del software, è possibile correggere le vulnerabilità del software nei dispositivi gestiti utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità*.

   L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per aggiornare e correggere le vulnerabilità del software di terze parti, incluso il software Microsoft, installato nei dispositivi gestiti. Questa attività consente di installare più aggiornamenti e correggere più vulnerabilità in base a determinate regole. Questa attività può essere creata solo se si dispone della licenza per la funzionalità Vulnerability e patch management. Per correggere le vulnerabilità del software l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* utilizza gli aggiornamenti software consigliati.

   L'attività *Correggi vulnerabilità* non richiede l'opzione di licenza per la funzionalità Vulnerability e patch management. Per utilizzare questa attività è necessario specificare manualmente le correzioni dell'utente per le vulnerabilità del software di terze parti elencato nelle impostazioni dell'attività. L'attività *Correggi vulnerabilità* utilizza le correzioni consigliate per il software Microsoft e le correzioni dell'utente per software di terze parti.

   È possibile avviare la Correzione guidata vulnerabilità che crea automaticamente una di queste attività oppure è possibile creare una di queste attività manualmente.

   Istruzioni dettagliate:

   - Administration Console: Selezione di correzioni utente per le vulnerabilità del software di terze parti, Correzione delle vulnerabilità delle applicazioni
   - Kaspersky Security Center Web Console: Selezione di correzioni utente per le vulnerabilità del software di terze parti, Correzione delle vulnerabilità del software di terze parti, Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità

4. **Pianificazione delle attività**

   Per assicurarsi che l'elenco delle vulnerabilità sia sempre aggiornato, pianificare l'attività *Trova vulnerabilità e aggiornamenti richiesti* affinché venga eseguita periodicamente in modo automatico. La frequenza media consigliata è una volta alla settimana.

   Se è stata creata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile pianificarla in modo che venga eseguita con la stessa frequenza dell'attività *Trova vulnerabilità e aggiornamenti richiesti* o con una frequenza inferiore. Quando si pianifica l'attività *Correggi vulnerabilità*, tenere presente che è necessario selezionare le correzioni per il software Microsoft o specificare ogni volta le correzioni utente per il software di terze parti prima di avviare l'attività.

   Quando si pianificano le attività, assicurarsi che al termine dell'attività *Trova vulnerabilità e aggiornamenti richiesti* venga avviata un'attività per correggere la vulnerabilità.

5. **Ignorare le vulnerabilità del software (facoltativo)**

   Se lo si desidera, è possibile ignorare le vulnerabilità del software da correggere in tutti i dispositivi gestiti o solo nei dispositivi gestiti selezionati.

   Istruzioni dettagliate:

   - Administration Console: Ignorare le vulnerabilità del software
   - Kaspersky Security Center Web Console: Ignorare le vulnerabilità del software

6. **Esecuzione di un'attività di correzione della vulnerabilità**

   Avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità*. Al termine dell'attività, assicurarsi che questa abbia lo stato *Completato* nell'elenco attività.

7. **Creare il rapporto sui risultati della correzione delle vulnerabilità del software (facoltativo)**

   Per visualizzare le statistiche dettagliate sulla correzione delle vulnerabilità, generare il Rapporto sulle vulnerabilità. Il rapporto visualizza informazioni sulle vulnerabilità del software che non sono state corrette. In tal modo è possibile avere un'idea sulla ricerca e la correzione delle vulnerabilità del software di terze parti, incluso il software Microsoft, presente nell'organizzazione.

   Istruzioni dettagliate:

   - Administration Console: Creazione e visualizzazione di un rapporto
   - Kaspersky Security Center Web Console: Generazione e visualizzazione di un rapporto

8. **Verifica della configurazione e individuazione e correzione delle vulnerabilità del software di terze parti**

   Assicurarsi di avere eseguito le seguenti operazioni:

   - Avere ottenuto e rivisto l'elenco delle vulnerabilità del software nei dispositivi gestiti
   - Avere eventualmente ignorato le vulnerabilità del software
   - Avere configurato l'attività per correggere le vulnerabilità
   - Avere pianificato le attività per individuare e correggere le vulnerabilità del software in modo che vengano avviate in sequenza
   - Aver controllato che sia stata eseguita l'attività per correggere le vulnerabilità del software

Risultati

Se è stata creata e configurata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, le vulnerabilità vengono corrette automaticamente nei dispositivi gestiti. Quando viene eseguita, l'attività collega l'elenco degli aggiornamenti software disponibili alle regole specificate nelle impostazioni dell'attività. Tutti gli aggiornamenti software che soddisfano i criteri nelle regole verranno scaricati nell'archivio di Administration Server e verranno installati per correggere le vulnerabilità del software.

Se è stata creata l'attività *Correggi vulnerabilità*, vengono corrette solo le vulnerabilità del software nel software Microsoft.

Informazioni sulla ricerca e la correzione delle vulnerabilità del software

Kaspersky Security Center rileva e corregge le vulnerabilità del software nei dispositivi gestiti che eseguono i sistemi operativi delle famiglie Microsoft Windows. Le vulnerabilità vengono rilevate nel sistema operativo e nel software di terze parti, incluso il software Microsoft.

Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Individuazione delle vulnerabilità del software

Per individuare le vulnerabilità del software, Kaspersky Security Center utilizza le caratteristiche del database delle vulnerabilità note. Questo database viene creato dagli specialisti di Kaspersky. Contiene informazioni sulle vulnerabilità, come la descrizione della vulnerabilità, la data di rilevamento della vulnerabilità, il livello di criticità della vulnerabilità. Per informazioni dettagliate sulle vulnerabilità del software, visitare il sito Web di Kaspersky.

Kaspersky Security Center utilizza l'attività *Trova vulnerabilità e aggiornamenti richiesti* per rilevare le vulnerabilità del software.

In alcuni casi le vulnerabilità rilevate in un sistema operativo Microsoft Windows possono essere corrette utilizzando uno dei seguenti metodi:

- Installazione di un aggiornamento per il sistema operativo.
- Aggiornamento del sistema operativo a una versione più recente (ad esempio da Windows 10 a Windows 11).

In questo scenario Kaspersky Security Center mostra due voci per la stessa vulnerabilità.

Correzione delle vulnerabilità del software

Per correggere le vulnerabilità del software Kaspersky Security Center utilizza gli aggiornamenti software rilasciati dai relativi fornitori. I metadati degli aggiornamenti software vengono scaricati nell'archivio di Administration Server a seguito dell'esecuzione delle seguenti attività:

- *Scarica aggiornamenti nell'archivio dell'Administration Server*. Questa attività ha lo scopo di scaricare i metadati degli aggiornamenti per software Kaspersky e di terze parti. Questa attività viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. È possibile creare manualmente l'attività Scarica aggiornamenti nell'archivio dell'Administration Server.
- *Esegui sincronizzazione di Windows Update*. Questa attività ha lo scopo di scaricare i metadati degli aggiornamenti per il software Microsoft.

Gli aggiornamenti software per correggere le vulnerabilità possono essere rappresentati come patch o pacchetti o di distribuzione completi. Gli aggiornamenti software che correggono le vulnerabilità del software vengono denominati *correzioni*. Le *correzioni consigliate* sono quelle consigliate per l'installazione dagli specialisti di Kaspersky. Le *correzioni dell'utente* sono quelle specificate manualmente per l'installazione da parte degli utenti. Per installare una correzione dell'utente, è necessario creare un pacchetto di installazione contenente questa correzione.

Se si dispone della licenza di Kaspersky Security Center con la funzionalità Vulnerability e patch management, per correggere le vulnerabilità del software è possibile utilizzare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. Questa attività corregge automaticamente più vulnerabilità installando le correzioni consigliate. Per questa attività è possibile configurare manualmente determinate regole per correggere più vulnerabilità.

Se non si dispone della licenza di Kaspersky Security Center con la funzionalità Vulnerability e patch management, per correggere le vulnerabilità del software è possibile utilizzare l'attività *Correggi vulnerabilità*. Tramite questa attività è possibile correggere le vulnerabilità installando le correzioni consigliate per il software Microsoft e le correzioni dell'utente per altri software di terze parti.

Per motivi di sicurezza, tutti gli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management vengono automaticamente analizzati alla ricerca di malware dalle tecnologie Kaspersky. Queste tecnologie vengono utilizzate per il controllo automatico dei file e includono la scansione virus, l'analisi statica, l'analisi dinamica, l'analisi del comportamento nell'ambiente sandbox e il machine learning.

Gli esperti Kaspersky non eseguono l'analisi manuale degli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management. Inoltre, gli esperti di Kaspersky non ricercano vulnerabilità (note o sconosciute) o funzionalità non documentate in tali aggiornamenti, né eseguono altri tipi di analisi degli aggiornamenti diversi da quelli specificati nel paragrafo precedente.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Per correggere alcune vulnerabilità del software, è necessario accettare il Contratto di licenza con l'utente finale (EULA) per l'installazione del software, se è richiesta l'accettazione del Contratto di licenza con l'utente finale. Se non si accetta il Contratto di licenza con l'utente finale, la vulnerabilità del software non viene corretta.

Visualizzazione delle informazioni sulle vulnerabilità del software

Per visualizzare un elenco delle vulnerabilità rilevate nei dispositivi client:

Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Vulnerabilità del software**.

La pagina visualizza un elenco delle vulnerabilità nelle applicazioni rilevate nei dispositivi gestiti.

Per ottenere informazioni su una vulnerabilità selezionata:

Selezionare **Proprietà** dal menu di scelta rapida della vulnerabilità.

Verrà visualizzata la finestra delle proprietà della vulnerabilità, in cui sono visualizzate le seguenti informazioni:

- Applicazione in cui è stata rilevata la vulnerabilità.
- Elenco di dispositivi in cui è stata rilevata la vulnerabilità.
- Informazioni sull'applicazione o meno di una correzione per la vulnerabilità.

Per visualizzare il rapporto su tutte le vulnerabilità rilevate:

Nella cartella **Vulnerabilità del software** fare clic sul collegamento **Visualizza rapporto sulle vulnerabilità**.

Verrà generato un rapporto sulle vulnerabilità nelle applicazioni installate nei dispositivi. È possibile visualizzare questo rapporto nel nodo con il nome dell'Administration Server corrispondente, aprendo la scheda **Rapporti**.

Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti

È possibile visualizzare le statistiche per ogni vulnerabilità del software nei dispositivi gestiti. Le statistiche sono rappresentate sotto forma di diagramma. Il diagramma mostra il numero di dispositivi con i seguenti stati:

- *Ignorato in: <numero di dispositivi>*. Questo stato viene assegnato se, nelle proprietà della vulnerabilità, è stata impostata manualmente l'opzione per ignorare la vulnerabilità.
- *Corretto in: <numero di dispositivi>*. Questo stato viene assegnato se l'attività di correzione della vulnerabilità è stata completata.
- *Correzione pianificata in data: <numero di dispositivi>*. Questo stato viene assegnato se è stata creata l'attività per correggere la vulnerabilità ma l'attività non è ancora stata eseguita.
- *Patch applicata in: <numero di dispositivi>*. Questo stato viene assegnato se è stato selezionato manualmente un aggiornamento software per correggere la vulnerabilità ma questo software aggiornato non ha corretto la vulnerabilità.
- *È necessaria una correzione in: <numero di dispositivi>*. Questo stato viene assegnato se la vulnerabilità è stata corretta solo in alcuni dispositivi gestiti e deve essere corretta in più dispositivi gestiti.

Per visualizzare le statistiche di una vulnerabilità nei dispositivi gestiti:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Vulnerabilità del software**.

   La pagina visualizza un elenco delle vulnerabilità nelle applicazioni rilevate nei dispositivi gestiti.

2. Selezionare una vulnerabilità per la quale si desidera visualizzare le statistiche.

   Nella sezione relativa a un oggetto selezionato viene visualizzato un diagramma degli stati di vulnerabilità. Facendo clic su uno stato, viene aperto un elenco dei dispositivi in cui la vulnerabilità ha lo stato selezionato.

Scansione delle applicazioni per rilevare la presenza di vulnerabilità

Se è stata configurata l'applicazione tramite l'Avvio rapido guidato, l'attività *Scansione vulnerabilità* viene creata automaticamente. È possibile visualizzare l'attività nella cartella **Dispositivi gestiti**, nella scheda **Attività**.

Per creare un'attività per la scansione delle vulnerabilità delle applicazioni installate nei dispositivi client:

1. Nella struttura della console selezionare **Avanzate** → **Gestione applicazioni**, quindi selezionare la sottocartella **Vulnerabilità del software**.

2. Nell'area di lavoro selezionare **Azioni aggiuntive** → **Configura scansione vulnerabilità**.

   Se esiste già un'attività per la scansione delle vulnerabilità, verrà visualizzata la scheda **Attività** della cartella **Dispositivi gestiti**, con l'attività esistente selezionata. In caso contrario, verrà avviata la Creazione guidata dell'attività Trova vulnerabilità e aggiornamenti richiesti. Seguire le istruzioni della procedura guidata.

3. Nella finestra **Selezionare il tipo di attività** selezionare **Trova vulnerabilità e aggiornamenti richiesti**.

4. Nella pagina **Impostazioni** della procedura guidata specificare le impostazioni dell'attività nel modo seguente:

- **Cerca vulnerabilità e aggiornamenti elencati da Microsoft**

  Durante la ricerca di vulnerabilità e aggiornamenti, Kaspersky Security Center utilizza le informazioni sugli aggiornamenti Microsoft applicabili della sorgente degli aggiornamenti di Microsoft e disponibili al momento.

  È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft e gli aggiornamenti delle applicazioni di terze parti.

  Per impostazione predefinita, questa opzione è abilitata.

  Le informazioni sugli aggiornamenti facoltativi di Microsoft Windows non vengono inviate ad Administration Server.

- **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati**

Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft. I seguenti server possono operare come sorgente degli aggiornamenti Microsoft:

- Kaspersky Security Center Administration Server (vedere le impostazioni del criterio di Network Agent)
- Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione
- Server degli aggiornamenti Microsoft

Se questa opzione è abilitata, Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft per aggiornare le informazioni sugli aggiornamenti di Microsoft Windows applicabili.

Se questa opzione è disabilitata, l'Agente di Windows Update in un dispositivo gestito utilizza le informazioni sugli aggiornamenti di Microsoft Windows applicabili ricevuti dalla sorgente degli aggiornamenti Microsoft in precedenza.

La connessione alla sorgente degli aggiornamenti Microsoft può comportare un notevole utilizzo di risorse. Potrebbe essere necessario disabilitare questa opzione se è stata impostata una connessione standard a questa sorgente degli aggiornamenti in un'altra attività o nelle proprietà del criterio Network Agent, nella sezione **Vulnerabilità e aggiornamenti software**. Se non si desidera disabilitare questa opzione, per ridurre l'overload del Server è possibile configurare la pianificazione delle attività in modo da utilizzare il ritardo casuale per l'avvio delle attività entro 360 minuti.

Per impostazione predefinita, questa opzione è abilitata.

La combinazione delle seguenti opzioni delle impostazioni del criterio di Network Agent definisce il modo in cui si ottengono gli aggiornamenti:

- In un dispositivo gestito, l'Agente di Windows Update si connette al server degli aggiornamenti per ottenere gli aggiornamenti solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è abilitata nelle proprietà dell'attività *Trova vulnerabilità e aggiornamenti richiesti* e l'opzione **Modalità di ricerca di Windows Update** è impostata su **Attiva** nelle impostazioni del criterio di Network Agent.
- Se non è necessario che Network Agent avvii una connessione alla sorgente degli aggiornamenti di Microsoft Windows e scarichi gli aggiornamenti durante l'esecuzione dell'attività *Scansione vulnerabilità*, è possibile impostare l'opzione **Modalità di ricerca di Windows Update** su **Passiva**, mentre l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** deve rimanere abilitata. In questo modo, è possibile risparmiare risorse e utilizzare gli aggiornamenti di Windows ricevuti in precedenza per la scansione delle vulnerabilità. È possibile utilizzare la modalità passiva se si configura la ricezione degli aggiornamenti DI Microsoft Windows in modo diverso. Se la ricezione degli aggiornamenti di Microsoft Windows non è configurata in altro modo, non impostare l'opzione **Modalità di ricerca di Windows Update** su **Passiva**, poiché in questo caso non si riceveranno le informazioni sugli aggiornamenti, in alcun caso.
- Indipendentemente dallo stato dell'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** (abilitata o disabilitata), se l'opzione **Modalità di ricerca di Windows Update** è impostata su **Disabilitata**, Kaspersky Security Center non richiede informazioni sugli aggiornamenti.

- Cerca vulnerabilità e aggiornamenti di terze parti elencati da Kaspersky

Se questa opzione è abilitata, Kaspersky Security Center esegue la ricerca delle vulnerabilità e degli aggiornamenti richiesti per le applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) nel Registro di sistema di Windows e nelle cartelle specificate con **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**. L'elenco completo delle applicazioni di terze parti supportate è gestito da Kaspersky.

Se questa opzione è disabilitata, Kaspersky Security Center non esegue la ricerca di vulnerabilità e aggiornamenti richiesti per le applicazioni di terze parti. È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft Windows e gli aggiornamenti delle applicazioni di terze parti.

Per impostazione predefinita, questa opzione è abilitata.

- **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**

  Cartelle in cui Kaspersky Security Center esegue la ricerca delle applicazioni di terze parti che richiedono la correzione delle vulnerabilità e l'installazione di aggiornamenti. È possibile utilizzare le variabili di sistema.

  Specificare le cartelle in cui sono installate le applicazioni. Per impostazione predefinita, l'elenco contiene le cartelle di sistema in cui viene installata la maggior parte delle applicazioni.

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive i file di traccia anche se la scrittura dei file di traccia è disabilitata per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

5. Nella pagina **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N settimane**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

  - **Settimanale**

    L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- In base ai giorni della settimana

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- Mensile

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- Manualmente

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- Ogni mese nei giorni specificati delle settimane selezionate

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- Quando vengono scaricati nuovi aggiornamenti nell'archivio

  L'attività viene eseguita dopo il download degli aggiornamenti nell'archivio. È ad esempio possibile utilizzare questa pianificazione per l'attività Trova vulnerabilità e aggiornamenti richiesti.

- Durante un'epidemia di virus

L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

- Anti-virus per workstation e file server
- Anti-virus per la difesa perimetrale
- Anti-virus per i sistemi di posta

Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

  L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

  È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

  Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

  - Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
  - Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

    Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
  - Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

6. Nella pagina **Definire il nome dell'attività** della procedura guidata specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

7. Nella pagina **Completare la creazione dell'attività** della procedura guidata fare clic sul pulsante **Fine** per chiudere la procedura guidata.

   Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Al termine della procedura guidata, l'attività **Trova vulnerabilità e aggiornamenti richiesti** verrà visualizzata nell'elenco delle attività della cartella **Dispositivi gestiti**, nella scheda **Attività**.

Oltre alle impostazioni specificate durante la creazione dell'attività, è possibile modificare altre proprietà di un'attività creata.

Dopo il completamento dell'attività *Trova vulnerabilità e aggiornamenti richiesti*, Administration Server visualizza un elenco delle vulnerabilità rilevate nelle applicazioni installate nel dispositivo. Vengono inoltre visualizzati tutti gli aggiornamenti software necessari per correggere le vulnerabilità rilevate.

Se si visualizza 0x80240033 "Errore 80240033 di Windows Update Agent ("Non è stato possibile scaricare le condizioni di licenza")", è possibile risolvere questo problema tramite il Registro di sistema di Windows.

Administration Server non visualizza l'elenco degli aggiornamenti software richiesti quando si eseguono due attività di seguito: l'attività *Esegui sincronizzazione di Windows Update* con l'opzione **Scarica file di installazione rapidi** disabilitata e l'attività *Trova vulnerabilità e aggiornamenti richiesti*. Per visualizzare l'elenco degli aggiornamenti software richiesti, è necessario eseguire nuovamente l'attività *Trova vulnerabilità e aggiornamenti richiesti*.

Network Agent riceve le informazioni su qualsiasi aggiornamento disponibile per Windows e altri prodotti Microsoft da Windows Update o da Administration Server, se Administration Server opera come WSUS. Le informazioni vengono trasmesse all'avvio delle applicazioni (se questo è consentito dal criterio) e a ogni esecuzione dell'attività *Ricerca di vulnerabilità e aggiornamenti richiesti* nei dispositivi client.

Correzione delle vulnerabilità delle applicazioni

Se è stato selezionato **Cerca e installa gli aggiornamenti richiesti** nella pagina **Impostazioni per la gestione degli aggiornamenti** dell'Avvio rapido guidato, verrà creata automaticamente l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. L'attività viene visualizzata nell'area di lavoro della cartella **Dispositivi gestiti**, nella scheda **Attività**.

In caso contrario, è possibile eseguire qualsiasi delle seguenti operazioni:

- Creare un'attività per la correzione delle vulnerabilità tramite l'installazione degli aggiornamenti disponibili.
- Aggiungere una regola per la correzione di una vulnerabilità a un'attività esistente per la correzione delle vulnerabilità.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Correzione delle vulnerabilità tramite la creazione di un'attività di correzione delle vulnerabilità

È possibile eseguire qualsiasi delle seguenti operazioni:

- Creare un'attività per la correzione di più vulnerabilità che corrispondono a determinate regole.
- Selezionare una vulnerabilità e creare un'attività per la correzione di tale vulnerabilità e delle vulnerabilità analoghe.

Per correggere le vulnerabilità che corrispondono a determinate regole:

1. Nella struttura della console, selezionare Administration Server nei dispositivi per i quali si desidera correggere le vulnerabilità.
2. Nel menu **Visualizza** della finestra principale dell'applicazione selezionare **Configura interfaccia**.
3. Nella finestra visualizzata selezionare la casella di controllo **Visualizza Vulnerability e patch management**, quindi fare clic su **OK**.
4. Nella finestra con il messaggio dell'applicazione fare clic su **OK**.
5. Riavviare Administration Console, in modo che le modifiche abbiano effetto.
6. Nella struttura della console selezionare la cartella **Dispositivi gestiti**.
7. Nell'area di lavoro selezionare la scheda **Attività**.
8. Fare clic sul pulsante **Crea attività** per eseguire la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

9. Nella pagina **Selezionare il tipo di attività** della procedura guidata selezionare **Installa aggiornamenti richiesti e correggi vulnerabilità**.

   Se l'attività non viene visualizzata, verificare se l'account dispone dei diritti di **lettura**, **modifica** ed **esecuzione** per l'area funzionale **Gestione sistema**: **Vulnerability e patch management**. Senza questi diritti di accesso, non è possibile creare e configurare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.

10. Nella pagina **Impostazioni** della procedura guidata specificare le impostazioni dell'attività nel modo seguente:

- **Specificare le regole per l'installazione degli aggiornamenti**

  Queste regole vengono applicate all'installazione degli aggiornamenti nei dispositivi client. Se non si specificano regole, l'attività non esegue alcuna operazione. Per informazioni sulle operazioni con le regole, vedere Regole per l'installazione dell'aggiornamento.

- **Avvia l'installazione al riavvio o all'arresto del dispositivo**

  Se questa opzione è abilitata, gli aggiornamenti vengono installati al riavvio o all'arresto del dispositivo. In caso contrario, gli aggiornamenti vengono installati in base a una pianificazione.

  Utilizzare questa opzione se l'installazione degli aggiornamenti può influire sulle prestazioni del dispositivo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Installa i componenti generali del sistema richiesti**

  Se questa opzione è abilitata, prima di installare un aggiornamento l'applicazione installa automaticamente tutti i componenti di sistema generali (prerequisiti) richiesti per installare l'aggiornamento. Questi prerequisiti possono ad esempio essere aggiornamenti del sistema operativo.

  Se questa opzione è disabilitata, può essere necessario installare manualmente i prerequisiti.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Consenti l'installazione di nuove versioni dell'applicazione durante gli aggiornamenti**

  Se questa opzione è abilitata, gli aggiornamenti sono consentiti se implicano l'installazione di una nuova versione di un'applicazione software.

  Se questa opzione è disabilitata, l'upgrade del software non viene eseguito. È quindi possibile installare le nuove versioni del software manualmente o tramite un'altra attività. È ad esempio possibile utilizzare questa opzione se l'infrastruttura aziendale non è supportata da una nuova versione del software o se si desidera verificare un aggiornamento in un'infrastruttura di test.

  Per impostazione predefinita, questa opzione è abilitata.

  L'upgrade dell'applicazione può causare un malfunzionamento delle applicazioni dipendenti installate nei dispositivi client.

- **Scarica gli aggiornamenti nel dispositivo senza installarli**

  Se questa opzione è abilitata, l'applicazione scarica gli aggiornamenti nel dispositivo client ma non li installa automaticamente. È quindi possibile installare manualmente gli aggiornamenti scaricati.

  Gli aggiornamenti Microsoft vengono scaricati nell'archiviazione di sistema di Windows. Gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) vengono scaricati nella cartella specificata nel campo **Scarica aggiornamenti in**.

  Se questa opzione è disabilitata, gli aggiornamenti vengono installati automaticamente nel dispositivo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica aggiornamenti in**

  Questa cartella viene utilizzata per scaricare gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft).

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive i file di traccia anche se la scrittura dei file di traccia è disabilitata per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

11. Nella pagina **Selezione dell'opzione per il riavvio del sistema operativo** della procedura guidata selezionare l'azione da eseguire quando il sistema operativo nei dispositivi client deve essere riavviato dopo l'operazione:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

12. Nella pagina **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N settimane**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

  - **Settimanale**

    L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  > Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- **Durante un'epidemia di virus**

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

- Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
- Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

  Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
- Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

13. Nella pagina **Definire il nome dell'attività** della procedura guidata specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

14. Nella pagina **Completare la creazione dell'attività** della procedura guidata fare clic sul pulsante **Fine** per chiudere la procedura guidata.

    Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Al termine della procedura guidata, verrà creata l'attività **Installa aggiornamenti richiesti e correggi vulnerabilità**, che sarà visualizzata nella cartella **Attività**.

Oltre alle impostazioni specificate durante la creazione dell'attività, è possibile modificare altre proprietà di un'attività creata.

Se i risultati dell'attività contengono l'errore 0x80240033 "Errore 80240033 di Windows Update Agent ("Non è stato possibile scaricare le condizioni di licenza")", è possibile risolvere questo problema tramite il Registro di sistema di Windows.

Per correggere una specifica vulnerabilità e quelle analoghe:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Vulnerabilità del software**.

2. Selezionare la vulnerabilità che si desidera correggere.

3. Fare clic sul pulsante **Esegui Correzione guidata vulnerabilità**.

   Verrà avviata la Correzione guidata vulnerabilità.

   Le funzionalità della Correzione guidata vulnerabilità sono disponibili solo con la licenza per Vulnerability e patch management.

   Seguire le istruzioni della procedura guidata.

4. Nella finestra **Cerca attività di correzione vulnerabilità esistenti** specificare i seguenti parametri:

   - **Mostra solo le attività che consentono di correggere la vulnerabilità**

     Se questa opzione è abilitata, la Correzione guidata vulnerabilità cerca le attività esistenti per la correzione della vulnerabilità selezionata.

     Se questa opzione è disabilitata o se la ricerca non recupera attività applicabili, la Correzione guidata vulnerabilità richiede di creare una regola o un'attività per la correzione della vulnerabilità selezionata.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Approva aggiornamenti in grado di correggere la vulnerabilità**

     Gli aggiornamenti che correggono una vulnerabilità verranno approvati per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

     Per impostazione predefinita, questa opzione è disabilitata.

5. Se si sceglie di eseguire la ricerca delle attività esistenti di correzione delle vulnerabilità e la ricerca recupera alcune attività, è possibile visualizzare le proprietà di queste attività o avviarle manualmente. Non sono necessarie ulteriori operazioni.

   In caso contrario, fare clic sul pulsante **Nuova attività di correzione vulnerabilità**.

6. Selezionare il tipo di regola di correzione delle vulnerabilità da aggiungere alla nuova attività e fare clic sul pulsante **Fine**.

7. Scegliere l'operazione da eseguire quando viene richiesto se installare tutti gli aggiornamenti precedenti dell'applicazione. Fare clic su **Sì** se si desidera installare in modo incrementale le versioni successive dell'applicazione, se questo è necessario per l'installazione degli aggiornamenti selezionati. Fare clic su **No** se si desidera eseguire l'aggiornamento delle applicazioni in modo diretto, senza installare le versioni successive. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

   Viene avviata la Creazione guidata attività di installazione aggiornamenti e correzione vulnerabilità. Seguire le istruzioni della procedura guidata.

8. Nella pagina **Selezione dell'opzione per il riavvio del sistema operativo** della procedura guidata selezionare l'azione da eseguire quando il sistema operativo nei dispositivi client deve essere riavviato dopo l'operazione:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

9. Nella pagina **Selezionare i dispositivi a cui assegnare l'attività** della procedura guidata selezionare una delle seguenti opzioni:

- **Seleziona i dispositivi della rete rilevati da Administration Server**

  L'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

  Questa opzione può ad esempio essere utilizzata in un'attività per l'installazione di Network Agent nei dispositivi non assegnati.

- **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**

  È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

  Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

- **Assegna un'attività a una selezione dispositivi**

  L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

- **Assegna un'attività a un gruppo di amministrazione**

  L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

  Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

10. Nella pagina **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N settimane**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

  - **Settimanale**

    L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  > Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- **Durante un'epidemia di virus**

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

- Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
- Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

  Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
- Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

11. Nella pagina **Definire il nome dell'attività** della procedura guidata specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

12. Nella pagina **Completare la creazione dell'attività** della procedura guidata fare clic sul pulsante **Fine** per chiudere la procedura guidata.

    Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Al termine della procedura guidata, verrà creata l'attività **Installa aggiornamenti richiesti e correggi vulnerabilità**, che sarà visualizzata nella cartella **Attività**.

Oltre alle impostazioni specificate durante la creazione dell'attività, è possibile modificare altre proprietà di un'attività creata.

Correzione di una vulnerabilità tramite l'aggiunta di una regola a un'attività di correzione delle vulnerabilità esistente

Per correggere una vulnerabilità tramite l'aggiunta di una regola a un'attività di correzione delle vulnerabilità esistente:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Vulnerabilità del software**.

2. Selezionare la vulnerabilità che si desidera correggere.

3. Fare clic sul pulsante **Esegui Correzione guidata vulnerabilità**.

   Verrà avviata la Correzione guidata vulnerabilità.

Le funzionalità della Correzione guidata vulnerabilità sono disponibili solo con la licenza per Vulnerability e patch management.

Seguire le istruzioni della procedura guidata.

4. Nella finestra **Cerca attività di correzione vulnerabilità esistenti** specificare i seguenti parametri:

   - **Mostra solo le attività che consentono di correggere la vulnerabilità**

     Se questa opzione è abilitata, la Correzione guidata vulnerabilità cerca le attività esistenti per la correzione della vulnerabilità selezionata.

     Se questa opzione è disabilitata o se la ricerca non recupera attività applicabili, la Correzione guidata vulnerabilità richiede di creare una regola o un'attività per la correzione della vulnerabilità selezionata.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Approva aggiornamenti in grado di correggere la vulnerabilità**

     Gli aggiornamenti che correggono una vulnerabilità verranno approvati per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

     Per impostazione predefinita, questa opzione è disabilitata.

5. Se si sceglie di eseguire la ricerca delle attività esistenti di correzione delle vulnerabilità e la ricerca recupera alcune attività, è possibile visualizzare le proprietà di queste attività o avviarle manualmente. Non sono necessarie ulteriori operazioni.

   In caso contrario, fare clic sul pulsante **Aggiungi regola di correzione vulnerabilità a un'attività esistente**.

6. Selezionare l'attività a cui aggiungere una regola, quindi fare clic sul pulsante **Aggiungi regola**.

   È inoltre possibile visualizzare le proprietà delle attività esistenti, avviarle manualmente o creare una nuova attività.

7. Selezionare il tipo di regola da aggiungere all'attività selezionata e fare clic sul pulsante **Fine**.

8. Scegliere l'operazione da eseguire quando viene richiesto se installare tutti gli aggiornamenti precedenti dell'applicazione. Fare clic su **Sì** se si desidera installare in modo incrementale le versioni successive dell'applicazione, se questo è necessario per l'installazione degli aggiornamenti selezionati. Fare clic su **No** se si desidera eseguire l'aggiornamento delle applicazioni in modo diretto, senza installare le versioni successive. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

Una nuova regola per la correzione delle vulnerabilità viene aggiunta all'attività **Installa aggiornamenti richiesti e correggi vulnerabilità** esistente.

Correzione delle vulnerabilità in una rete isolata

Questa sezione descrive i passaggi possibili per correggere le vulnerabilità del software di terze parti nei dispositivi gestiti connessi ad Administration Server che non dispongono dell'accesso a Internet.

Scenario: Correzione delle vulnerabilità del software di terze parti in una rete isolata

È possibile installare gli aggiornamenti e correggere le vulnerabilità del software di terze parti installato nei dispositivi gestiti in una rete isolata. Tali reti includono Administration Server e dispositivi gestiti ad essi collegati che non hanno accesso a Internet. Per correggere le vulnerabilità in questo tipo di rete, è necessario un Administration Server connesso a Internet. Sarà quindi possibile scaricare le patch (gli aggiornamenti richiesti) utilizzando l'Administration Server con accesso a Internet, quindi trasmettere le patch agli Administration Server isolati.

> È possibile scaricare gli aggiornamenti software di terze parti rilasciati dai fornitori di software, ma non è possibile scaricare gli aggiornamenti per il software Microsoft in Administration Server isolati utilizzando Kaspersky Security Center.

Per scoprire come funziona il processo di correzione delle vulnerabilità in una rete isolata, vedere la descrizione e lo schema di questo processo.

Prerequisiti

Prima di iniziare, procedere come segue:

1. Assegnare un dispositivo per la connessione a Internet e il download delle patch. Questo dispositivo verrà conteggiato come Administration Server con accesso a Internet.
2. Installare Kaspersky Security Center, versione 14 o successiva, nei seguenti dispositivi:
   - Dispositivo assegnato, che fungerà da Administration Server con accesso a Internet.
   - Dispositivi isolati, che fungeranno da Administration Server isolati da Internet (di seguito denominati Administration Server isolati).
3. Assicurarsi che ogni Administration Server disponga di spazio su disco sufficiente per scaricare e archiviare aggiornamenti e patch.

Passaggi

L'installazione degli aggiornamenti e la correzione delle vulnerabilità del software di terze parti nei dispositivi gestiti di Administration Server isolati prevede le fasi seguenti:

1. **Configurazione di Administration Server con accesso a Internet**

   Fornire ad Administration Server l'accesso a Internet per gestire le richieste relative agli aggiornamenti software di terze parti necessari e per scaricare le patch.

2. **Configurazione di Administration Server isolati**

   Predisporre gli Administration Server isolati in modo che possano formare regolarmente elenchi degli aggiornamenti necessari e gestire le patch scaricate dall'Administration Server con accesso a Internet. Dopo la configurazione, gli Administration Server isolati non tentano più di scaricare le patch da Internet. In alternativa, ricevono gli aggiornamenti tramite patch.

3. **Trasmissione di patch e installazione di aggiornamenti in Administration Server isolati**

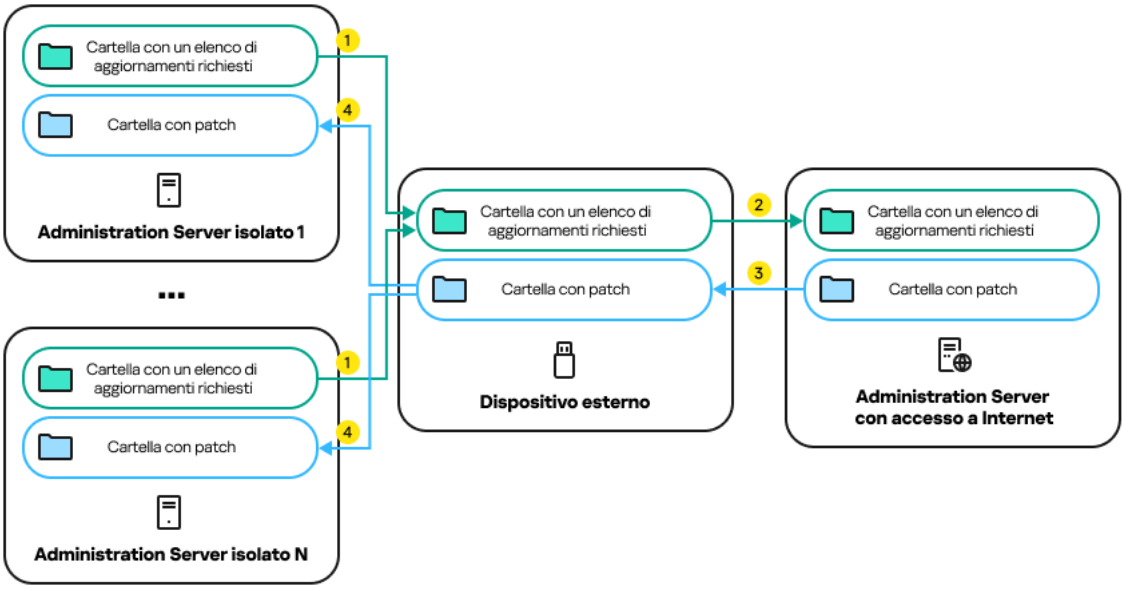
Al termine della configurazione degli Administration Server, è possibile trasmettere le patch e gli elenchi degli aggiornamenti necessari tra l'Administration Server con accesso a Internet e gli Administration Server isolati. Successivamente, gli aggiornamenti delle patch verranno installati nei dispositivi gestiti utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.

Risultati

Pertanto, gli aggiornamenti software di terze parti vengono trasmessi agli Administration Server isolati e installati nei dispositivi gestiti collegati tramite Kaspersky Security Center. È sufficiente configurare gli Administration Server una sola volta. Dopodiché sarà possibile ricevere gli aggiornamenti al bisogno, ad esempio una o più volte al giorno.

Informazioni sulla correzione delle vulnerabilità del software di terzi in una rete isolata

Il processo di correzione delle vulnerabilità del software di terzi in una rete isolata è mostrato nella figura e descritto di seguito. È possibile ripetere questo processo periodicamente.



Il processo di trasmissione delle patch e l'elenco degli aggiornamenti necessari tra Administration Server con accesso a Internet e Administration Server isolati

Ogni Administration Server isolato da Internet (di seguito denominato Administration Server isolato) genera un elenco di aggiornamenti che devono essere installati nei dispositivi gestiti connessi a tale Administration Server. L'elenco degli aggiornamenti richiesti è archiviato in una cartella specifica e presenta una serie di file binari. Ciascun file ha un nome che contiene l'ID della patch con l'aggiornamento richiesto. Di conseguenza, ogni file nell'elenco fa riferimento a una patch specifica.

Utilizzando un dispositivo esterno, si trasferisce l'elenco degli aggiornamenti richiesti dall'Administration Server isolato all'Administration Server allocato con accesso a Internet. Successivamente, l'Administration Server allocato scarica le patch da Internet e le inserisce in una cartella separata.

Quando tutte le patch vengono scaricate e posizionate nella relativa cartella, le patch vengono spostate in ogni Administration Server isolato da cui è stato prelevato un elenco degli aggiornamenti richiesti. Le patch vengono salvate nella cartella creata appositamente per loro sull'Administration Server isolato. Di conseguenza, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* esegue le patch e installa gli aggiornamenti nei dispositivi gestiti degli Administration Server isolati.

Configurazione dell'Administration Server con accesso a Internet per correggere le vulnerabilità in una rete isolata

Per prepararsi a correggere le vulnerabilità e trasmettere le patch in una rete isolata, configurare prima di tutto un Administration Server con l'accesso a Internet, quindi configurare gli Administration Server isolati.

Per configurare un Administration Server con l'accesso a Internet:

1. Creare due cartelle su un disco in cui è installato Administration Server:

   - Una cartella per l'elenco degli aggiornamenti necessari
   - Cartella per le patch

   È possibile nominare queste cartelle in qualsiasi modo.

2. Concedere Modifica i diritti di accesso al gruppo KL Admins nelle cartelle create, utilizzando gli strumenti di amministrazione standard del sistema operativo.

3. Utilizzare l'utilità klscflag per scrivere i percorsi delle cartelle nelle proprietà di Administration Server.

   Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

4. Immettere i seguenti comandi nel prompt dei comandi di Windows:

   - Per impostare il percorso della cartella per le patch:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<percorso della cartella>"`
   - Per impostare il percorso della cartella per un elenco degli aggiornamenti necessari:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<percorso della cartella>"`

   Esempio: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "C:\<cartella delle patch>"`

5. Se necessario, utilizzare l'utilità klscflag per specificare la frequenza con cui Administration Server deve verificare la presenza di nuove richieste di patch:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <valore in secondi>`

   Il valore predefinito è 120 secondi.

   Esempio: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. Creare l'attività *Trova vulnerabilità e aggiornamenti richiesti* per ottenere informazioni sulle patch per il software di terze parti installato nei dispositivi gestiti, quindi impostare la pianificazione dell'attività.

7. Creare l'attività *Correggi vulnerabilità* per specificare le patch per il software di terze parti utilizzato per correggere le vulnerabilità, quindi impostare la pianificazione dell'attività.

   Eseguire le attività manualmente se si desidera che vengano eseguite prima di quanto specificato nella pianificazione. L'ordine in cui vengono avviate le attività è importante. L'attività *Correggi vulnerabilità* deve essere eseguita al termine dell'attività *Trova vulnerabilità e aggiornamenti richiesti*.

8. Riavviare il servizio Administration Server.

Adesso l'Administration Server con accesso a Internet è pronto per scaricare e trasmettere aggiornamenti agli Administration Server isolati. Prima di iniziare a correggere le vulnerabilità, configurare gli Administration Server isolati.

Configurazione di Administration Server isolati per la correzione delle vulnerabilità in una rete isolata

Al termine della configurazione di Administration Server con l'accesso a Internet, preparare tutti gli Administration Server isolati nella rete, così da correggere le vulnerabilità e installare gli aggiornamenti nei dispositivi gestiti connessi agli Administration Server isolati.

Per configurare gli Administration Server isolati, eseguire le seguenti azioni su ogni Administration Server:

1. Attivare una chiave di licenza per la funzionalità Vulnerability e patch management (VAPM).

2. Creare due cartelle su un disco in cui è installato Administration Server:

   - Una cartella in cui verrà visualizzato l'elenco degli aggiornamenti necessari
   - Cartella per le patch

   È possibile nominare queste cartelle in qualsiasi modo.

3. Concedere l'autorizzazione Modifica al gruppo *KL Admins* nelle cartelle create, utilizzando gli strumenti di amministrazione standard del sistema operativo.

4. Utilizzare l'utilità klscflag per scrivere i percorsi delle cartelle nelle proprietà di Administration Server.

   Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

5. Immettere i seguenti comandi nel prompt dei comandi di Windows:

   - Per impostare il percorso della cartella per le patch:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<percorso della cartella>"`
   - Per impostare il percorso della cartella per un elenco degli aggiornamenti necessari:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<percorso della cartella>"`

   Esempio: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "C:\<cartella delle patch>"`

6. Se necessario, utilizzare l'utilità klscflag per specificare la frequenza con cui l'Administration Server isolato deve verificare la presenza di nuove patch:
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <valore in secondi>
   ```
   Il valore predefinito è 120 secondi.
   Esempio: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. Se necessario, utilizzare l'utilità klscflag per calcolare gli hash SHA256 delle patch:
   ```
   klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1
   ```
   Se si immette questo comando, è possibile assicurarsi che le patch non siano state modificate durante il trasferimento all'Administration Server isolato e di aver ricevuto le patch corrette con gli aggiornamenti richiesti.
   Per impostazione predefinita, Kaspersky Security Center non calcola gli hash SHA256 delle patch. Se si abilita questa opzione, dopo che l'Administration Server isolato ha ricevuto le patch, Kaspersky Security Center calcola gli hash e confronta i valori acquisiti con gli hash archiviati nel database di Administration Server. Se l'hash calcolato non corrisponde all'hash nel database, si verifica un errore ed è necessario sostituire le patch errate.

8. Creare l'attività *Trova vulnerabilità e aggiornamenti richiesti* per ottenere informazioni sulle patch per il software di terze parti installato nei dispositivi gestiti, quindi impostare la pianificazione dell'attività.

9. Creare l'attività *Correggi vulnerabilità* per specificare le patch per il software di terze parti utilizzato per correggere le vulnerabilità, quindi impostare la pianificazione dell'attività.
   Eseguire le attività manualmente se si desidera che vengano eseguite prima di quanto specificato nella pianificazione. L'ordine in cui vengono avviate le attività è importante. L'attività *Correggi vulnerabilità* deve essere eseguita al termine dell'attività *Trova vulnerabilità e aggiornamenti richiesti*.

10. Riavviare il servizio Administration Server.

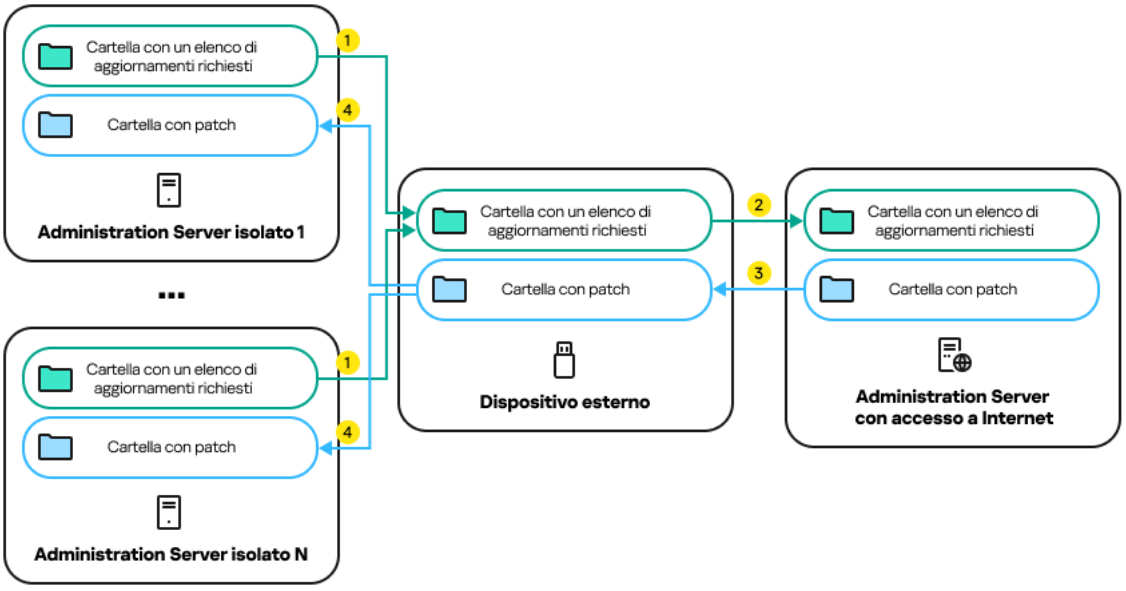
Dopo aver configurato tutti gli Administration Server, è possibile spostare le patch e gli elenchi degli aggiornamenti necessari e correggere le vulnerabilità del software di terze parti nei dispositivi gestiti nella rete isolata.

Trasmissione delle patch e installazione degli aggiornamenti in una rete isolata

Al termine della configurazione degli Administration Server, è possibile trasferire patch che contengono gli aggiornamenti richiesti dall'Administration Server con accesso a Internet agli Administration Server isolati. È possibile trasmettere e installare gli aggiornamenti tutte le volte necessarie, ad esempio una o più volte al giorno.

È necessario un dispositivo esterno, ad esempio un'unità rimovibile per trasferire le patch e l'elenco degli aggiornamenti necessari tra gli Administration Server. Assicurarsi quindi che il dispositivo esterno disponga di spazio su disco sufficiente per scaricare e archiviare patch.

Il processo di trasmissione delle patch e l'elenco degli aggiornamenti necessari viene mostrato nella figura e descritto di seguito:



Il processo di trasmissione delle patch e l'elenco degli aggiornamenti necessari tra Administration Server con accesso a Internet e Administration Server isolati

Per installare gli aggiornamenti e correggere le vulnerabilità nei dispositivi gestiti connessi ad Administration Server isolati:

1. Avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* se non è ancora in esecuzione.
2. Collegare un dispositivo esterno a qualsiasi Administration Server isolato.
3. Creare due cartelle nel dispositivo esterno: una per l'elenco degli aggiornamenti necessari e una per le patch. È possibile nominare queste cartelle in qualsiasi modo.

   Se queste cartelle sono state create in precedenza, è necessario cancellarle.
4. Copiare l'elenco degli aggiornamenti richiesti da ogni Administration Server isolato e incollarlo nella cartella per l'elenco degli aggiornamenti richiesti sul dispositivo esterno.

   Di conseguenza, si uniscono tutti gli elenchi acquisiti da tutti gli Administration Server isolati in un'unica cartella. Questa cartella contiene file binari con gli ID delle patch richieste per tutti gli Administration Server isolati.
5. Collegare il dispositivo esterno all'Administration Server con accesso a Internet.
6. Copiare l'elenco degli aggiornamenti richiesti dal dispositivo esterno e incollarlo nella cartella per l'elenco degli aggiornamenti richiesti sull'Administration Server con accesso a Internet.

   Tutte le patch richieste vengono scaricate automaticamente da Internet nella cartella delle patch nell'Administration Server. Questa operazione può richiedere diverse ore.

7. Assicurarsi che tutte le patch necessarie vengano scaricate. A tale scopo, è possibile eseguire una delle seguenti operazioni:

   - Controllare la cartella per le patch nell'Administration Server con accesso a Internet. Tutte le patch specificate nell'elenco degli aggiornamenti necessari devono essere scaricate nella cartella opportuna. L'operazione è più agevole se è necessario un numero limitato di patch.

   - Preparare uno script speciale, ad esempio uno script shell. Se si ottiene un numero elevato di patch, sarà difficile verificare autonomamente che tutte le patch siano state scaricate. In questi casi, è meglio automatizzare il controllo.

8. Copiare le patch dall'Administration Server con accesso a Internet e incollarle nella cartella corrispondente nel dispositivo esterno.

9. Trasferire le patch in ogni Administration Server isolato. Inserire le patch in una cartella specifica.

Di conseguenza, ogni Administration Server isolato crea un elenco effettivo di aggiornamenti necessari per i dispositivi gestiti collegati all'Administration Server corrente. Dopo che l'Administration Server con accesso a Internet ha ricevuto l'elenco degli aggiornamenti necessari, l'Administration Server scarica le patch da Internet. Quando queste patch vengono visualizzate negli Administration Server isolati, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* gestisce le patch. Gli aggiornamenti vengono quindi installati nei dispositivi gestiti e le vulnerabilità del software di terze parti vengono corrette.

Quando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* è in esecuzione, non riavviare il dispositivo Administration Server e non eseguire l'attività *Backup dei dati di Administration Server* (causerà anche un riavvio). Di conseguenza, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene interrotta e gli aggiornamenti non vengono installati. In questo caso, è necessario riavviare l'attività manualmente o attendere che l'attività venga avviata in base alla pianificazione configurata.

Disabilitazione dell'opzione per trasmettere patch e installare aggiornamenti in una rete isolata

È possibile disabilitare la trasmissione delle patch negli Administration Server isolati se, ad esempio, si decide di rimuovere uno o più Administration Server da una rete isolata. È quindi possibile ridurre il numero di patch e il tempo di download.

Per disabilitare l'opzione per la trasmissione delle patch negli Administration Server isolati:

1. Se si desidera eliminare l'isolamento di tutti gli Administration Server, nelle proprietà di Administration Server con accesso a Internet eliminare i percorsi delle cartelle per le patch e l'elenco degli aggiornamenti necessari. Se si desidera mantenere alcuni Administration Server in una rete isolata, ignorare questo passaggio.

   Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Immettere i seguenti comandi nel prompt dei comandi:

   - Per eliminare il percorso della cartella per le patch:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```

   - Per eliminare il percorso della cartella per un elenco degli aggiornamenti necessari:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Riavviare il servizio Administration Server se sono stati eliminati i percorsi delle cartelle in questo Administration Server.

3. Nelle proprietà di ogni Administration Server per cui si desidera eliminare l'isolamento, eliminare i percorsi delle cartelle per le patch e l'elenco degli aggiornamenti necessari.

   Immettere i seguenti comandi nel prompt dei comandi di Windows, utilizzando i diritti di amministratore:

   - Per eliminare il percorso della cartella per le patch:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - Per eliminare il percorso della cartella per un elenco degli aggiornamenti necessari:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Riavviare il servizio di ogni Administration Server in cui sono stati eliminati i percorsi delle cartelle.

Di conseguenza, se è stato riconfigurato Administration Server con l'accesso a Internet, non si riceveranno più patch tramite Kaspersky Security Center. Se sono stati riconfigurati solo alcuni Administration Server isolati, ad esempio rimuovendone alcuni dalla rete isolata, si otterranno patch solo per gli Administration Server isolati rimanenti.

Se in futuro si desidera iniziare a correggere le vulnerabilità negli Administration Server isolati disabilitati, è necessario configurare nuovamente questi Administration Server e l'Administration Server con accesso a Internet.

Ignorare le vulnerabilità del software

È possibile ignorare le vulnerabilità del software da correggere. I motivi per ignorare le vulnerabilità del software potrebbero essere, ad esempio, i seguenti:

- La vulnerabilità del software non viene considerata critica per l'organizzazione.
- Si ritiene che la correzione della vulnerabilità del software possa danneggiare i dati relativi al software per cui era necessaria la correzione della vulnerabilità.
- Si ha la certezza che la vulnerabilità del software non sia pericolosa per la rete dell'organizzazione in quanto si utilizzano altre misure per proteggere i dispositivi gestiti.

È possibile ignorare una vulnerabilità del software in tutti i dispositivi gestiti o solo nei dispositivi gestiti selezionati.

Per ignorare una vulnerabilità del software in tutti i dispositivi gestiti:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Vulnerabilità del software**.

   Nell'area di lavoro della cartella verrà visualizzato un elenco delle vulnerabilità rilevate dal Network Agent installato nei dispositivi.

2. Selezionare la vulnerabilità che si desidera ignorare.

3. Selezionare **Proprietà** dal menu di scelta rapida della vulnerabilità.

   Verrà visualizzata la finestra delle proprietà della vulnerabilità.

4. Nella sezione **Generale** selezionare l'opzione **Ignora vulnerabilità**.

5. Fare clic su **OK**.

   Viene chiusa la finestra delle proprietà delle vulnerabilità del software.

La vulnerabilità del software viene ignorata in tutti i dispositivi gestiti.

Per ignorare una vulnerabilità del software nel dispositivo gestito selezionato:

1. Aprire la finestra delle proprietà del dispositivo gestito selezionato e selezionare la sezione **Vulnerabilità del software**.
2. Selezionare una vulnerabilità del software.
3. Ignorare la vulnerabilità selezionata.

La vulnerabilità del software viene ignorata nel dispositivo selezionato.

La vulnerabilità del software ignorata non verrà corretta dopo il completamento dell'attività *Correggi vulnerabilità* o dell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. È possibile escludere le vulnerabilità del software ignorate dall'elenco delle vulnerabilità utilizzando il filtro.

Selezione di correzioni utente per le vulnerabilità del software di terze parti

Per utilizzare l'attività *Correggi vulnerabilità*, è necessario specificare manualmente gli aggiornamenti software per correggere le vulnerabilità del software di terze parti elencato nelle impostazioni dell'attività. L'attività *Correggi vulnerabilità* utilizza le correzioni consigliate per il software Microsoft e le correzioni dell'utente per altri software di terze parti. Le *correzioni dell'utente* sono aggiornamenti software per correggere le vulnerabilità che l'amministratore specifica manualmente per l'installazione.

Per selezionare le correzioni utente per le vulnerabilità del software di terze parti:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Vulnerabilità del software**.

   Nell'area di lavoro della cartella verrà visualizzato un elenco delle vulnerabilità rilevate dal Network Agent installato nei dispositivi.
2. Selezionare la vulnerabilità per cui si desidera specificare una correzione utente.
3. Selezionare **Proprietà** dal menu di scelta rapida della vulnerabilità.

   Verrà visualizzata la finestra delle proprietà della vulnerabilità.
4. Nella sezione **Correzioni utente e altre correzioni** fare clic sul pulsante **Aggiungi**.

   Verrà visualizzato l'elenco dei pacchetti di installazione disponibili. L'elenco dei pacchetti di installazione visualizzati corrisponde all'elenco **Installazione remota** → **Pacchetti di installazione**. Se non è stato creato un pacchetto di installazione contenente una correzione utente per la vulnerabilità selezionata, è possibile creare il pacchetto subito avviando la Creazione guidata nuovo pacchetto.
5. Selezionare un pacchetto di installazione (o più pacchetti) contenente una correzione utente (o correzioni utente) per la vulnerabilità del software di terze parti.
6. Fare clic su **OK**.

Vengono specificati i pacchetti di installazione contenenti le correzioni utente per la vulnerabilità del software. Quando l'attività *Correggi vulnerabilità* viene avviata, il pacchetto di installazione verrà installato e la vulnerabilità del software verrà corretta.

Regole per l'installazione dell'aggiornamento

Durante la correzione delle vulnerabilità delle applicazioni, è necessario specificare le regole per l'installazione degli aggiornamenti. Queste regole determinano gli aggiornamenti da installare e le vulnerabilità da correggere.

Le esatte impostazioni dipendono dall'esigenza di creare una regola per gli aggiornamenti delle applicazioni Microsoft, delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) o di tutte le applicazioni. Durante la creazione di una regola per le applicazioni Microsoft o per le applicazioni di terze parti, è possibile selezionare le specifiche applicazioni e versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Durante la creazione di una regola per tutte le applicazioni, è possibile selezionare gli specifici aggiornamenti da installare e le vulnerabilità che si desidera risolvere tramite l'installazione degli aggiornamenti.

Per creare una nuova regola per gli aggiornamenti di tutte le applicazioni:

1. Nella pagina **Impostazioni** della Creazione guidata nuova attività fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Seguire le istruzioni della procedura guidata.

2. Nella pagina **Tipo di regola** selezionare **Regola per tutti gli aggiornamenti**.

3. Nella pagina **Criteri generali** utilizzare gli elenchi a discesa per specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Aggiornamenti** selezionare gli aggiornamenti da installare:

   - **Installa tutti gli aggiornamenti appropriati**

     Installa tutti gli aggiornamenti software che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

   - **Installa solo gli aggiornamenti nell'elenco**

     Installa solo gli aggiornamenti software che selezionati manualmente dall'elenco. Questo elenco contiene tutti gli aggiornamenti software disponibili.

     Ad esempio, è possibile selezionare aggiornamenti specifici nei seguenti casi: per verificarne l'installazione in un ambiente di test, per aggiornare solo le applicazioni critiche o per aggiornare solo specifiche applicazioni.

     - **Installa automaticamente tutti gli aggiornamenti precedenti dell'applicazione necessari per l'installazione degli aggiornamenti selezionati**

       Mantenere abilitata questa opzione se si desidera consentire l'installazione delle versioni intermedie delle applicazioni quando questa operazione è necessaria per l'installazione degli aggiornamenti selezionati.

       Se questa opzione è disabilitata, vengono installate solo le versioni delle applicazioni selezionate. Disabilitare questa opzione se si desidera aggiornare le applicazioni in modo diretto, senza tentare di installare le versioni successive in modo incrementale. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

       Si supponga di avere la versione 3 di un'applicazione installata in un dispositivo e di voler eseguire l'aggiornamento alla versione 5, ma la versione 5 di questa applicazione può essere installata solo sulla versione 4. Se questa opzione è abilitata, il software installa prima la versione 4 e quindi la versione 5. Se questa opzione è disabilitata, il software non riesce a eseguire l'aggiornamento l'applicazione.

       Per impostazione predefinita, questa opzione è abilitata.

5. Nella pagina **Vulnerabilità** selezionare le vulnerabilità da correggere tramite l'installazione degli aggiornamenti selezionati:

   - **Correggi tutte le vulnerabilità che corrispondono ad altri criteri**

     Verranno corrette tutte le vulnerabilità che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

   - **Correggi solo le vulnerabilità nell'elenco**

     Verranno corrette solo le vulnerabilità selezionate manualmente dall'elenco. Questo elenco contiene tutte le vulnerabilità rilevate.

     Ad esempio, è possibile selezionare vulnerabilità specifiche nei seguenti casi: per verificarne la correzione in un ambiente di test, per correggere solo le vulnerabilità di applicazioni critiche o per correggere le vulnerabilità solo in specifiche applicazioni.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà creata e visualizzata nel campo **Specificare le regole per l'installazione degli aggiornamenti** della Creazione guidata nuova attività.

Per creare una nuova regola per gli aggiornamenti delle applicazioni Microsoft:

1. Nella pagina **Impostazioni** della Creazione guidata nuova attività fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Seguire le istruzioni della procedura guidata.

2. Nella pagina **Tipo di regola** selezionare **Regola per Windows Update**.

3. Nella pagina **Criteri generali** specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

   - **Correggi le vulnerabilità con un livello di criticità MSRC uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Microsoft Security Response Center (MSRC) è uguale o superiore al valore selezionato nell'elenco (**Basso**, **Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Categorie di aggiornamenti** selezionare le categorie di aggiornamenti da installare. Queste categorie sono identiche a quelle del catalogo di Microsoft Update. Per impostazione predefinita, tutte le categorie sono selezionate.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà creata e visualizzata nel campo **Specificare le regole per l'installazione degli aggiornamenti** della Creazione guidata nuova attività.

Per creare una nuova regola per gli aggiornamenti delle applicazioni di terze parti:

1. Nella pagina **Impostazioni** della Creazione guidata nuova attività fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Seguire le istruzioni della procedura guidata.

2. Nella pagina **Tipo di regola** selezionare **Regola per gli aggiornamenti di terze parti**.

3. Nella pagina **Criteri generali** specificare le seguenti impostazioni:

   - Set di aggiornamenti da installare

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - Correggi le vulnerabilità con un livello di criticità uguale o superiore a

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà creata e visualizzata nel campo **Specificare le regole per l'installazione degli aggiornamenti** della Creazione guidata nuova attività.

Gruppi di applicazioni

In questa sezione viene descritto come gestire i gruppi di applicazioni installate nei dispositivi.

Creazione delle categorie di applicazioni

Kaspersky Security Center consente di creare categorie di applicazioni installate nei dispositivi.

È possibile creare categorie di applicazioni in uno dei seguenti modi:

- L'amministratore specifica una cartella che contiene i file eseguibili da includere nella categoria selezionata.
- L'amministratore specifica un dispositivo che contiene i file eseguibili da includere nella categoria selezionata.
- L'amministratore imposta i criteri da utilizzare per includere le applicazioni nella categoria selezionata.

Al momento della creazione di una categoria di applicazioni, l'amministratore può impostare le regole per la categoria. Le regole definiscono il comportamento delle applicazioni incluse nella categoria specificata. Ad esempio, è possibile bloccare o consentire l'avvio delle applicazioni incluse nella categoria.

Gestione delle applicazioni in esecuzione nei dispositivi

Kaspersky Security Center consente di gestire l'avvio delle applicazioni nei dispositivi in modalità Lista consentiti. Per una descrizione dettagliata, vedere la Guida in linea di Kaspersky Endpoint Security for Windows. In modalità Lista consentiti, nei dispositivi selezionati sarà consentito solo l'avvio delle applicazioni incluse nelle categorie specificate. L'amministratore può visualizzare i risultati dell'analisi statica delle regole di avvio delle applicazioni nei dispositivi per ogni utente.

Inventario del software installato nei dispositivi

Kaspersky Security Center consente di creare un inventario del software installato nei dispositivi che eseguono Windows e Linux. Network Agent recupera informazioni su tutte le applicazioni installate nei dispositivi. Le informazioni ottenute durante l'inventario vengono visualizzate nell'area di lavoro della cartella **Registro delle applicazioni**. L'amministratore può visualizzare informazioni dettagliate su qualsiasi applicazione, inclusi la versione e il produttore.

Il numero di file eseguibili ricevuti da un singolo dispositivo non può essere superiore a 150.000. Una volta raggiunto questo limite, Kaspersky Security Center non può ricevere nuovi file.

Gestione gruppo di applicazioni concesse in licenza

Kaspersky Security Center consente di creare gruppi di applicazioni concesse in licenza. Un gruppo di applicazioni concesse in licenza include le applicazioni che soddisfano i criteri impostati dall'amministratore. L'amministratore può specificare i seguenti criteri per i gruppi di applicazioni concesse in licenza:

- Nome applicazione
- Versione applicazione
- Produttore
- Tag applicazione

Le applicazioni che soddisfano uno o più criteri vengono automaticamente incluse in un gruppo. Per creare un gruppo di applicazioni concesse in licenza, è necessario impostare almeno un criterio per l'inclusione delle applicazioni nel gruppo.

Ogni gruppo di applicazioni concesse in licenza dispone di una propria chiave di licenza. La chiave di licenza di un gruppo di applicazioni concesse in licenza definisce il numero massimo di installazioni consentite per le applicazioni incluse nel gruppo. Se il numero di installazioni ha superato i limiti impostati dalla chiave di licenza, viene registrato un evento informativo in Administration Server. L'amministratore può specificare una data di scadenza per la chiave di licenza. Alla scadenza, viene registrato un evento informativo in Administration Server.

Visualizzazione delle informazioni sui file eseguibili

Kaspersky Security Center recupera tutte le informazioni sui file eseguibili avviati nei dispositivi a partire dall'installazione del sistema operativo. Le informazioni sui file eseguibili vengono visualizzate nella finestra principale dell'applicazione, nell'area di lavoro della cartella **File eseguibili**.

Utilizzo di Controllo Applicazioni per gestire i file eseguibili

È possibile utilizzare il componente Controllo Applicazioni per consentire o bloccare l'avvio dei file eseguibili nei dispositivi dell'utente. Il componente Controllo Applicazioni supporta i sistemi operativi basati su Windows e Linux.

Per i sistemi operativi basati su Linux, il componente Application Control è disponibile a partire da Kaspersky Endpoint Security 11.2 per Linux. Inoltre, il componente è disponibile per Kaspersky Embedded Systems Security per Windows 3.0 o versioni successive.

Prerequisiti

- Kaspersky Security Center viene distribuito nell'organizzazione.
- Il criterio di Kaspersky Endpoint Security for Windows o Kaspersky Endpoint Security for Linux è stato creato ed è attivo.
- Il criterio di Kaspersky Embedded Systems Security for Windows o Kaspersky Embedded Systems Security for Linux è stato creato ed è attivo.

Passaggi

Lo scenario di utilizzo di Controllo Applicazioni prevede diversi passaggi:

1. **Creazione e visualizzazione dell'elenco dei file eseguibili nei dispositivi client**

   Questo passaggio consente di scoprire quali file eseguibili sono presenti nei dispositivi gestiti. Visualizzare l'elenco dei file eseguibili e confrontarlo con l'elenco dei file eseguibili consentiti e non consentiti. Le restrizioni relative all'utilizzo dei file eseguibili possono essere correlate ai criteri di sicurezza delle informazioni dell'organizzazione.

   Istruzioni dettagliate:

   - Administration Console: Inventario dei file eseguibili
   - Kaspersky Security Center Web Console: Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client

2. **Creazione di categorie per i file eseguibili utilizzati nell'organizzazione**

   Analizzare gli elenchi dei file eseguibili archiviati nei dispositivi gestiti. In base all'analisi, creare categorie per i file eseguibili. È consigliabile creare una categoria "Applicazioni di lavoro" che includa il set standard di file eseguibili utilizzati nell'organizzazione. Se differenti gruppi di sicurezza utilizzano i propri set di file eseguibili nel proprio lavoro, è possibile creare una categoria distinta per ciascun gruppo di sicurezza.

   Istruzioni dettagliate:

   - Administration Console: Creazione di una categoria di applicazioni con contenuto aggiunto manualmente, Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati, Creazione di una categoria di applicazioni che include i file eseguibili in una cartella selezionata.
   - Kaspersky Security Center Web Console: Creazione di una categoria di applicazioni con contenuto aggiunto manualmente, Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati, Creazione di una categoria di applicazioni che include i file eseguibili in una cartella specifica.

3. **Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security**

   Configurare il componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security utilizzando le categorie create nel passaggio precedente.

   Istruzioni dettagliate:

   - Administration Console: Configurazione della gestione dell'avvio delle applicazioni nei dispositivi client
   - Kaspersky Security Center Web Console: Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

4. **Configurazione di Controllo Applicazioni nel criterio dell'applicazione Kaspersky Embedded Systems Security**

   Configurare il componente Controllo applicazioni nel criterio Kaspersky Embedded Systems Security for Windows utilizzando le categorie create. Per ulteriori informazioni sul componente Controllo applicazioni, fare riferimento alla Guida di Kaspersky Embedded Systems Security for Windows o alla Guida di Kaspersky Embedded Systems Security for Linux.

   Se si utilizza un numero elevato di regole, potrebbe verificarsi un errore durante il caricamento del criterio. È possibile aumentare la dimensione massima della richiesta in byte utilizzando i seguenti comandi:

   - Per la richiesta JSON:

     ```
     klscflag -fset -pv ".core/.independent" -s KLLIM -n
     LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
     ```

- Per la richiesta HTTP:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
  ```

  Dove `<max_request_size>` è la dimensione massima della richiesta in byte (ad esempio, `200000000`).

5. **Attivazione del componente Controllo Applicazioni in modalità di test**

   Per garantire che le regole di Controllo Applicazioni non blocchino i file eseguibili richiesti per il lavoro dell'utente, è consigliabile abilitare il test delle regole di Controllo Applicazioni e analizzarne il funzionamento dopo aver creato le nuove regole. Quando il test è abilitato, Kaspersky Endpoint Security for Windows o Kaspersky Embedded Systems Security non bloccherà i file eseguibili il cui avvio non è consentito dalle regole di Controllo Applicazioni, ma invierà invece notifiche sul relativo avvio ad Administration Server.

   Durante il test delle regole di Controllo Applicazioni, è consigliabile eseguire le seguenti azioni:

   - Determinare il periodo di test. Il periodo di test può variare da alcuni giorni a due mesi.
   - Esaminare gli eventi risultanti dal test del funzionamento di Controllo Applicazioni.

   Istruzioni dettagliate per Kaspersky Security Center Web Console: Configurazione del componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows. Seguire queste istruzioni e abilitare l'opzione **Modalità test** nel processo di configurazione.

6. **Modifica delle impostazioni delle categorie del componente Controllo Applicazioni**

   Se necessario, apportare modifiche alle impostazioni di Controllo Applicazioni. In base ai risultati del test, è possibile aggiungere i file eseguibili correlati agli eventi del componente Controllo Applicazioni a una categoria con contenuto aggiunto manualmente.

   Istruzioni dettagliate:

   - Administration Console: Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni
   - Kaspersky Security Center Web Console: Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni

7. **Applicazione delle regole di Controllo Applicazioni in modalità operativa**

   Dopo aver testato le regole di Controllo Applicazioni e completato la configurazione delle categorie, è possibile applicare le regole di Controllo Applicazioni in modalità operativa.

   Istruzioni dettagliate per Kaspersky Security Center Web Console: Configurazione del componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows. Seguire queste istruzioni e disabilitare l'opzione **Modalità test** nel processo di configurazione.

8. **Verifica della configurazione di Controllo Applicazioni**

   Assicurarsi di avere eseguito le seguenti operazioni:

   - Categorie create per i file eseguibili.
   - Configurazione di Controllo Applicazioni tramite le categorie.
   - Applicazione delle regole di Controllo Applicazioni in modalità operativa.

Risultati

Al termine dello scenario, viene controllato l'avvio dei file eseguibili nei dispositivi gestiti. Gli utenti possono eseguire solo i file eseguibili consentiti nell'organizzazione e non possono eseguire quelli non consentiti.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Guida di Kaspersky Embedded Systems Security for Windows
- Guida di Kaspersky Embedded Systems Security for Linux

Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client

È possibile ottenere l'elenco dei file eseguibili archiviati sui dispositivi client in uno dei seguenti modi:

- Abilitazione delle notifiche sull'avvio delle applicazioni nel criterio di Kaspersky Endpoint Security.
- Creazione di un'attività di inventario.

Abilitazione delle notifiche sull'avvio delle applicazioni nel criterio di Kaspersky Endpoint Security

Per abilitare le notifiche sull'avvio delle applicazioni:

1. Aprire le impostazioni dei criteri di Kaspersky Endpoint Security, quindi passare a **Impostazioni generali** → **Rapporti e archivi**.
2. Nel gruppo di impostazioni **Trasferimento dati ad Administration Server**, selezionare la casella di controllo **Informazioni sulle applicazioni avviate** e salvare le modifiche.

Quando un utente tenta di avviare file eseguibili, le informazioni su tali file vengono aggiunte all'elenco dei file eseguibili su un dispositivo client. Kaspersky Endpoint Security invia queste informazioni a Network Agent, che a sua volta le invia ad Administration Server.

Creazione di un'attività di inventario

La funzione di inventario dei file eseguibili è disponibile per le seguenti applicazioni:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux versione 11.2 e successive
- Kaspersky Security for Virtualization 4.0 Light Agent e versioni successive

È possibile ridurre il carico sul database mentre si ottengono informazioni sulle applicazioni installate. Per risparmiare spazio, eseguire un'attività di inventario sui dispositivi di riferimento in cui è installato un set standard di software. Il numero preferibile di dispositivi è 1-3.

Si sconsiglia vivamente di eseguire l'attività di inventario quando si utilizzano i seguenti database: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (tutte le edizioni).

Per creare un'attività di inventario per i file eseguibili nei dispositivi client:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Nell'area di lavoro della cartella **Attività** fare clic sul pulsante **Nuova attività**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nella finestra **Selezionare il tipo di attività** della procedura guidata selezionare **Kaspersky Endpoint Security** come tipo di attività, selezionare **Inventario** come sottotipo di attività, quindi fare clic su **Avanti**.
4. Seguire le rimanenti istruzioni della procedura guidata.

   Al termine della Creazione guidata nuova attività, l'attività **Inventario** sarà creata e configurata. Se si desidera, è possibile modificare le impostazioni per l'attività creata. La nuova attività creata verrà visualizzata nell'elenco delle attività. Se si desidera, è possibile modificare le impostazioni per l'attività creata.

Per una descrizione dettagliata dell'attività di inventario, fare riferimento alle seguenti Guide:

- Guida di Kaspersky Endpoint Security for Windows
- Guida di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Dopo l'esecuzione dell'attività **Inventario**, viene formato l'elenco dei file eseguibili archiviati nei dispositivi gestiti ed è possibile visualizzarlo.

Durante l'esecuzione dell'attività di inventario, è possibile rilevare file eseguibili nei seguenti formati (a seconda dell'opzione selezionata nelle proprietà dell'attività di inventario): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Visualizzazione dell'elenco dei file eseguibili archiviati nei dispositivi gestiti

Per visualizzare l'elenco dei file eseguibili archiviati nei dispositivi client:

Nella struttura della console, passare ad **Avanzate** → **Gestione applicazioni** → **File eseguibili**.

Se necessario, è possibile inviare un file eseguibile da un dispositivo gestito al dispositivo su cui è installata l'Administration Console.

Per inviare un file eseguibile:

1. Nella struttura della console, passare ad **Avanzate** → **Gestione applicazioni** → **File eseguibili**.
2. Fare clic sul collegamento del file eseguibile che si desidera inviare al dispositivo su cui è installata l'Administration Console.
3. Nella finestra visualizzata, accedere alla sezione **Dispositivi**, quindi selezionare la casella di controllo del dispositivo gestito da cui si desidera inviare il file eseguibile.

   Prima di inviare il file eseguibile, assicurarsi che il dispositivo gestito disponga di una connessione diretta ad Administration Server selezionando la casella di controllo **Non eseguire la disconnessione da Administration Server**.

4. Fare clic sul pulsante **Invia**, selezionare la cartella di destinazione, quindi fare clic su **OK**.

Il file eseguibile selezionato viene scaricato per essere inviato al dispositivo su cui è installata l'Administration Console.

Creazione delle categorie di applicazioni per i criteri di Kaspersky Endpoint Security for Windows

È possibile creare categorie di applicazioni per i criteri di Kaspersky Endpoint Security for Windows dalla cartella **Categorie di applicazioni** e dalla finestra **Proprietà** di un criterio di Kaspersky Endpoint Security for Windows.

*Per creare una categoria di applicazioni per un criterio di Kaspersky Endpoint Security dalla cartella **Categorie di applicazioni**:*

1. Nella struttura della console selezionare **Avanzate** → **Gestione applicazioni** → **Categorie di applicazioni**.
2. Nell'area di lavoro della cartella **Categorie di applicazioni** fare clic sul pulsante **Nuova categoria**.

   Verrà avviata la Creazione guidata nuova categoria.

3. Nella pagina **Tipo di categoria** selezionare il tipo di categoria utente:

   - **Categoria con contenuto aggiunto manualmente**. Specificare i criteri da utilizzare per assegnare i file eseguibili alla categoria creata.
   - **Categoria con contenuto aggiunto automaticamente**. Specificare la cartella in cui sono presenti i file eseguibili da assegnare automaticamente alla categoria creata.

     Al momento della creazione di una categoria con contenuto aggiunto automaticamente, l'applicazione esegue l'inventario dei seguenti tipi di file: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX e SCR.

   - **Categoria che include i file eseguibili dei dispositivi selezionati**. Specificare un dispositivo di cui assegnare automaticamente i file eseguibili alla categoria.

4. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, viene creata una categoria di applicazioni personalizzata. È possibile visualizzare le nuove categorie create utilizzando l'elenco di categorie nell'area di lavoro della cartella **Categorie di applicazioni**.

Se si desidera esportare una categoria di applicazioni in un file KLC, fare clic con il pulsante destro del mouse sul nome della categoria, selezionare **Esporta** nel menu, quindi nella finestra che si apre specificare il nome del file e fare clic su **Save**.

È inoltre possibile creare una categoria di applicazioni dalla cartella **Criteri**.

*Per creare una categoria di applicazioni dalla finestra **Proprietà** di un criterio di Kaspersky Endpoint Security for Windows:*

1. Nella struttura della console selezionare la cartella **Criteri**.
2. Nell'area di lavoro della cartella **Criteri** selezionare un criterio di Kaspersky Endpoint Security per cui si desidera creare una categoria.
3. Fare clic con il pulsante destro del mouse e selezionare **Proprietà**.
4. Nella finestra **Proprietà** visualizzata, nel riquadro sinistro **Sezioni**, selezionare **Controlli di sicurezza** → **Controllo Applicazioni**.
5. Nella sezione **Controllo Applicazioni**, negli elenchi a discesa **Modalità di controllo** e **Azione**, effettuare le selezioni per la lista consentiti o la lista vietati, quindi fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Regola di Controllo Applicazioni** con un elenco di categorie.
6. Fare clic sul pulsante **Crea nuova**.
7. Immettere il nome della nuova categoria e fare clic su **OK**.

   Verrà avviata la Creazione guidata nuova categoria.
8. Nella pagina **Tipo di categoria** selezionare il tipo di categoria utente:

   - **Categoria con contenuto aggiunto manualmente**. Specificare i criteri da utilizzare per assegnare i file eseguibili alla categoria creata.
   - **Categoria con contenuto aggiunto automaticamente**. Specificare la cartella in cui sono presenti i file eseguibili da assegnare automaticamente alla categoria creata.

     Al momento della creazione di una categoria con contenuto aggiunto automaticamente, l'applicazione esegue l'inventario dei seguenti tipi di file: EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX e SCR.
   - **Categoria che include i file eseguibili dei dispositivi selezionati**. Specificare un dispositivo di cui assegnare automaticamente i file eseguibili alla categoria.
9. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, viene creata una categoria di applicazioni personalizzata. È possibile visualizzare le nuove categorie create nell'elenco delle categorie.

Le categorie di applicazioni vengono utilizzate dal componente Controllo Applicazioni incluso in Kaspersky Endpoint Security for Windows. Controllo Applicazioni consente all'amministratore di applicare restrizioni all'avvio delle applicazioni nei dispositivi client, ad esempio limitando gli avvii delle applicazioni in una categoria specificata.

Creazione di una categoria di applicazioni con contenuto aggiunto manualmente

È possibile specificare un set di criteri come modello per i file eseguibili di cui consentire o bloccare l'avvio nell'organizzazione. In base ai file eseguibili corrispondenti ai criteri, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per creare una categoria di applicazioni con contenuto aggiunto manualmente:

1. Nella struttura della console, nella cartella **Avanzate** → **Gestione applicazioni** selezionare la sottocartella **Categorie di applicazioni**.

2. Fare clic sul pulsante **Nuova categoria**.

   Verrà avviata la **Creazione guidata nuova categoria**. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nella pagina della procedura guidata **Tipo di categoria**, selezionare **Categoria con contenuto aggiunto manualmente** come tipo di categoria utente.

4. Nella pagina della procedura guidata **Immettere il nome della categoria di applicazioni**, immettere il nuovo nome della categoria dell'applicazione.

5. Nella pagina **Configurazione delle condizioni per l'inclusione delle applicazioni nelle categorie** fare clic sul pulsante **Aggiungi**.

6. Nell'elenco a discesa specificare le impostazioni desiderate:

- **Dall'elenco di file eseguibili**

  Se questa opzione è selezionata, è possibile utilizzare l'elenco dei file eseguibili nel dispositivo client per selezionare e aggiungere applicazioni alla categoria.

- **Dalle proprietà dei file**

  Se questa opzione è selezionata, è possibile specificare dati dettagliati per i file eseguibili da aggiungere alla categoria utente di applicazioni.

- **Metadati dai file nella cartella**

  Specificare una cartella nel dispositivo client contenente i file eseguibili. I metadati dei file eseguibili inclusi nella cartella specificata verranno inviati ad Administration Server. I file eseguibili che contengono gli stessi metadati verranno aggiunti alla categoria utente di applicazioni.

- **Checksum dei file nella cartella**

  Se questa opzione è selezionata, è possibile selezionare o creare una cartella nel dispositivo client. L'hash MD5 dei file in una cartella specificata verrà inviato ad Administration Server. Le applicazioni con lo stesso hash dei file nella cartella specificata verranno aggiunte alla categoria di applicazioni dell'utente.

- **Certificati per i file della cartella**

  Se questa opzione è selezionata, è possibile specificare la cartella nel dispositivo client che contiene file eseguibili firmati con certificati. I certificati dei file eseguibili vengono letti e aggiunti alle condizioni della categoria. I file eseguibili firmati in base ai certificati specificati verranno aggiunti alla categoria utente.

- **Metadati dei file del programma di installazione MSI**

  Se questa opzione è selezionata, è possibile specificare il file di un programma di installazione MSI come condizione per l'aggiunta di applicazioni alla categoria utente. I metadati del programma di installazione dell'applicazione verranno inviati ad Administration Server. Le applicazioni per cui i metadati del programma di installazione corrispondono a quelli del programma di installazione MSI specificato verranno aggiunte alla categoria utente di applicazioni.

- **Checksum dei file dal programma di installazione MSI dell'applicazione**

  Se questa opzione è selezionata, è possibile specificare il file di un programma di installazione MSI come condizione per l'aggiunta di applicazioni alla categoria utente. L'hash dei file del programma di installazione dell'applicazione verrà inviato ad Administration Server. Le applicazioni per cui l'hash dei file del programma di installazione MSI è identico all'hash specificato vengono aggiunte alla categoria di applicazioni dell'utente.

- **Da categoria KL**

Se questa opzione è selezionata, è possibile specificare una categoria di applicazioni Kaspersky come condizione per l'aggiunta di applicazioni alla categoria utente. Le applicazioni della categoria Kaspersky specificata verranno aggiunte alla categoria utente di applicazioni.

- **Specificare il percorso dell'applicazione (maschere supportate)**

  Se questa opzione è selezionata, è possibile specificare il percorso di un file o una cartella nel dispositivo client che contiene i file eseguibili da aggiungere alla categoria utente di applicazioni. È possibile utilizzare espressioni regolari come *C:\path_to_exe**, ad esempio: *C:\Program Files\Internet Explorer**.

- **Seleziona certificato dall'archivio**

  Se questa opzione è selezionata, è possibile specificare i certificati dell'archivio. La condizione di categoria corrisponde solo ai file eseguibili firmati dal certificato specificato.

  I certificati vengono aggiunti all'archivio se è stata creata e avviata un'attività di inventario o se è stata selezionata la casella di controllo **Informazioni sulle applicazioni avviate** nel criterio di Kaspersky Endpoint Security. È possibile eseguire entrambe le azioni.

- **Tipo di unità**

  Se questa opzione è selezionata, è possibile specificare il tipo di supporto (qualsiasi unità o unità rimovibile) in cui viene eseguita l'applicazione. Le applicazioni che sono state eseguite nel tipo di unità selezionato verranno aggiunte alla categoria utente di applicazioni.

7. Nella pagina della procedura guidata **Creazione della categoria di applicazioni**, fare clic sul pulsante **Fine**.

Kaspersky Security Center gestisce solo i metadati dei file con firma digitale. Non è possibile creare una categoria in base ai metadati dei file che non contengono una firma digitale.

Al termine della procedura guidata, viene creata una categoria di applicazioni dell'utente con contenuto aggiunto manualmente. È possibile visualizzare la nuova categoria creata utilizzando l'elenco di categorie nell'area di lavoro della cartella **Categorie di applicazioni**.

Se si desidera esportare una categoria di applicazioni in un file KLC, fare clic con il pulsante destro del mouse sul nome della categoria, selezionare **Esporta** nel menu, quindi nella finestra che si apre specificare il nome del file e fare clic su **Save**.

Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati

È possibile utilizzare i file eseguibili nei dispositivi selezionati come modello per i file eseguibili da consentire o bloccare. In base ai file eseguibili nei dispositivi selezionati, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per recuperare l'elenco dei file eseguibili dai dispositivi:

1. Assicurarsi che il criterio di Kaspersky Endpoint Security for Windows o Kaspersky Endpoint Security for Linux sia stato creato e sia attivo. Abilitare il componente Controllo Applicazioni nel criterio.

2. Recuperare un elenco dei file eseguibili archiviati nei dispositivi client.

Per creare una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati:

1. Nella struttura della console, nella cartella **Avanzate** → **Gestione applicazioni** selezionare la sottocartella **Categorie di applicazioni**.

2. Fare clic sul pulsante **Nuova categoria**.

   Verrà avviata la **Creazione guidata nuova categoria**. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nella pagina della procedura guidata **Tipo di categoria**, selezionare **Categoria che include i file eseguibili dai dispositivi selezionati** come tipo di categoria utente.

4. Nella pagina della procedura guidata **Immettere il nome della categoria di applicazioni**, immettere il nuovo nome della categoria dell'applicazione.

5. Nella pagina della procedura guidata **Impostazioni** fare clic sul pulsante **Aggiungi**.

6. Selezionare uno o più dispositivi che contengono i file eseguibili da utilizzare per creare la categoria di applicazioni.

7. Specificare le seguenti impostazioni:

- **Algoritmo di calcolo del valore hash**

  A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center per i file di questa categoria. Le informazioni sui valori hash calcolati dalle funzioni hash vengono memorizzate nel database di Administration Server.

  SHA256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive supportano il calcolo di SHA256. Il calcolo della funzione hash MD5 è supportato da tutte le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

  Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center per i file della categoria:

  - Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive, selezionare la casella di controllo **SHA256**. Non è consigliabile aggiungere categorie create in base al criterio dell'hash SHA256 di un file eseguibile per le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Questo può generare errori durante l'esecuzione dell'applicazione di protezione. In questo caso, è possibile utilizzare la funzione hash di criptaggio MD5 per i file della categoria.

  - Se nella rete sono installate versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, selezionare **Hash MD5**. Non è possibile aggiungere una categoria che è stata creata in base al criterio del checksum MD5 di un file eseguibile per Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive. In questo caso, è possibile utilizzare la funzione hash di criptaggio SHA256 per i file della categoria.

  Se diversi dispositivi della rete utilizzano versioni precedenti e successive di Kaspersky Endpoint Security 10, selezionare sia la casella di controllo **SHA256** che la casella di controllo **Hash MD5**.

  La casella di controllo **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)** è selezionata per impostazione predefinita.

  La casella di controllo **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** è deselezionata per impostazione predefinita.

- **Sincronizza i dati con l'archivio dell'Administration Server**

  Selezionare questa opzione se si desidera che Administration Server controlli periodicamente le modifiche nelle cartelle specificate.

  Per impostazione predefinita, questa opzione è disabilitata.

  Se si abilita questa opzione, specificare il periodo (in ore) per la verifica delle modifiche nelle cartelle specificate. Per impostazione predefinita, l'intervallo per la scansione è di 24 ore.

8. Nella pagina della procedura guidata **Filtro**, specificare le seguenti impostazioni:

   - Tipo di file

     In questa sezione è possibile specificare il tipo di file utilizzato per creare la categoria di applicazioni.

     Tutti i file. Durante la creazione della categoria vengono presi in considerazione tutti i file. Per impostazione predefinita, questa opzione è selezionata.

     Solo i file esterni alle categorie di applicazioni. Durante la creazione della categoria vengono presi in considerazione solo i file esterni alle categorie di applicazioni.

   - Cartelle

     In questa sezione è possibile specificare quali cartelle nei dispositivi selezionati contengono i file utilizzati per creare la categoria di applicazioni.

     Tutte le cartelle. Per la creazione della categoria vengono prese in considerazione tutte le cartelle. Per impostazione predefinita, questa opzione è selezionata.

     Cartella specificata. Per la creazione della categoria viene presa in considerazione solo la cartella specificata. Se si seleziona questa opzione, è necessario specificare il percorso della cartella.

9. Nella pagina della procedura guidata **Creazione della categoria di applicazioni**, fare clic sul pulsante **Fine**.

   Al termine della procedura guidata, viene creata una categoria di applicazioni utente. È possibile visualizzare la nuova categoria creata utilizzando l'elenco di categorie nell'area di lavoro della cartella **Categorie di applicazioni**.

Se si desidera esportare una categoria di applicazioni in un file KLC, fare clic con il pulsante destro del mouse sul nome della categoria, selezionare **Esporta** nel menu, quindi nella finestra che si apre specificare il nome del file e fare clic su **Save**.

Creazione di una categoria di applicazioni che include i file eseguibili da una cartella specifica

È possibile utilizzare i file eseguibili in una cartella selezionata come standard per i file eseguibili da consentire o bloccare nell'organizzazione. In base ai file eseguibili nella cartella selezionata, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per creare una categoria di applicazioni che includa i file eseguibili da una cartella specifica:

1. Nella struttura della console, nella cartella **Avanzate** → **Gestione applicazioni** selezionare la sottocartella **Categorie di applicazioni**.

2. Fare clic sul pulsante **Nuova categoria**.

   Verrà avviata la **Creazione guidata nuova categoria**. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nella pagina della procedura guidata **Tipo di categoria**, selezionare **Categoria che include i file eseguibili da una cartella specifica** come tipo di categoria utente.

4. Nella pagina della procedura guidata **Immettere il nome della categoria di applicazioni**, immettere il nuovo nome della categoria dell'applicazione.

5. Nella pagina della procedura guidata **Cartella archivio**, fare clic sul pulsante **Sfoglia**.

6. Specificare la cartella i cui file eseguibili verranno utilizzati per creare la categoria di applicazioni.

7. Definire le seguenti impostazioni:

- **Includi librerie di collegamento dinamico (DLL) in questa categoria**

  La categoria di applicazioni include le librerie di collegamento dinamico (file in formato DLL) e il componente Controllo Applicazioni registra le azioni di tali librerie in esecuzione nel sistema. L'inclusione dei file DLL nella categoria può ridurre le prestazioni di Kaspersky Security Center.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Includi i dati degli script in questa categoria**

  La categoria di applicazioni include i dati sugli script e gli script non vengono bloccati da Protezione minacce Web. L'inclusione dei dati sugli script nella categoria può ridurre le prestazioni di Kaspersky Security Center.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Algoritmo di calcolo del valore hash**: **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive) / Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center per i file di questa categoria. Le informazioni sui valori hash calcolati dalle funzioni hash vengono memorizzate nel database di Administration Server.

SHA256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive supportano il calcolo di SHA256. Il calcolo della funzione hash MD5 è supportato da tutte le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center per i file della categoria:

- Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive, selezionare la casella di controllo **SHA256**. Non è consigliabile aggiungere categorie create in base al criterio dell'hash SHA256 di un file eseguibile per le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Questo può generare errori durante l'esecuzione dell'applicazione di protezione. In questo caso, è possibile utilizzare la funzione hash di criptaggio MD5 per i file della categoria.

- Se nella rete sono installate versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, selezionare **Hash MD5**. Non è possibile aggiungere una categoria che è stata creata in base al criterio del checksum MD5 di un file eseguibile per Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive. In questo caso, è possibile utilizzare la funzione hash di criptaggio SHA256 per i file della categoria.

Se diversi dispositivi della rete utilizzano versioni precedenti e successive di Kaspersky Endpoint Security 10, selezionare sia la casella di controllo **SHA256** che la casella di controllo **Hash MD5**.

La casella di controllo **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)** è selezionata per impostazione predefinita.

La casella di controllo **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** è deselezionata per impostazione predefinita.

- Forza scansione delle modifiche nella cartella

Se questa opzione è abilitata, l'applicazione controlla periodicamente la presenza di modifiche nella cartella di aggiunta di contenuto nelle categorie. È possibile specificare la frequenza dei controlli (in ore) nel campo di immissione accanto alla casella di controllo. Per impostazione predefinita, l'intervallo di tempo fra i controlli forzati è di 24 ore.

Se questa opzione è disabilitata, non verranno forzati controlli della cartella. Il server tenta di accedere ai file modificati, aggiunti o eliminati.

Per impostazione predefinita, questa opzione è disabilitata.

8. Nella pagina della procedura guidata **Creazione della categoria di applicazioni**, fare clic sul pulsante **Fine**.

Al termine della procedura guidata, viene creata una categoria di applicazioni utente. È possibile visualizzare la nuova categoria creata utilizzando l'elenco di categorie nell'area di lavoro della cartella **Categorie di applicazioni**.

Se si desidera esportare una categoria di applicazioni in un file KLC, fare clic con il pulsante destro del mouse sul nome della categoria, selezionare **Esporta** nel menu, quindi nella finestra che si apre specificare il nome del file e fare clic su **Save**.

Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni

È possibile aggiungere file eseguibili relativi agli eventi **Avvio dell'applicazione non consentito** e **Avvio dell'applicazione non consentito in modalità di test** a una categoria di applicazioni esistente con contenuto aggiunto manualmente o a una nuova categoria di applicazioni.

Per aggiungere file eseguibili relativi agli eventi di Controllo Applicazioni alla categoria di applicazioni:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Nella scheda **Eventi** selezionare gli eventi desiderati.
4. Nel menu di scelta rapida di uno degli eventi selezionati selezionare **Aggiungi a categoria**.

5. Nella finestra **Azione sul file eseguibile relativo all'evento** visualizzata specificare le impostazioni attinenti:

   Selezionare uno dei seguenti:

   - **Aggiungi a una nuova categoria di applicazioni**

     Selezionare questa opzione se si desidera creare una nuova categoria di applicazioni.

     Fare clic sul pulsante **OK** per eseguire la Creazione guidata nuova categoria. Al termine della procedura guidata, viene creata la categoria con le impostazioni specificate.

     Per impostazione predefinita, questa opzione non è selezionata.

   - **Aggiungi a una categoria di applicazioni esistente**

     Selezionare questa opzione se si desidera aggiungere regole a una categoria di applicazioni esistente. Selezionare la categoria appropriata nell'elenco delle categorie di applicazioni.

     Questa opzione è selezionata per impostazione predefinita.

   Nella sezione **Tipo di regola** selezionare una delle seguenti impostazioni:

   - **Aggiungi a categoria**

     Selezionare questa opzione se si desidera aggiungere regole alle condizioni della categoria di applicazioni.

     Questa opzione è selezionata per impostazione predefinita.

   - **Regole per l'aggiunta alle esclusioni**

     Selezionare questa opzione se si desidera aggiungere regole alle esclusioni della categoria di applicazioni.

   Nella sezione **Tipo di info sul file** selezionare una delle seguenti impostazioni:

   - **Dettagli del certificato (o hash SHA256 per i file senza certificato)**

     I file possono essere firmati con un certificato. Più file possono essere firmati con lo stesso certificato. Ad esempio, lo stesso certificato può essere utilizzato per firmare differenti versioni della stessa applicazione o diverse applicazioni dello stesso fornitore. Quando si seleziona un certificato, possono essere inserite nella categoria diverse versioni di un'applicazione o diverse applicazioni dello stesso fornitore.

     Ogni file dispone di una specifica funzione hash SHA256 univoca. Quando si seleziona una funzione hash SHA256, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

     Selezionare questa opzione se si desidera aggiungere alle regole della categoria i dettagli del certificato di un file eseguibile (o la funzione hash SHA256 per i file senza certificato).

     Per impostazione predefinita, questa opzione è selezionata.

   - **Dettagli del certificato (i file senza certificato verranno ignorati)**

I file possono essere firmati con un certificato. Più file possono essere firmati con lo stesso certificato. Ad esempio, lo stesso certificato può essere utilizzato per firmare differenti versioni della stessa applicazione o diverse applicazioni dello stesso fornitore. Quando si seleziona un certificato, possono essere inserite nella categoria diverse versioni di un'applicazione o diverse applicazioni dello stesso fornitore.

Selezionare questa opzione se si desidera aggiungere i dettagli del certificato di un file eseguibile alle regole della categoria. Se il file eseguibile non dispone di alcun certificato, verrà ignorato. Nessuna informazione sul file verrà aggiunta alla categoria.

- **Solo SHA256 (i file senza hash verranno ignorati)**

  Ogni file dispone di una specifica funzione hash SHA256 univoca. Quando si seleziona una funzione hash SHA256, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

  Selezionare questa opzione se si desidera aggiungere solo i dettagli della funzione hash SHA256 del file eseguibile.

- **Solo MD5 (modalità non più in uso, solo per la versione di Kaspersky Endpoint Security 10 Service Pack 1)**

  Ogni file dispone di una specifica funzione hash MD5 univoca. Quando si seleziona una funzione hash MD5, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

  Selezionare questa opzione se si desidera aggiungere solo i dettagli della funzione hash MD5 del file eseguibile. Il calcolo della funzione hash MD5 è supportato da Kaspersky Endpoint Security 10 Service Pack 1 for Windows e da tutte le versioni precedenti.

6. Fare clic su **OK**.

Configurazione della gestione dell'avvio delle applicazioni nei dispositivi client

La categorizzazione delle applicazioni consente di ottimizzare la gestione delle esecuzioni delle applicazioni nei dispositivi. È possibile creare una categoria di applicazioni e configurare Controllo Applicazioni per un criterio in modo che solo le applicazioni della categoria specificata vengano avviate nei dispositivi in cui è applicato il criterio. Ad esempio, è stata creata una categoria che include le applicazioni denominate *Application_1* e *Application_2*. Dopo avere aggiunto questa categoria a un criterio, solo due applicazioni possono essere avviate nei dispositivi in cui viene applicato il criterio: *Application_1* e *Application_2*. Se un utente tenta di avviare un'applicazione che non è stata inclusa nella categoria, ad esempio *Application_3*, l'avvio dell'applicazione viene bloccato. Verrà visualizzata una notifica che indica che l'avvio di *Application_3* è vietato in base a una regola di Controllo Applicazioni. È possibile creare una categoria con contenuti aggiunti automaticamente in base a diversi criteri da una cartella specifica. In questo caso i file vengono automaticamente aggiunti alla categoria dalla cartella specificata. I file eseguibili delle applicazioni vengono copiati nella cartella specificata ed elaborati automaticamente. Le relative metriche vengono aggiunte alla categoria.

Per configurare la gestione dell'avvio delle applicazioni nei dispositivi client:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Categorie di applicazioni**.

2. Nell'area di lavoro della cartella **Categorie di applicazioni** creare una categoria di applicazioni che si desidera gestire durante l'avvio.

3. Nella cartella **Dispositivi gestiti**, nella scheda **Criteri**, fare clic sul pulsante **Nuovo criterio** per creare un nuovo criterio per Kaspersky Endpoint Security for Windows e seguire le istruzioni della procedura guidata.

   Se tale criterio esiste già, è possibile ignorare questo passaggio. È possibile configurare la gestione dell'avvio delle applicazioni in una categoria specificata tramite le impostazioni di questo criterio. Il nuovo criterio creato viene visualizzato nella cartella **Dispositivi gestiti**, nella scheda **Criteri**.

4. Selezionare **Proprietà** dal menu di scelta rapida del criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio di Kaspersky Endpoint Security for Windows.

5. Nella finestra delle proprietà del criterio di Kaspersky Endpoint Security for Windows, nella sezione **Controlli di sicurezza** → **Controllo Applicazioni** selezionare la casella **Controllo Applicazioni**.

6. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Regola di Controllo Applicazioni**.

7. Nella finestra **Regola di Controllo Applicazioni**, nell'elenco a discesa **Categoria** selezionare la categoria di applicazioni a cui applicare la regola di avvio. Configurare la regola di avvio per la categoria di applicazioni selezionata.

   Per Kaspersky Endpoint Security 10 Service Pack 2 e versioni successive, le categorie non vengono visualizzate se create in base al criterio dell'hash MD5 di un file eseguibile.

   Non è consigliabile aggiungere categorie create in base al criterio dell'hash SHA256 di un file eseguibile per le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2. Questo può comportare errori dell'applicazione.

   Istruzioni dettagliate per la configurazione delle regole di controllo sono disponibili nella Guida in linea di Kaspersky Endpoint Security for Windows.

8. Fare clic su **OK**.

Le applicazioni saranno eseguite nei dispositivi inclusi nella categoria specificata in base alla regola che è stata creata. La nuova regola creata verrà visualizzata nella finestra delle proprietà del criterio di Kaspersky Endpoint Security for Windows, nella sezione **Controllo Applicazioni**.

Visualizzazione dei risultati dell'analisi statistica delle regole di avvio applicate ai file eseguibili

Per visualizzare le informazioni sui file eseguibili di cui non è consentita l'esecuzione da parte degli utenti:

1. Nella cartella **Dispositivi gestiti** della struttura della console selezionare la scheda **Criteri**.

2. Selezionare **Proprietà** dal menu di scelta rapida del criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio dell'applicazione.

3. Nel riquadro **Sezioni** selezionare **Controlli di Sicurezza** e selezionare la sottosezione **Controllo Applicazioni**.

4. Fare clic sul pulsante **Analisi statica**.

   Verrà visualizzata la finestra **Analisi dell'elenco di diritti di accesso**. Nella parte sinistra della finestra viene visualizzato un elenco di utenti basato sui dati di Active Directory.

5. Selezionare un utente dall'elenco.

   Nella parte destra della finestra vengono visualizzate le categorie di applicazioni assegnate all'utente.

6. Per visualizzare i file eseguibili di cui non è consentita l'esecuzione da parte degli utenti, nella finestra **Analisi dell'elenco di diritti di accesso** fare clic sul pulsante **Visualizza file**.

   Verrà visualizzata una finestra, che contiene un elenco di file eseguibili proibiti.

7. Per visualizzare un elenco dei file eseguibili inclusi in una categoria, selezionare la categoria di applicazioni e fare clic sul pulsante **Visualizza i file nella categoria**.

   Viene visualizzata una finestra con un elenco dei file eseguibili inclusi nella categoria di applicazioni.

Visualizzazione del registro delle applicazioni

Kaspersky Security Center esegue l'inventario di tutto il software installato nei dispositivi gestiti.

Network Agent compila un elenco delle applicazioni installate in un dispositivo Windows o Linux, quindi trasmette questo elenco ad Administration Server. Per i dispositivi client basati su Windows, Network Agent riceve la maggior parte delle informazioni sulle applicazioni installate dal Registro di sistema di Windows. Per i dispositivi client basati su Linux, gli strumenti di gestione di pacchetti forniscono informazioni sulle applicazioni installate a Network Agent.

Per visualizzare il registro delle applicazioni installate nei dispositivi client:

Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Registro delle applicazioni**.

L'area di lavoro della cartella **Registro delle applicazioni** consente di visualizzare un elenco delle applicazioni installate nei dispositivi client e in Administration Server.

È possibile visualizzare i dettagli di qualsiasi applicazione aprendo il relativo menu di scelta rapida e selezionando **Proprietà**. La finestra delle proprietà dell'applicazione visualizza i dettagli dell'applicazione e le informazioni sui relativi file eseguibili, oltre a un elenco di dispositivi in cui è installata l'applicazione.

Nel menu di scelta rapida di un'applicazione presente nell'elenco è possibile:

- Aggiungere l'applicazione a una categoria di applicazioni.
- Assegnare un tag all'applicazione.
- Esportare l'elenco delle applicazioni in un file CSV o TXT.
- Visualizzare le proprietà dell'applicazione, ad esempio il nome del fornitore, il numero di versione, l'elenco dei file eseguibili, l'elenco dei dispositivi in cui è installata l'applicazione, l'elenco degli aggiornamenti software disponibili o l'elenco delle vulnerabilità del software rilevate.

Per visualizzare le applicazioni che corrispondono ai criteri specificati, è possibile utilizzare i campi di filtro nell'area di lavoro della cartella **Registro delle applicazioni**.

Nella finestra delle proprietà del dispositivo selezionato, nella sezione **Registro delle applicazioni** è possibile visualizzare l'elenco delle applicazioni installate nel dispositivo.

Generazione di un rapporto sulle applicazioni installate

Nell'area di lavoro **Registro delle applicazioni** è inoltre possibile fare clic sul pulsante **Visualizza il rapporto sulle applicazioni installate** per generare un rapporto contenente le statistiche dettagliate sulle applicazioni installate, incluso il numero di dispositivi in cui è installata ciascuna applicazione. Questo rapporto, che rimanda alla pagina **Rapporto sulle applicazioni installate**, contiene le informazioni sulle applicazioni Kaspersky e sul software di terze parti. Se si desiderano informazioni solo sulle applicazioni Kaspersky installate nei dispositivi client, nell'elenco **Riepilogo** selezionare AO Kaspersky Lab.

Le informazioni sulle applicazioni Kaspersky e sul software di terze parti installati nei dispositivi connessi agli Administration Server secondari e virtuali vengono anche memorizzate nel registro delle applicazioni dell'Administration Server primario. Dopo avere aggiunto i dati provenienti dagli Administration Server secondari e virtuali, fare clic sul pulsante **Visualizza il rapporto sulle applicazioni installate** e nella pagina **Rapporto sulle applicazioni installate** visualizzata sarà possibile visualizzare queste informazioni.

Per aggiungere informazioni dagli Administration Server secondari e virtuali al rapporto sulle applicazioni installate:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Nella scheda **Rapporti** selezionare **Rapporto sulle applicazioni installate**.
4. Selezionare **Proprietà** dal menu di scelta rapida del rapporto.

   Verrà visualizzata la finestra **Proprietà: Rapporto sulle applicazioni installate**.
5. Nella sezione **Gerarchia di Administration Server** selezionare la casella di controllo **Includi i dati degli Administration Server secondari e virtuali**.
6. Fare clic su **OK**.

   Le informazioni degli Administration Server secondari e virtuali saranno incluse nel **Rapporto sulle applicazioni installate**.

Modifica dell'ora di inizio dell'inventario software

Kaspersky Security Center esegue l'inventario di tutto il software installato nei dispositivi client gestiti che eseguono Windows.

Network Agent compila un elenco delle applicazioni installate in un dispositivo, quindi trasmette questo elenco ad Administration Server. Network Agent riceve automaticamente le informazioni sulle applicazioni installate dal Registro di sistema di Windows.

Per ridurre l'utilizzo delle risorse del dispositivo, per impostazione predefinita Network Agent inizia a ricevere le informazioni sulle applicazioni installate 10 minuti dopo l'avvio del servizio Network Agent.

Per modificare l'ora di inizio dell'inventario software dall'inizio dell'esecuzione del servizio Network Agent in un dispositivo:

1. Aprire il Registro di sistema del dispositivo in cui è installato Network Agent (ad esempio, in locale, utilizzando il comando regedit dal menu **Start** → **Esegui**).
2. Passare al seguente hive:
   - Per i sistemi a 32 bit:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - Per i sistemi a 64 bit:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. Per la chiave KLINV_INV_COLLECTOR_START_DELAY_SEC impostare il valore richiesto in secondi.
   Il valore predefinito è 600 secondi.
4. Riavviare il servizio Network Agent.

L'ora di inizio dell'inventario software, che viene calcolata a partire dall'esecuzione del servizio Network Agent, viene modificata.

Informazioni sulla gestione delle chiavi di licenza di applicazioni di terze parti

Kaspersky Security Center consente di tenere traccia dell'utilizzo della chiavi di licenza per le applicazioni di terze parti installate nei dispositivi gestiti. L'elenco delle applicazioni per le quali è possibile tenere traccia dell'utilizzo delle chiavi di licenza viene acquisito dal Registro delle applicazioni. Per ogni chiave di licenza è possibile specificare e tenere traccia della violazione delle seguenti restrizioni:

- Numero massimo di dispositivi in cui è possibile installare l'applicazione utilizzando questa chiave di licenza
- Data di scadenza della chiave di licenza

Kaspersky Security Center non controlla se si specifica o meno una chiave di licenza reale. È possibile tenere traccia solo delle restrizioni specificate. Se una delle restrizioni imposte su una chiave di licenza viene violata, Administration Server registra un evento di tipo informativo, avviso o errore funzionale.

Le chiavi di licenza sono associate a gruppi di applicazioni. Un gruppo di applicazioni è un gruppo di applicazioni di terze parti combinate in base a uno o più criteri. È possibile definire le applicazioni in base al nome dell'applicazione, alla versione, al fornitore e al tag. Un'applicazione viene aggiunta al gruppo se viene soddisfatto almeno uno dei criteri. A ogni gruppo di applicazioni è possibile associare più chiavi di licenza, ma ciascuna chiave di licenza può essere associata a un solo gruppo di applicazioni.

Un altro strumento che è possibile utilizzare per tenere traccia dell'utilizzo delle chiavi di licenza è il Rapporto sullo stato dei gruppi di applicazioni concesse in licenza. Questo rapporto fornisce informazioni sullo stato corrente dei gruppi di applicazioni concesse in licenza, tra cui:

- Numero di installazioni delle chiavi di licenza in ogni gruppo di applicazioni
- Numero di chiavi di licenza in uso e chiavi di licenza disponibili
- Elenco dettagliato delle applicazioni concesse in licenza installate nei dispositivi gestiti

Gli strumenti per la gestione delle chiavi di licenza di applicazioni di terze parti si trovano nella sottocartella **Utilizzo licenze di terze parti** (**Avanzate → Gestione applicazioni → Utilizzo licenze di terze parti**). In questa sottocartella è possibile creare gruppi di applicazioni, aggiungere chiavi di licenza e generare il Rapporto sullo stato dei gruppi di applicazioni concesse in licenza.

Gli strumenti per la gestione delle chiavi di licenza di applicazioni di terzi sono disponibili solo se è stata abilitata l'opzione Vulnerability e patch management nella finestra **Configura interfaccia**.

Creazione di gruppi di applicazioni concesse in licenza

Per creare un gruppo di applicazioni concesse in licenza:

1. Nella cartella **Avanzate → Gestione applicazioni** della struttura della console selezionare la sottocartella **Utilizzo licenze di terze parti**.

2. Fare clic sul pulsante **Aggiungi un gruppo di applicazioni concesse in licenza** per eseguire la procedura Aggiunta guidata gruppo di applicazioni concesse in licenza.

   Verrà avviata l'Aggiunta guidata gruppo di applicazioni concesse in licenza.

3. Nel passaggio **Dettagli del gruppo di applicazioni concesse in licenza** specificare quali applicazioni si desidera includere nel gruppo di applicazioni:

   - **Nome del gruppo di applicazioni concesse in licenza**

   - **Registra violazioni delle limitazioni**

     Se una delle restrizioni imposte su una chiave di licenza del gruppo di applicazioni viene violata, Administration Server registra un evento di tipo informativo, avviso o errore funzionale:

     - Evento informativo: **Sta per essere superato il limite di installazioni (è stato utilizzato più del 95%) per uno dei gruppi di applicazioni concesse in licenza**
     - Evento di avviso: **Il limite di installazioni sta per essere superato per uno dei gruppi di applicazioni concesse in licenza**
     - Evento di errore funzionale: **Limite di installazioni superato per uno dei gruppi di applicazioni concesse in licenza**

       Un evento viene registrato una sola volta, quando viene soddisfatta la condizione indicata. La volta successiva, lo stesso evento può essere registrato solo quando il numero di installazioni viene ripristinato a un livello normale e l'evento si verifica di nuovo. Un evento non può essere registrato più di una volta all'ora.

   - **Criteri per l'aggiunta delle applicazioni rilevate al gruppo di applicazioni concesse in licenza**

     Specificare i criteri per definire le applicazioni che si desidera includere nel gruppo di applicazioni. È possibile definire le applicazioni in base al nome dell'applicazione, alla versione, al fornitore e al tag. È necessario specificare almeno un criterio. Un'applicazione viene aggiunta al gruppo se viene soddisfatto almeno uno dei criteri.

4. Nel passaggio **Immettere i dati sulle chiavi di licenza esistenti** specificare le chiavi di licenza di cui si desidera tenere traccia. Selezionare l'opzione **Controlla il superamento del limite di licenze**, quindi aggiungere le chiavi di licenza:

   a. Fare clic sul pulsante **Aggiungi**.

   b. Selezionare la chiave di licenza che si desidera aggiungere e fare clic sul pulsante **OK**. Se la chiave di licenza richiesta non è elencata, fare clic sul pulsante **Aggiungi**, quindi specificare le proprietà della chiave di licenza.

5. Nella passaggio **Aggiungi gruppo di applicazioni concesse in licenza** fare clic sul pulsante **Fine**.

Verrà creato un gruppo di applicazioni concesse in licenza, che sarà visualizzato nella cartella **Utilizzo licenze di terze parti**.

Gestione delle chiavi di licenza per i gruppi di applicazioni concesse in licenza

Per creare una chiave di licenza per un gruppo di applicazioni concesse in licenza:

1. Nella cartella **Avanzate → Gestione applicazioni** della struttura della console selezionare la sottocartella **Utilizzo licenze di terze parti**.

2. Nell'area di lavoro della cartella **Utilizzo licenze di terze parti** fare clic sul pulsante **Gestisci chiavi di licenza delle applicazioni concesse in licenza**.

   Verrà aperta la finestra **Gestione delle chiavi di licenza nelle applicazioni concesse in licenza**.

3. Nella finestra **Gestione delle chiavi di licenza nelle applicazioni concesse in licenza** fare clic sul pulsante **Aggiungi**.

   Verrà aperta la finestra **Chiave di licenza**.

4. Nella finestra **Chiave di licenza** specificare le proprietà della chiave di licenza e le limitazioni imposte dalla chiave di licenza al gruppo di applicazioni concesse in licenza.

   - **Nome**. Nome della chiave di licenza.
   - **Commento**. Note sulla chiave di licenza selezionata.
   - **Limitazione**. Numero di dispositivi in cui è possibile installare l'applicazione utilizzando questa chiave di licenza.
   - **Scadenza**. Data di scadenza della chiave di licenza.

Le chiavi di licenza create vengono visualizzate nella finestra **Gestione delle chiavi di licenza nelle applicazioni concesse in licenza**.

Per applicare una chiave di licenza a un gruppo di applicazioni concesse in licenza:

1. Nella cartella **Avanzate → Gestione applicazioni** della struttura della console selezionare la sottocartella **Utilizzo licenze di terze parti**.

2. Nella cartella **Utilizzo licenze di terze parti** selezionare un gruppo di applicazioni concesse in licenza a cui si desidera applicare una chiave di licenza.

3. Selezionare **Proprietà** dal menu di scelta rapida del gruppo di applicazioni concesse in licenza.

   Verrà visualizzata la finestra delle proprietà del gruppo di applicazioni concesse in licenza.

4. Nella finestra delle proprietà del gruppo di applicazioni concesse in licenza, nella sezione **Chiavi di licenza** selezionare **Controlla il superamento del limite di licenze**.

5. Fare clic sul pulsante **Aggiungi**.

   Verrà aperta la finestra **Selezione di una chiave di licenza**.

6. Nella finestra **Selezione di una chiave di licenza** selezionare una chiave di licenza da applicare a un gruppo di applicazioni concesse in licenza.

7. Fare clic su **OK**.

Le limitazioni definite per un gruppo di applicazioni concesse in licenza e specificate nella chiave di licenza verranno applicate anche al gruppo di applicazioni concesse in licenza selezionato.

Inventario dei file eseguibili

È possibile ottenere un elenco di file eseguibili archiviati nei dispositivi gestiti. Per eseguire un inventario dei file eseguibili, è necessario creare un'attività di inventario.

La funzione di inventario dei file eseguibili è disponibile per le seguenti applicazioni:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent e versioni successive

Il numero di file eseguibili ricevuti da un singolo dispositivo non può essere superiore a 150.000. Una volta raggiunto questo limite, Kaspersky Security Center non può ricevere nuovi file.

Prima di iniziare, abilitare le notifiche sull'avvio delle applicazioni nel criterio Kaspersky Endpoint Security e nel criterio Network Agent, in modo da poter trasferire i dati all'Administration Server.

Per abilitare le notifiche sull'avvio delle applicazioni:

- Aprire le impostazioni dei criteri di Kaspersky Endpoint Security ed effettuare le seguenti operazioni:

  1. Passare a **Impostazioni generali** → **Rapporti e archivi**.
  2. Nella sezione **Trasferimento dei dati ad Administration Server**, selezionare la casella di controllo **Informazioni sulle applicazioni avviate**.
  3. Salvare le modifiche.

- Aprire le impostazioni dei criteri di Network Agent e procedere come segue:

  1. Passare alla sezione **Archivi**.
  2. Selezionare la casella di controllo **Informazioni dettagliate sulle applicazioni installate**.
  3. Salvare le modifiche.

Per creare un'attività di inventario per i file eseguibili nei dispositivi client:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Nell'area di lavoro della cartella **Attività** fare clic sul pulsante **Nuova attività**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nella finestra **Selezionare il tipo di attività** della procedura guidata selezionare **Kaspersky Endpoint Security** come tipo di attività, selezionare **Inventario** come sottotipo di attività, quindi fare clic su **Avanti**.
4. Seguire le rimanenti istruzioni della procedura guidata.

   Al termine della procedura guidata, verrà creata un'attività di inventario per Kaspersky Endpoint Security. L'attività creata viene visualizzata nell'elenco di attività nell'area di lavoro della cartella **Attività**.

Un elenco dei file eseguibili rilevati nei dispositivi durante l'inventario viene visualizzato nell'area di lavoro della cartella **File eseguibili**.

Durante inventario, l'applicazione rileva i file eseguibili nei seguenti formati: MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Visualizzazione delle informazioni sui file eseguibili

Per visualizzare un elenco di tutti i file eseguibili rilevati nei dispositivi client:

Nella cartella **Gestione applicazioni** della struttura della console selezionare la sottocartella **File eseguibili**.

Nell'area di lavoro della cartella **File eseguibili** viene visualizzato un elenco dei file eseguibili avviati nei dispositivi o rilevati durante l'esecuzione dell'attività di inventario di Kaspersky Endpoint Security for Windows.

Per visualizzare i dettagli sui file eseguibili che soddisfano i criteri specificati, è possibile utilizzare i filtri.

Per visualizzare le proprietà di un file eseguibile:

Dal menu di scelta rapida del file selezionare **Proprietà**.

Verrà visualizzata una finestra che contiene le informazioni sul file eseguibile e un elenco dei dispositivi in cui è stato rilevato il file eseguibile.

Monitoraggio e generazione dei rapporti

Questa sezione illustra le funzionalità di monitoraggio e reportistica di Kaspersky Security Center. Queste funzionalità offrono una panoramica dell'infrastruttura, degli stati di protezione e delle statistiche.

Dopo la distribuzione di Kaspersky Security Center o durante l'esecuzione, è possibile configurare le funzionalità di monitoraggio e generazione dei rapporti in base alle esigenze.

- **Indicatori a semaforo**

  Administration Console consente di valutare rapidamente lo stato attuale di Kaspersky Security Center e dei dispositivi gestiti controllando indicatori a semaforo.

- **Statistiche**

  Le statistiche sullo stato del sistema di protezione e dei dispositivi gestiti vengono visualizzate in riquadri informazioni che possono essere personalizzati.

- **Rapporti**

  La funzionalità Rapporti consente di ottenere informazioni numeriche dettagliate sulla sicurezza della rete dell'organizzazione, nonché di salvare le informazioni in un file, inviarlo tramite e-mail e stamparlo.

- **Eventi**

  Le selezioni eventi consentono di visualizzare i set denominati degli eventi selezionati dal database di Administration Server. Questi set di eventi sono raggruppati in base alle seguenti categorie:

  - In base al livello di importanza: **Eventi critici**, **Errori funzionali**, **Avvisi** e **Eventi informativi**
  - In base al tempo: **Eventi recenti**
  - In base al tipo: **Richieste utente** e **Eventi di controllo**

È possibile creare e visualizzare le selezioni eventi definite dall'utente in base alle impostazioni disponibili per la configurazione nell'interfaccia di Kaspersky Security Center Web Console.

Scenario: monitoraggio e generazione dei rapporti

Questa sezione fornisce uno scenario per la configurazione della funzionalità di monitoraggio e generazione dei rapporti in Kaspersky Security Center.

Prerequisiti

Dopo aver distribuito Kaspersky Security Center nella rete di un'organizzazione, è possibile iniziare a monitorarlo e generare rapporti sul relativo funzionamento.

Passaggi

Il monitoraggio e la generazione dei rapporti nella rete di un'organizzazione prevede diversi passaggi:

1. **Configurazione del passaggio degli stati del dispositivo**

   Acquisire familiarità con le impostazioni che definiscono l'assegnazione degli stati del dispositivo in base a condizioni specifiche. Modificando queste impostazioni, è possibile modificare il numero di eventi con livelli di importanza *Critico* o *Avviso*.

   Quando si configura la modifica degli stati del dispositivo, assicurarsi che le nuove impostazioni non siano in conflitto con i criteri di protezione delle informazioni della propria organizzazione e di essere in grado di reagire tempestivamente agli eventi di sicurezza importanti nella rete dell'organizzazione.

2. **Configurazione delle notifiche degli eventi nei dispositivi client**

   Configurare la notifica (tramite e-mail, SMS o avviando un file eseguibile) degli eventi nei dispositivi client in base alle esigenze dell'organizzazione.

3. **Modifica della risposta della rete di sicurezza all'evento Epidemia di virus**

   Per regolare la risposta della rete ai nuovi eventi, è possibile modificare le specifiche soglie nelle proprietà di Administration Server. È inoltre possibile creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.

4. **Gestione delle statistiche**

   Configurare la visualizzazione delle statistiche in base alle esigenze dell'organizzazione.

5. **Analisi dello stato di sicurezza della rete dell'organizzazione**

   Per analizzare lo stato di sicurezza della rete dell'organizzazione, è possibile eseguire una delle seguenti operazioni:

   - Nell'area di lavoro del nodo di **Administration Server**, nella scheda **Statistiche** aprire la scheda di secondo livello (pagina) **Stato protezione** ed esaminare il riquadro informazioni **Stato protezione in tempo reale**
   - Generare ed esaminare il **Rapporto sullo stato della protezione**
   - Generare ed esaminare il **Rapporto sugli errori**

6. **Individuazione dei dispositivi client che non sono protetti**

   Per individuare i dispositivi client non protetti, accedere all'area di lavoro del nodo di **Administration Server**, nella scheda **Statistiche** aprire la scheda di secondo livello (pagina) **Stato protezione** ed esaminare il riquadro informazioni **Cronologia di individuazione dei nuovi dispositivi nella rete**. È inoltre possibile generare ed esaminare il **Rapporto sulla distribuzione della protezione**.

7. **Verifica della protezione dei dispositivi client**

   Per verificare la protezione dei dispositivi client, accedere all'area di lavoro del nodo di **Administration Server**, nella scheda **Statistiche** aprire la scheda di secondo livello (pagina) **Distribuzione** o **Statistiche delle minacce** ed esaminare i relativi riquadri informazioni. È inoltre possibile avviare ed esaminare la selezione eventi **Eventi critici**.

8. **Valutazione e limitazione del carico di eventi nel database**

   Le informazioni sugli eventi che si verificano durante il funzionamento delle applicazioni gestite vengono trasferite da un dispositivo client e registrate nel database di Administration Server. Per ridurre il carico su Administration Server, valutare e limitare il numero massimo di eventi che possono essere archiviati nel database.

   Per valutare il carico di eventi sul database, calcolare lo spazio nel database. È inoltre possibile limitare il numero massimo di eventi per evitare l'overflow del database.

9. **Analisi delle informazioni sulla licenza**

   Per esaminare le informazioni sulla licenza, accedere all'area di lavoro del nodo di **Administration Server**, nella scheda **Statistiche** aprire la scheda di secondo livello (pagina) **Distribuzione** ed esaminare il riquadro informazioni **Utilizzo chiavi di licenza**. È inoltre possibile generare ed esaminare il **Rapporto sull'utilizzo delle chiavi di licenza**.

Risultati

Al termine dello scenario, si dispone di informazioni sulla protezione della rete dell'organizzazione e quindi è possibile pianificare le azioni per il miglioramento della protezione.

Monitoraggio dei semafori e degli eventi registrati in Administration Console

Administration Console consente di valutare rapidamente lo stato attuale di Kaspersky Security Center e dei dispositivi gestiti controllando indicatori a semaforo. Gli indicatori a semaforo sono visualizzati nell'area di lavoro del nodo **Administration Server**, nella scheda **Monitoraggio**. La scheda fornisce sei riquadri informazioni con indicatori a semaforo ed eventi registrati. L'indicatore a semaforo è una barra verticale colorata a sinistra di un riquadro. Ogni riquadro con un indicatore corrisponde a uno specifico ambito funzionale di Kaspersky Security Center (vedere la tabella seguente).

Ambiti coperti dagli indicatori a semaforo in Administration Console

Nome del riquadro	Ambito dell'indicatore
Distribuzione	Installazione di Network Agent e delle applicazioni di protezione nei dispositivi nella rete di un'organizzazione
Schema di gestione	Struttura dei gruppi di amministrazione. Scansione della rete. Regole di spostamento dei dispositivi
Impostazioni di protezione	Funzionalità dell'applicazione di protezione: stato protezione, scansione malware
Aggiorna	Aggiornamenti e patch
Monitoraggio	Stato protezione
Administration Server	Funzionalità e proprietà di Administration Server

Ogni indicatore a semaforo può assumere cinque colori (vedere la tabella seguente). Il colore di un indicatore dipende dallo stato attuale di Kaspersky Security Center e dagli eventi che sono stati registrati.

Colori degli indicatori a semaforo

Stato	Colore dell'indicatore	Significato del colore dell'indicatore
Informativo	Verde	Non è richiesto l'intervento dell'amministratore.
Avviso	Giallo	È richiesto l'intervento dell'amministratore.
Critico	Rosso	Si sono verificati problemi gravi. È richiesto l'intervento dell'amministratore per risolverli.

Stato	Colore dell'indicatore	Significato del colore dell'indicatore
Informativo	Azzurro	Sono stati registrati eventi che non sono correlati a minacce potenziali o effettive per la sicurezza dei dispositivi gestiti.
Informativo	Grigio	I dettagli degli eventi non sono disponibili o non sono stati ancora recuperati.

L'obiettivo dell'amministratore è quello di tenere attivi gli indicatori a semaforo in tutti i riquadri informazioni nella scheda **Monitoraggio** verde.

I riquadri informazioni mostrano anche gli eventi registrati che interessano i semafori e lo stato di Kaspersky Security Center (vedere la tabella seguente).

Nome, descrizione e colori dei semafori degli eventi registrati

Colore dell'indicatore	Nome visualizzato del tipo di evento	Tipo di evento	Descrizione
Rosso	**Licenza scaduta in %1 dispositivi**	IDS_AK_STATUS_LIC_EXPAIRED	Eventi di questo tipo si verificano alla scadenza della licenza commerciale. Una volta al giorno, Kaspersky Security Center verifica se la licenza nei dispositivi è scaduta. Alla scadenza della licenza commerciale, Kaspersky Security Center fornisce solo le funzionalità di base. Per continuare a utilizzare Kaspersky Security Center, rinnovare la licenza commerciale.
Rosso	**Applicazione di protezione non in esecuzione in: %1 dispositivi**	IDS_AK_STATUS_AV_NOT_RUNNING	Eventi di questo tipo si verificano quando l'applicazione di protezione installata nel dispositivo non è in esecuzione. Verificare che Kaspersky Endpoint Security sia in esecuzione nel dispositivo.
Rosso	**Protezione disabilitata in: %1 dispositivi**	IDS_AK_STATUS_RTP_NOT_RUNNING	Eventi di questo tipo si verificano quando l'applicazione di protezione nel dispositivo è stata disabilitata per un periodo superiore all'intervallo di tempo specificato. Verificare lo stato corrente della protezione in tempo reale nel dispositivo e assicurarsi che tutti i componenti di protezione necessari siano abilitati.
Rosso	**Una vulnerabilità del software è stata rilevata nei dispositivi**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Eventi di questo tipo si verificano quando l'attività *Trova vulnerabilità e aggiornamenti richiesti* ha rilevato vulnerabilità con il livello di criticità specificato nelle applicazioni installate nel dispositivo. Verificare l'elenco degli aggiornamenti disponibili nella sottocartella **Aggiornamenti software** inclusa nella cartella **Gestione applicazioni**. Questa cartella contiene un elenco degli aggiornamenti per le applicazioni Microsoft e di altri fornitori di software recuperati da Administration Server che possono essere distribuiti ai dispositivi. Dopo aver visualizzato le informazioni sugli aggiornamenti disponibili, installarli nel dispositivo.
Rosso	**Eventi critici registrati in Administration Server**	IDS_AK_STATUS_EVENTS_OCCURED	Eventi di questo tipo si verificano quando vengono rilevati eventi critici di Administration Server. Verificare l'elenco degli eventi archiviati in Administration Server, quindi correggere singolarmente gli eventi critici.

Colore dell'indicatore	Nome visualizzato del tipo di evento	Tipo di evento	Descrizione
Rosso	**Sono stati registrati errori negli eventi in Administration Server**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Eventi di questo tipo si verificano quando vengono registrati errori imprevisti sul lato Administration Server. Verificare l'elenco degli eventi archiviati in Administration Server, quindi correggere singolarmente gli errori.
Rosso	**Connessione a %1 dispositivi interrotta**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Eventi di questo tipo si verificano quando si perde la connessione tra Administration Server e il dispositivo. Visualizzare l'elenco dei dispositivi disconnessi e provare a riconnetterli.
Rosso	**%1 dispositivi non si connettono ad Administration Server da molto tempo**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Eventi di questo tipo si verificano quando il dispositivo non viene connesso ad Administration Server nell'intervallo di tempo specificato, perché il dispositivo era spento. Verificare che il dispositivo sia acceso e che Network Agent sia in esecuzione.
Rosso	**Dispositivi con stato diverso da OK: %1**	IDS_AK_STATUS_HOST_NOT_OK	Eventi di questo tipo si verificano quando lo stato *OK* del dispositivo connesso ad Administration Server cambia in *Critico* o *Avviso*. È possibile risolvere il problema utilizzando l'utilità di diagnostica remota di Kaspersky Security Center.
Rosso	**Database non aggiornati in: %1 dispositivi**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Eventi di questo tipo si verificano quando i database anti-virus non sono stati aggiornati nel dispositivo nell'intervallo di tempo specificato. Seguire le istruzioni per aggiornare i database di Kaspersky.
Rosso	**Dispositivi in cui la verifica della disponibilità di aggiornamenti di Windows Update non viene eseguita da molto tempo: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Eventi di questo tipo si verificano quando l'attività *Esegui sincronizzazione di Windows Update* non viene eseguita nell'intervallo di tempo specificato. Seguire le istruzioni per sincronizzare gli aggiornamenti di Windows Update con Administration Server.
Rosso	**È necessario installare %1 plug-in per Kaspersky Security Center**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Eventi di questo tipo si verificano quando è necessario installare plug-in aggiuntivi per le applicazioni Kaspersky. Scaricare e installare i plug-in di gestione richiesti per l'applicazione Kaspersky dal sito Web del servizio di assistenza tecnica di Kaspersky.

Utilizzo di rapporti, statistiche e notifiche

Questa sezione contiene informazioni sull'utilizzo dei rapporti, delle statistiche e delle selezioni eventi e dispositivi in Kaspersky Security Center, oltre che sulle modalità di configurazione delle notifiche di Administration Server.

Utilizzo dei rapporti

I rapporti in Kaspersky Security Center contengono informazioni sullo stato dei dispositivi gestiti. I rapporti vengono generati in base alle informazioni memorizzate in Administration Server. È possibile creare rapporti per i seguenti tipi di oggetti:

- Per selezioni dispositivi create in base a impostazioni specifiche.
- Per gruppi di amministrazione.
- Per dispositivi specifici in diversi gruppi di amministrazione.
- Per tutti i dispositivi della rete (nel rapporto sulla distribuzione).

L'applicazione dispone di una selezione di modelli di rapporto standard. È inoltre possibile creare modelli di rapporto personalizzati. I rapporti vengono visualizzati nella finestra principale dell'applicazione, nella cartella **Administration Server** della struttura della console.

Creazione di un modello di rapporto

Per creare un modello di rapporto:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Fare clic sul pulsante **Nuovo modello di rapporto**.

   Verrà avviata la Creazione guidata nuovo modello di rapporto. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, il modello di rapporto creato verrà aggiunto nella cartella **Administration Server** selezionata nella struttura della console. È possibile utilizzare questo modello per la creazione e la visualizzazione dei rapporti.

Visualizzazione e modifica delle proprietà dei modelli di rapporto

È possibile visualizzare e modificare le proprietà di base di un modello di rapporto, ad esempio il nome del modello di rapporto o i campi visualizzati nel rapporto.

Per visualizzare e modificare le proprietà di un modello di rapporto:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Nell'elenco dei modelli di rapporto selezionare il modello di rapporto desiderato.

4. Selezionare **Proprietà** dal menu di scelta rapida del modello di rapporto selezionato.

   In alternativa, è possibile generare il rapporto e quindi fare clic sul pulsante **Apri proprietà del modello di rapporto** o sul pulsante **Configura colonne del rapporto**.

5. Nella finestra visualizzata modificare le proprietà del modello di rapporto. Le proprietà di ogni rapporto possono contenere solo alcune delle sezioni descritte di seguito.

   - Sezione **Generale**:
     - Nome del modello di rapporto
     - Numero massimo di voci da visualizzare

       Se questa opzione è abilitata, il numero di voci visualizzate nella tabella con i dati dettagliati del rapporto non supera il valore specificato.

       Le voci nei rapporti vengono prima ordinate in base alle regole specificate nella sezione **Campi** → **Campi dettagli** delle proprietà del modello di rapporto, quindi vengono mantenute solo le prime voci risultanti. Il titolo della tabella con i dati dettagliati del rapporto mostra il numero di voci visualizzate e il numero totale di voci disponibili, corrispondenti alle altre impostazioni del modello di rapporto.

       Se questa opzione è disabilitata, la tabella con i dati dettagliati del rapporto conterrà tutte le voci disponibili. Non è consigliabile disabilitare questa opzione. La limitazione del numero di voci visualizzate nel rapporto consente di ridurre il carico sul sistema di gestione database (DBMS) e il tempo necessario per la creazione e l'esportazione del rapporto. Alcuni rapporti contengono un numero eccessivo di voci. In questi casi, potrebbe essere difficile leggerle e analizzarle tutte. Inoltre, nel dispositivo potrebbe verificarsi l'esaurimento della memoria durante la generazione di un rapporto e, in questo caso, non sarà possibile visualizzare il rapporto.

       Per impostazione predefinita, questa opzione è abilitata. Il valore predefinito è 1000.

     - Versione per la stampa

       L'output del rapporto viene ottimizzato per la stampa, aggiungendo spazi tra alcuni valori per una maggiore leggibilità.

       Per impostazione predefinita, questa opzione è abilitata.

   - Sezione **Campi**.

     Selezionare i campi che verranno visualizzati nel rapporto e l'ordine di questi campi e configurare se le informazioni nel rapporto devono essere ordinate e filtrate in base a ognuno dei campi.

   - Sezione **Intervallo**.

     Modificare il periodo del rapporto. I valori disponibili sono i seguenti:

     - Tra le due date specificate
     - Dalla data specificata alla data di creazione del rapporto
     - Dalla data di creazione del rapporto meno il numero specificato di giorni alla data di creazione del rapporto

   - Sezione **Gruppo**, **Device selection** o **Devices**.

     Modificare il set di dispositivi client per cui creare il rapporto. Solo una di queste sezioni può essere presente, a seconda delle impostazioni specificate durante la creazione del modello di rapporto.

- Sezione **Impostazioni**.

  Modificare le impostazioni del rapporto. Il set di impostazioni esatto dipende dallo specifico rapporto.

- Sezione **Sicurezza**. **Eredita le impostazioni da Administration Server**

  Se questa opzione è abilitata, le impostazioni di protezione del rapporto vengono ereditate dall'Administration Server.

  Se questa opzione è disabilitata, è possibile configurare le impostazioni di protezione per il rapporto. È possibile assegnare un ruolo a un utente o un gruppo di utenti o assegnare autorizzazioni a un utente o un gruppo di utenti, come applicabile per il rapporto.

  Per impostazione predefinita, questa opzione è abilitata.

  La sezione **Sicurezza** è disponibile se la casella di controllo **Visualizza le sezioni delle impostazioni di protezione** è selezionata nella finestra delle impostazioni dell'interfaccia.

- Sezione **Gerarchia di Administration Server**:

  - **Includi i dati degli Administration Server secondari e virtuali**

    Se questa opzione è abilitata, il rapporto include le informazioni ottenute dagli Administration Server secondari e virtuali subordinati all'Administration Server per cui viene creato il modello di rapporto.

    Disabilitare questa opzione per visualizzare solo i dati relativi all'Administration Server corrente.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Fino al livello di nidificazione**

    Il rapporto include i dati degli Administration Server secondari e virtuali posizionati al di sotto dell'Administration Server corrente a un livello di nidificazione minore o uguale al valore specificato.

    Il valore predefinito è 1. È consigliabile modificare questo valore se è necessario recuperare informazioni da Administration Server secondari posizionati a livelli inferiori della struttura.

  - **Intervallo di attesa dati (min.)**

    Prima della generazione del rapporto, l'Administration Server per cui viene creato il modello di rapporto attende i dati dagli Administration Server secondari per il numero di minuti specificato. Se non viene ricevuto alcun dato da un Administration Server secondario al termine di questo periodo, il rapporto viene eseguito comunque. Anziché i dati effettivi, il rapporto mostra i dati recuperati dalla cache (se è abilitata l'opzione **Salva nella cache i dati degli Administration Server secondari**) oppure **N/D** (non disponibile) in caso contrario.

    Il valore predefinito è 5 (minuti).

  - **Salva nella cache i dati degli Administration Server secondari**

Gli Administration Server secondari trasferiscono regolarmente i dati all'Administration Server per cui viene creato il modello di rapporto. I dati trasferiti vengono quindi archiviati nella cache.

Se l'Administration Server corrente non riesce a ricevere i dati da un Administration Server secondario durante la generazione del rapporto, il rapporto mostra i dati recuperati dalla cache. Verrà anche visualizzata la data in cui i dati sono stati trasferiti nella cache.

Se questa opzione è abilitata, è possibile visualizzare le informazioni dagli Administration Server secondari, anche se non è possibile recuperare i dati aggiornati. I dati visualizzati potrebbero tuttavia essere obsoleti.

Per impostazione predefinita, questa opzione è disabilitata.

- **Frequenza di aggiornamento cache (ore)**

  A intervalli regolari gli Administration Server secondari trasferiscono i dati all'Administration Server per cui viene creato il modello di rapporto. È possibile specificare questo periodo in ore. Se si specificano 0 ore, i dati vengono trasferiti solo al momento della generazione del rapporto.

  Il valore predefinito è 0.

- **Trasferisci informazioni dettagliate dagli Administration Server secondari**

  Nel rapporto generato, la tabella con i dati dettagliati del rapporto include i dati ottenuti dagli Administration Server secondari dell'Administration Server per cui viene creato il modello di rapporto.

  L'abilitazione di questa opzione rallenta la generazione dei rapporti e aumenta il traffico tra gli Administration Server. È tuttavia possibile visualizzare tutti i dati in un solo rapporto.

  Anziché attivare questa opzione, può essere preferibile analizzare i dati dettagliati del rapporto per identificare un Administration Server secondario che presenta problemi e quindi generare lo stesso rapporto solo per tale Administration Server.

  Per impostazione predefinita, questa opzione è disabilitata.

Formato filtro esteso nei modelli di rapporto

In Kaspersky Security Center 15.1 è possibile applicare il formato filtro esteso a un modello di rapporto. Il formato filtro esteso offre maggiore flessibilità rispetto al formato predefinito. È possibile creare condizioni di filtro complesse utilizzando un set di filtri, che verrà applicato al rapporto tramite l'operatore logico OR durante la creazione del rapporto, come illustrato di seguito:

Filtro[1](Campo[1] AND Filtro[2]... AND Campo[n]) OR Filtro[2](Campo[1] AND Campo[2]... AND Campo[n]) OR... Filtro[n](Campo[1] AND Campo[2]... AND Campo[n])

Con il formato filtro esteso è inoltre possibile impostare un valore di intervallo di tempo in un formato di tempo relativo (utilizzando ad esempio una condizione "Per gli ultimi N giorni") per determinati campi in un filtro. La disponibilità e il set di condizioni dell'intervallo di tempo dipendono dal tipo di modello di rapporto.

Conversione del filtro nel formato esteso

Il formato filtro esteso per i modelli di rapporto è supportato solo in Kaspersky Security Center 12 e versioni successive. Dopo la conversione del filtro predefinito nel formato esteso, il modello di rapporto diventa incompatibile con gli Administration Server della rete in cui sono installate versioni precedenti di Kaspersky Security Center. Le informazioni di questi Administration Server non verranno ricevute per il rapporto.

Per convertire il filtro predefinito del modello di rapporto nel formato esteso:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Nell'elenco dei modelli di rapporto selezionare il modello di rapporto desiderato.
4. Selezionare **Proprietà** dal menu di scelta rapida del modello di rapporto selezionato.
5. Nella finestra delle proprietà visualizzata selezionare la sezione **Campi**.
6. Nella scheda **Campi dettagli** fare clic sul collegamento **Converti filtro**.
7. Nella finestra visualizzata fare clic sul pulsante **OK**.

   La conversione nel formato di filtro esteso è irreversibile per il modello di rapporto a cui viene applicata. Se il collegamento **Converti filtro** è stato selezionato accidentalmente, è possibile annullare le modifiche facendo clic sul pulsante **Annulla** nella finestra delle proprietà del modello di rapporto.

8. Per applicare le modifiche, chiudere la finestra delle proprietà del modello di rapporto facendo clic sul pulsante **OK**.

   Quando si apre nuovamente la finestra delle proprietà del modello di rapporto, viene visualizzata la nuova sezione **Filtri** disponibile. In questa sezione è possibile configurare il filtro esteso.

Configurazione del filtro esteso

Per configurare il filtro esteso nelle proprietà del modello di rapporto:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Nell'elenco dei modelli di rapporto, selezionare il modello di rapporto precedentemente convertito nel formato di filtro esteso.
4. Selezionare **Proprietà** dal menu di scelta rapida del modello di rapporto selezionato.
5. Nella finestra delle proprietà visualizzata selezionare la sezione **Filtri**.

   La sezione **Filtri** non viene visualizzata se il modello di rapporto non è stato precedentemente convertito nel formato di filtro esteso.

   Nella sezione **Filtri** della finestra delle proprietà del modello di rapporto è possibile esaminare e modificare l'elenco dei filtri applicati al rapporto. Ogni filtro nell'elenco ha un nome univoco e rappresenta un set di filtri per i campi corrispondenti nel rapporto.

6. Aprire la finestra delle impostazioni di filtro in uno dei seguenti modi:

   - Per creare un nuovo filtro, fare clic sul pulsante **Aggiungi**.
   - Per modificare il filtro esistente, selezionare il filtro richiesto e fare clic sul pulsante **Modifica**.

7. Nella finestra visualizzata selezionare e specificare i valori dei campi richiesti del filtro.
8. Fare clic sul pulsante **OK** per salvare le modifiche e chiudere la finestra.

   Se si sta creando un nuovo filtro, è necessario specificare il nome del filtro nel campo **Nome filtro** prima di fare clic sul pulsante **OK**.

9. Chiudere la finestra delle proprietà del modello di rapporto facendo clic sul pulsante **OK**.

   Il filtro esteso nel modello di rapporto è stato configurato. Adesso è possibile creare rapporti utilizzando questo modello di rapporto.

Creazione e visualizzazione di un rapporto

Per creare e visualizzare un rapporto:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Nell'elenco dei modelli di rapporto fare doppio clic sul modello di rapporto desiderato.

   Verrà visualizzato un rapporto per il modello selezionato.

Il rapporto include i seguenti dati:

- Nome e tipo di rapporto, breve descrizione e periodo di generazione del rapporto, oltre che informazioni sul gruppo di dispositivi per cui è stato generato il rapporto.
- Grafico con i dati più significativi del rapporto.
- Tabella consolidata con indicatori del rapporto calcolati.
- Tabella con dati dettagliati del rapporto.

Salvataggio di un rapporto

Per salvare un rapporto creato:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Nell'elenco dei modelli di rapporto selezionare il modello di rapporto desiderato.
4. Selezionare **Salva** nel menu di scelta rapida del rapporto selezionato.

Verrà avviato il Salvataggio guidato rapporto. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, verrà aperta la cartella in cui è stato salvato il file del rapporto.

Quando si salva un rapporto come file XLS, tutte le immagini correlate, come il logo e il datagramma, vengono salvate come file separati.

Creazione di un'attività di invio dei rapporti

I rapporti possono esser inviati tramite e-mail. L'invio di rapporti in Kaspersky Security Center viene eseguito utilizzando l'attività di invio dei rapporti.

Per creare un'attività di invio per un singolo rapporto:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Nell'elenco dei modelli di rapporto selezionare il modello di rapporto desiderato.
4. Selezionare **Invia rapporti** nel menu di scelta rapida del modello di rapporto selezionato.

   Verrà avviata la Creazione guidata attività di invio rapporto. Seguire le istruzioni della procedura guidata.

Per creare un'attività di invio per più rapporti:

1. Nella struttura della console, nel nodo con il nome dell'Administration Server desiderato, selezionare la cartella **Attività**.
2. Nell'area di lavoro della cartella **Attività** fare clic sul pulsante **Crea attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

   L'attività di invio del rapporto creata è visualizzata nella cartella **Attività** nella struttura della console.

L'attività per l'invio del rapporto viene creata automaticamente se sono stati specificati le impostazioni e-mail durante l'installazione di Kaspersky Security Center.

Passaggio 1. Selezione del tipo di attività

Nella finestra **Selezionare il tipo di attività**, nell'elenco delle attività selezionare **Invia rapporti** come tipo di attività.

Fare clic su **Avanti** per procedere al passaggio successivo.

Passaggio 2. Selezione del tipo di rapporto

Nella finestra **Selezionare il tipo di rapporto**, nell'elenco dei modelli per la creazione delle attività, selezionare il tipo di rapporto.

Fare clic su **Avanti** per procedere al passaggio successivo.

Passaggio 3. Azioni su un rapporto

Nella finestra **Azione da applicare ai rapporti** specificare le seguenti impostazioni:

- **Invia rapporti tramite e-mail**

  Se questa opzione è abilitata, l'applicazione invia i rapporti generati tramite e-mail.

  È possibile configurare l'invio del rapporto tramite e-mail facendo clic sul collegamento **Impostazioni di notifica e-mail**. Il collegamento è disponibile se l'opzione è abilitata.

  Se questa opzione è disabilitata, l'applicazione salva i rapporti nella cartella specificata per l'archiviazione.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Salva rapporti nella cartella condivisa**

  Se questa opzione è abilitata, l'applicazione salva i rapporti nella cartella specificata nel campo sotto la casella di controllo. Per salvare i rapporti in una cartella condivisa, specificare il percorso UNC della cartella. In questo caso, nella finestra **Selezione di un account per l'esecuzione dell'attività** è necessario specificare l'account utente e la password per l'accesso a questa cartella.

  Se questa opzione è disabilitata, l'applicazione non salva i rapporti nella cartella ma li invia tramite e-mail.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Sovrascrivi i rapporti precedenti dello stesso tipo**

  Se questa opzione è abilitata, a ogni avvio dell'attività il nuovo file di rapporto sovrascriverà il file salvato nella cartella dei rapporti al precedente avvio dell'attività.

  Se questa opzione è disabilitata, i file di rapporto non verranno sovrascritti. Un nuovo file di rapporto viene archiviato nella cartella dei rapporti a ogni avvio dell'attività.

  La casella di controllo è disponibile se l'opzione **Salva rapporto nella cartella** è selezionata.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Specifica l'account per accedere alla cartella condivisa**

  Se questa opzione è abilitata, è possibile specificare l'account con cui il rapporto verrà salvato nella cartella. Se viene specificato un percorso UNC di una cartella condivisa per l'impostazione **Salva rapporto nella cartella** nella finestra **Azione da applicare al rapporto**, è necessario specificare l'account utente e la password per l'accesso a questa cartella.

  Se questa opzione è disabilitata, il rapporto viene salvato nella cartella con l'account di Administration Server.

  La casella di controllo è disponibile se l'opzione **Salva rapporto nella cartella** è selezionata.

  Per impostazione predefinita, questa opzione è disabilitata.

Quando si salva o si invia un rapporto come file XLS, tutte le immagini correlate, come il logo e il datagramma, vengono salvate come file separati.

Fare clic su **Avanti** per procedere al passaggio successivo.

Passaggio 4. Selezione dell'account per l'avvio dell'attività

Nella finestra **Selezione di un account per l'esecuzione dell'attività** è possibile specificare l'account da utilizzare durante l'esecuzione dell'attività. Selezionare una delle seguenti opzioni:

- **Account predefinito**

  L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

  Per impostazione predefinita, questa opzione è selezionata.

- **Specifica account**

  Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

  - **Account**

    Account tramite il quale viene eseguita l'attività.

  - **Password**

    Password dell'account con cui verrà eseguita l'attività.

Fare clic su **Avanti** per procedere al passaggio successivo.

Passaggio 5. Configurazione di una pianificazione attività

Nella pagina **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio delle attività. Se necessario, definire le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N settimane**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

  - **Settimanale**

    L'attività viene eseguita ogni settimana nel giorno specificato e all'ora specificata.

- **In base ai giorni della settimana**

  L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

  Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

- **Mensile**

  L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

  Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

  Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- **Durante un'epidemia di virus**

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

- Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
- Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

  Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
- Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

Passaggio 6. Definizione del nome dell'attività

Nella finestra **Definire il nome dell'attività** specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali (`"*<>?\:|`).

Fare clic su **Avanti** per procedere al passaggio successivo.

Passaggio 7. Completamento della creazione dell'attività

Nella finestra **Completare la creazione dell'attività** fare clic sul pulsante **Fine** per completare la procedura guidata.

Se si desidera che l'attività venga avviata al termine della procedura guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Gestione delle statistiche

Le statistiche sullo stato del sistema di protezione e dei dispositivi gestiti vengono visualizzate in riquadri informazioni che possono essere personalizzati. Le statistiche sono visualizzate nell'area di lavoro del nodo **Administration Server**, nella scheda **Statistiche**. La scheda contiene alcune schede di secondo livello (pagine). Ogni pagina a schede visualizza riquadri informazioni con statistiche, nonché collegamenti a notizie e altri materiali di Kaspersky. Le informazioni statistiche vengono visualizzate nei riquadri informazioni sotto forma di tabella o di grafico (a torta o a barre). I dati nei riquadri informazioni sono aggiornati mentre l'applicazione è in esecuzione e riflettono lo stato attuale dell'applicazione di protezione.

È possibile modificare il set di schede di secondo livello nella scheda **Statistiche**, il numero dei riquadri informazioni in ogni pagina a schede e la modalità di visualizzazione dei dati in tali riquadri.

*Per aggiungere una nuova scheda di secondo livello con i riquadri informazioni nella scheda **Statistiche**:*

1. Fare clic sul pulsante **Personalizza visualizzazione** nell'angolo superiore destro della scheda **Statistiche**.

   Verrà visualizzata la finestra delle proprietà delle statistiche. Questa finestra contiene un elenco di pagine a schede attualmente visualizzate nella scheda **Statistiche**. In questa finestra è possibile modificare l'ordine di visualizzazione delle pagine nella scheda, aggiungere e rimuovere pagine e procedere alla configurazione delle proprietà della pagina facendo clic sul pulsante **Proprietà**.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra delle proprietà di una nuova pagina.

3. Configurare la nuova pagina:

   - Nella sezione **Generale** specificare il nome della pagina.
   - Nella sezione **Riquadri informazioni** fare clic sul pulsante **Aggiungi** per aggiungere i riquadri informazioni che devono essere visualizzati nella pagina.

     Fare clic sul pulsante **Proprietà** nella sezione **Riquadri informazioni** per configurare le proprietà dei riquadri informazioni che sono stati aggiunti: nome, tipo e aspetto del grafico nel riquadro e i dati utilizzati per creare il grafico.

4. Fare clic su **OK**.

La pagina a schede con i riquadri informazioni aggiunti verrà visualizzata nella scheda **Statistiche**. Fare clic sull'icona delle impostazioni (⚙) per procedere immediatamente alla configurazione della pagina o di un riquadro informazioni selezionato nella pagina.

Configurazione delle notifiche degli eventi

Kaspersky Security Center consente di selezionare un metodo per la notifica all'amministratore degli eventi che si verificano nei dispositivi client e di configurare la notifica:

- E-mail. Quando si verifica un evento, l'applicazione invia una notifica agli indirizzi e-mail specificati. È possibile modificare il testo della notifica.
- SMS. Quando si verifica un evento, l'applicazione invia una notifica ai numeri di telefono specificati. È possibile configurare le notifiche SMS per l'invio tramite il gateway di posta.
- File eseguibile. Quando si verifica un evento in un dispositivo, il file eseguibile viene avviato nella workstation dell'amministratore. Utilizzando il file eseguibile, l'amministratore può ricevere i parametri di qualsiasi evento che si è verificato.

Per configurare le notifiche degli eventi che si verificano nei dispositivi client:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Fare clic sul collegamento **Configura notifiche ed esportazione eventi** e selezionare il valore **Configura notifiche** nell'elenco a discesa.

   Verrà visualizzata la finestra **Proprietà: Eventi**.

4. Nella sezione **Notifica** selezionare un metodo di notifica (via e-mail, SMS o attraverso un file eseguibile) e definire le impostazioni di notifica:

   - **E-mail**

La scheda **E-mail** consente di configurare le notifiche degli eventi tramite e-mail.

Nel campo **Destinatari (indirizzi e-mail)** specificare gli indirizzi e-mail a cui l'applicazione invierà le notifiche. È possibile specificare più indirizzi in questo campo, separandoli con punto e virgola.

Nel campo **Server SMTP** specificare gli indirizzi dei server di posta, separandoli con punto e virgola. È possibile utilizzare i seguenti valori:

- Indirizzo IPv4 o IPv6
- Nome di rete Windows (nome NetBIOS) del dispositivo
- Nome DNS del server SMTP

Nel campo **Porta server SMTP** specificare il numero di una porta di comunicazione del server SMTP. Il numero di porta predefinito è 25.

Se si abilita l'opzione **Usa ricerca DNS MX**, è possibile utilizzare più record MX degli indirizzi IP per lo stesso nome DNS del server SMTP. Lo stesso nome DNS può avere diversi record MX con valori di priorità differenti di ricezione dei messaggi e-mail. Administration Server tenta di inviare notifiche e-mail al server SMTP in ordine crescente di priorità dei record MX. Per impostazione predefinita, questa opzione è disabilitata.

Se si abilita l'opzione **Usa ricerca DNS MX** e non si abilita l'utilizzo delle impostazioni TLS, è consigliabile utilizzare le impostazioni DNSSEC nel dispositivo server come misura di protezione aggiuntiva per l'invio di notifiche e-mail.

Fare clic sul collegamento **Impostazioni** per definire impostazioni di notifica aggiuntive:

- Nome dell'oggetto (nome dell'oggetto di un messaggio e-mail)
- Indirizzo e-mail del mittente
- Impostazioni di autenticazione ESMTP

È necessario specificare un account per l'autenticazione in un server SMTP se l'opzione di autenticazione ESMTP è abilitata per il server SMTP.

- Impostazioni TLS per il server SMTP:
  - **Non utilizzare TLS**

    È possibile selezionare questa opzione se si desidera disabilitare il criptaggio dei messaggi e-mail.
  - **Usa TLS se supportato dal server SMTP**

    È possibile selezionare questa opzione se si desidera utilizzare una connessione TLS in un server SMTP. Se il server SMTP non supporta TLS, Administration Server si connette al server SMTP senza utilizzare TLS.
  - **Usa sempre TLS, controlla la validità del certificato del server**

    È possibile selezionare questa opzione se si desidera utilizzare le impostazioni di autenticazione TLS. Se il server SMTP non supporta TLS, Administration Server non può connettersi al server SMTP.

È consigliabile utilizzare questa opzione per una protezione più efficace della connessione con un server SMTP. Se si seleziona questa opzione, è possibile configurare le impostazioni di autenticazione per una connessione TLS.

Se si sceglie il valore **Usa sempre TLS, controlla la validità del certificato del server**, è possibile specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. È inoltre possibile specificare un certificato per l'autenticazione del client nel server SMTP.

È possibile specificare le impostazioni TLS per un server SMTP:

- Cercare un file di certificato del server SMTP:

È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Administration Server. Kaspersky Security Center verifica se anche il certificato di un server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center non può connettersi a un server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

- Cercare un file di certificato del client:

È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. È necessario specificare il certificato e la relativa chiave privata utilizzando uno dei seguenti tipi di certificato:

- Certificato X-509:

È necessario specificare un file con il certificato e un file con la chiave privata. Entrambi i file non dipendono l'uno dall'altro e l'ordine di caricamento dei file non è significativo. Quando entrambi i file vengono caricati, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

- Contenitore pkcs12:

È necessario caricare un singolo file che contenga il certificato e la relativa chiave privata. Quando il file viene caricato, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

Il campo **Messaggio di notifica** contiene testo standard con informazioni sull'evento inviate dall'applicazione quando si verifica un evento. Il testo include parametri sostitutivi, ad esempio il nome dell'evento, il nome del dispositivo e il nome di dominio. È possibile modificare il testo del messaggio aggiungendo altri parametri sostitutivi con dettagli più pertinenti dell'evento. L'elenco dei parametri sostitutivi è disponibile facendo clic sul pulsante a destra del campo.

Se il testo di notifica contiene un segno percentuale (%), è necessario digitarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

Fare clic sul collegamento **Configura un limite numerico per le notifiche** per specificare il numero massimo di notifiche che l'applicazione può inviare durante l'intervallo di tempo specificato.

Fare clic sul pulsante **Invia messaggio di test** per verificare se le notifiche sono state configurate correttamente. L'applicazione dovrebbe inviare una notifica di prova agli indirizzi e-mail specificati.

- SMS

La scheda **SMS** consente di configurare la trasmissione delle notifiche SMS di diversi eventi a un cellulare. I messaggi SMS vengono inviati tramite un gateway di posta.

Nel campo **Destinatari (indirizzi e-mail)** specificare gli indirizzi e-mail a cui l'applicazione invierà le notifiche. È possibile specificare più indirizzi in questo campo, separandoli con punto e virgola. Le notifiche verranno inviate ai numeri di telefono associati agli indirizzi e-mail specificati.

Nel campo **Server SMTP** specificare gli indirizzi dei server di posta, separandoli con punto e virgola. È possibile utilizzare i seguenti valori:

- Indirizzo IPv4 o IPv6
- Nome di rete Windows (nome NetBIOS) del dispositivo
- Nome DNS del server SMTP

Nel campo **Porta server SMTP** specificare il numero di una porta di comunicazione del server SMTP. Il numero di porta predefinito è 25.

Fare clic sul collegamento **Impostazioni** per definire impostazioni di notifica aggiuntive:

- Nome dell'oggetto (nome dell'oggetto di un messaggio e-mail)
- Indirizzo e-mail del mittente
- Impostazioni di autenticazione ESMTP

Se necessario, è possibile specificare un account per l'autenticazione in un server SMTP se l'opzione di autenticazione ESMTP è abilitata per il server SMTP.

- Impostazioni TLS per un server SMTP

È possibile disabilitare l'utilizzo di TLS, utilizzare TLS se il server SMTP supporta questo protocollo oppure forzare solo l'utilizzo di TLS. Se si sceglie di utilizzare solo TLS, è possibile specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. Inoltre, se si sceglie di utilizzare solo TLS, è possibile specificare un certificato per l'autenticazione client nel server SMTP.

- Cercare un file di certificato del server SMTP

È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Kaspersky Security Center. Kaspersky Security Center verifica se anche il certificato del server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center non può connettersi al server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

È necessario caricare un singolo file che contenga il certificato e la relativa chiave privata. Quando il file viene caricato, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata. Il campo **Messaggio di notifica** contiene testo standard con informazioni sull'evento che l'applicazione invia quando si verifica un evento. Il testo include parametri sostitutivi, ad esempio il nome dell'evento, il nome del dispositivo e il nome di dominio. È possibile modificare il testo del messaggio aggiungendo altri parametri sostitutivi con dettagli più pertinenti dell'evento. L'elenco dei parametri sostitutivi è disponibile facendo clic sul pulsante a destra del campo.

Se il testo di notifica contiene un segno percentuale (%), è necessario digitarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

Fare clic sul collegamento **Configura un limite numerico per le notifiche** per specificare il numero massimo di notifiche che l'applicazione può inviare nell'intervallo di tempo specificato.

Fare clic sul pulsante **Invia messaggio di prova** per verificare se le notifiche sono state configurate correttamente. L'applicazione dovrebbe inviare una notifica di prova al destinatario specificato.

- File eseguibile da avviare

Se è selezionato questo metodo di notifica, nel campo di immissione è possibile specificare l'applicazione che verrà avviata quando si verifica un evento.

Il collegamento **Configurare un limite numerico per la notifica** consente di specificare il numero massimo di notifiche che l'applicazione può inviare nell'intervallo di tempo specificato.

Il pulsante **Invia messaggio di prova** consente di verificare se le notifiche sono state configurate correttamente: l'applicazione invia una notifica di prova all'indirizzo e-mail specificato.

5. Nel campo **Messaggio di notifica** immettere il testo che l'applicazione invierà quando si verifica un evento.

   È possibile utilizzare l'elenco a discesa a destra del campo di testo per aggiungere impostazioni di sostituzione con dettagli sull'evento (ad esempio la descrizione dell'evento o l'ora in cui si è verificato).

   Se il testo di notifica contiene una percentuale (%), è necessario specificarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

6. Fare clic sul pulsante **Invia messaggio di test** per verificare se la notifica è stata configurata correttamente.

   L'applicazione invia una notifica test all'utente specificato.

7. Fare clic su **OK** per salvare le modifiche.

Le impostazioni di notifica modificate verranno applicate a tutti gli eventi che si verificano nei dispositivi client.

È possibile sostituire le impostazioni di notifica per determinati eventi nella sezione **Configurazione eventi** delle impostazioni di Administration Server, delle impostazioni di un criterio o delle impostazioni di un'applicazione.

Creazione di un certificato per un server SMTP

Per creare un certificato per un server SMTP:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Fare clic sul collegamento **Configura notifiche ed esportazione eventi** e selezionare il valore **Configura notifiche** nell'elenco a discesa.

   Verrà visualizzata la finestra delle proprietà dell'evento.

4. Nella scheda **E-mail** fare clic sul collegamento **Impostazioni** per aprire la finestra **Impostazioni**.
5. Nella finestra **Impostazioni** fare clic sul collegamento **Specifica certificato** per aprire la finestra **Certificato per la firma**.
6. Nella finestra **Certificato per la firma** fare clic sul pulsante **Sfoglia**.

   Verrà aperta la finestra **Certificato**.

7. Nell'elenco a discesa **Tipo di certificato** specificare il tipo di certificato, pubblico o privato:

   - Se è selezionato il tipo di certificato privato (**Contenitore PKCS #12**), specificare il file di certificato e la password.
   - Se è selezionato il tipo di certificato pubblico (**Certificato X.509**):

     a. Specificare il file della chiave privata (con l'estensione *.prk o *.pem).

     b. Specificare la password della chiave privata.

     c. Specificare il file della chiave pubblica (con l'estensione * cer).

8. Fare clic su **OK**.

Verrà emesso il certificato per il server SMTP.

Selezioni eventi

Le informazioni sugli eventi che si verificano durante l'esecuzione di Kaspersky Security Center e delle applicazioni gestite sono salvate sia nel database di Administration Server che nel registro di sistema di Microsoft Windows. È possibile visualizzare informazioni del database di Administration Server nell'area di lavoro del nodo **Administration Server**, nella scheda **Eventi**.

Le informazioni nella scheda **Eventi** sono rappresentate come un elenco di selezioni eventi. Ogni selezione include solo gli eventi di un determinato tipo. Ad esempio, la selezione "Lo stato del dispositivo è Critico" contiene solo i record relativi alle modifiche degli stati del dispositivo in "Critico". Dopo l'installazione dell'applicazione, la scheda **Eventi** contiene alcune selezioni eventi standard. È possibile creare selezioni eventi aggiuntive (personalizzate) o esportare in un file le informazioni sugli eventi.

Visualizzazione di una selezione eventi

Per visualizzare la selezione eventi:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Nell'elenco a discesa **Selezioni eventi** selezionare la selezione eventi desiderata.

   Se si desidera visualizzare sempre nell'area di lavoro gli eventi di questa selezione, fare clic sull'icona a forma di stella (☆) accanto alla selezione.

Nell'area di lavoro verrà visualizzato l'elenco degli eventi memorizzati in Administration Server del tipo selezionato.

È possibile ordinare le informazioni nell'elenco degli eventi, in ordine crescente o decrescente in ogni colonna.

Personalizzazione di una selezione eventi

Per personalizzare una selezione eventi:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Aprire la selezione eventi desiderata nella scheda **Eventi**.
4. Fare clic sul pulsante **Proprietà selezione**.

Nella finestra delle proprietà della selezione eventi visualizzata è possibile configurare la selezione eventi.

Creazione di una selezione eventi

Per creare una selezione eventi:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Fare clic sul pulsante **Crea selezione**.
4. Nella finestra **Nuova selezione eventi** visualizzata immettere il nome della nuova selezione, quindi fare clic su **OK**.

Una selezione con il nome specificato verrà creata nell'elenco a discesa **Selezioni eventi**.

Per impostazione predefinita, una selezione eventi creata contiene tutti gli eventi memorizzati in Administration Server. Per visualizzare solo gli eventi desiderati, è necessario personalizzare la selezione.

Esportazione di una selezione eventi in un file di testo

Per esportare una selezione eventi in un file di testo:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Fare clic sul pulsante **Importa/esporta**.
4. Nell'elenco a discesa selezionare **Esporta eventi in un file**.

Verrà avviata l'Esportazione guidata eventi. Seguire le istruzioni della procedura guidata.

Eliminazione di eventi da una selezione

Per eliminare gli eventi da una selezione:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Selezionare gli eventi da eliminare utilizzando il mouse, il tasto **MAIUSC** o il tasto **CTRL**.
4. Eliminare gli eventi selezionati in uno dei seguenti modi:
   - Selezionando **Elimina** nel menu di scelta rapida di uno degli eventi selezionati.

     Se si seleziona **Elimina tutto** dal menu di scelta rapida, tutti gli eventi visualizzati saranno eliminati dalla selezione, a prescindere dalla selezione eventi dell'utente.
   - Facendo clic sul collegamento **Elimina evento** (se è selezionato un solo evento) oppure sul collegamento **Elimina eventi** se sono selezionati più eventi nella finestra di informazioni di questi eventi.

Gli eventi selezionati vengono eliminati.

Aggiunta di applicazioni alle esclusioni in base alle richieste utente

Quando si ricevono richieste da parte degli utenti per lo sblocco di applicazioni bloccate per errore, è possibile creare un'esclusione dalle regole di Sicurezza adattiva per queste applicazioni. In tal modo, le applicazioni non verranno più bloccate nei dispositivi degli utenti. È possibile tenere traccia del numero di richieste utente nella scheda **Monitoraggio** di Administration Server.

Per aggiungere alle esclusioni le applicazioni bloccate da Kaspersky Endpoint Security in base alle richieste utente:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Eventi**.
3. Nell'elenco a discesa **Selezioni eventi** selezionare **Richieste utente**.
4. Fare clic con il pulsante destro del mouse su una o più richieste utente che contengono le applicazioni da aggiungere alle esclusioni e quindi scegliere **Aggiungi esclusione**.

   Verrà avviata l'Aggiunta guidata esclusioni. Seguire le istruzioni visualizzate.

Le applicazioni selezionate verranno escluse dall'elenco **Attivazioni di regole nello stato Smart Training** (in **Archivi** nella struttura della console) dopo la successiva sincronizzazione del dispositivo client con Administration Server e non saranno più visualizzate nell'elenco.

Selezioni dispositivi

Le informazioni sullo stato dei dispositivi sono visualizzate nella cartella **Selezioni dispositivi** nella struttura della console.

Le informazioni nella cartella **Selezioni dispositivi** sono visualizzate come un elenco di selezioni dispositivi. Ogni selezione contiene i dispositivi che soddisfano specifiche condizioni. Ad esempio, la selezione **Dispositivi con stato Critico** contiene solo i dispositivi con lo stato *Critico*. Dopo l'installazione dell'applicazione, la cartella **Selezioni dispositivi** contiene alcune selezioni standard. È possibile creare selezioni dispositivi (personalizzate) aggiuntive, esportare le impostazioni di selezione in un file o creare selezioni con impostazioni importate da un altro file.

Visualizzazione di una selezione dispositivi

Per visualizzare una selezione dispositivi:

1. Nella struttura della console selezionare la cartella **Selezioni dispositivi**.
2. Nell'area di lavoro della cartella, nell'elenco **Dispositivi in questa selezione**, selezionare la selezione dispositivi attinente.
3. Fare clic sul pulsante **Esegui selezione**.
4. Fare clic sulla scheda **Risultati selezione**.

Nell'area di lavoro verrà visualizzato un elenco dei dispositivi che soddisfano i criteri di selezione.

È possibile ordinare le informazioni nell'elenco dei dispositivi, in ordine crescente o decrescente, in ogni colonna.

Configurazione di una selezione dispositivi

Per configurare una selezione dispositivi:

1. Nella struttura della console selezionare la cartella **Selezioni dispositivi**.
2. Nell'area di lavoro fare clic sulla scheda **Selezione** e quindi scegliere la selezione dispositivi desiderata nell'elenco delle selezioni utente.
3. Fare clic sul pulsante **Proprietà selezione**.
4. Nella finestra delle proprietà visualizzata specificare le seguenti impostazioni:
   - Proprietà generali della selezione.
   - Condizioni da soddisfare per l'inclusione dei dispositivi nella selezione. Per configurare le condizioni, selezionare il nome di una condizione e fare clic sul pulsante **Proprietà**.
   - Impostazioni della protezione.
5. Fare clic su **OK**.

   Le impostazioni verranno applicate e salvate.

Di seguito sono descritte le condizioni per l'assegnazione dei dispositivi a una selezione. Le condizioni vengono combinate tramite l'operatore logico OR: la selezione conterrà i dispositivi conformi ad almeno una delle condizioni elencate.

Generale

Nella sezione **Generale** è possibile modificare il nome della condizione di selezione e specificare se tale condizione deve essere invertita:

Inverti condizione selezione

Per impostazione predefinita, questa opzione è disabilitata.

Se si abilita questa opzione, la condizione di selezione specificata verrà invertita. La selezione includerà tutti i dispositivi che non soddisfano la condizione.

L'esempio seguente mostra la logica del lavoro di inversione:

- **Condizione**: nel dispositivo è presente un sistema operativo con il tipo Linux e il numero di build 00.0.000.
- **Condizione invertita**: nel dispositivo è presente un sistema operativo con NOT (il tipo Linux e il numero di build 00.0.000), che equivale a quanto segue:

  È presente un sistema operativo con il tipo NOT Linux OR numero di build NOT 00.0. 000.

Pertanto, la selezione includerà i dispositivi con un sistema operativo, ad esempio di tipo Windows e numero di build 00.0.000, o di tipo Linux e qualsiasi numero di build diverso da 00.0.000.

Rete

Nella sezione **Rete** è possibile specificare i criteri che verranno utilizzati per includere i dispositivi nella selezione in base ai dati della rete:

- **Nome o indirizzo IP dispositivo**

  Nome di rete Windows (nome NetBIOS) del dispositivo o indirizzo IPv4 o IPv6.

- **Dominio Windows**

  Visualizza tutti i dispositivi inclusi nel dominio Windows specificato.

- **Gruppo di amministrazione**

  Visualizza i dispositivi inclusi nel gruppo di amministrazione specificato.

- **Descrizione**

  Testo contenuto nella finestra delle proprietà del dispositivo: nel campo **Descrizione** della sezione **Generale**.

  Per inserire il testo nel campo **Descrizione**, è possibile utilizzare i seguenti caratteri:

  - All'interno di una parola:

    - *****. Sostituisce qualsiasi stringa con qualsiasi numero di caratteri.

    Esempio:

    Per descrivere parole come **Server** o **Server's**, è possibile immettere **Server***.

    - **?.** Sostituisce qualsiasi carattere singolo.

    Esempio:

    Per descrivere parole come **Finestra** o **Finestre**, è possibile immettere **Finestr?**.

    Non è possibile utilizzare l'asterisco (*****) o il punto interrogativo (**?**) come primo carattere nella query.

  - Per trovare più parole:

    - Spazio. Visualizza tutti i dispositivi le cui descrizioni contengono una delle parole elencate.

    Esempio:

    Per trovare una frase contenente le parole **Secondario** o **Virtuale**, è possibile includere la riga **Secondario Virtuale** nella query.

    - **+**. Quando una parola è preceduta dal segno +, tutti i risultati della ricerca conterranno tale parola.

    Esempio:

    Per trovare una frase contenente sia **Secondario** che **Virtuale**, immettere la query **+Secondario+Virtuale**.

    - **-**. Quando una parola è preceduta dal segno -, nessun risultato della ricerca conterrà tale parola.

    Esempio:

    Per trovare una frase contenente **Secondario** e non contenente **Virtuale**, immettere la query **+Secondario-Virtuale**.

    - **"<testo>"**. Verranno visualizzati i risultati che contengono il testo racchiuso tra virgolette.

    Esempio:

    Per trovare una frase contenente la combinazione di parole **Server secondario**, è possibile immettere **"Server secondario"** nella query.

- **Intervallo IP**

  Se questa opzione è abilitata, è possibile immettere gli indirizzi IP iniziale e finale dell'intervallo IP in cui i dispositivi rilevanti devono essere inclusi.

  Per impostazione predefinita, questa opzione è disabilitata.

Tag

Nella sezione **Tag** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base alle parole chiave (tag) che sono state aggiunte in precedenza alle descrizioni dei dispositivi gestiti:

- **Applica se almeno uno dei tag specificati corrisponde**

  Se questa opzione è abilitata, i risultati di ricerca visualizzeranno i dispositivi con descrizioni contenenti almeno uno dei tag selezionati.

  Se questa opzione è disabilitata, i risultati di ricerca visualizzeranno solo i dispositivi con descrizioni contenenti tutti i tag selezionati.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Il tag deve essere incluso**

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

  Per impostazione predefinita, questa opzione è selezionata.

- **Il tag deve essere escluso**

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni non contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

Active Directory

Nella sezione **Active Directory** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base ai dati di Active Directory:

- **Il dispositivo si trova in un'unità organizzativa di Active Directory**

  Se questa opzione è abilitata, la selezione includerà i dispositivi dell'unità organizzativa Active Directory specificata nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Includi unità organizzative secondarie**

  Se questa opzione è abilitata, la selezione includerà i dispositivi in tutte le unità organizzative secondarie dell'unità organizzativa del dominio specificato.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Il dispositivo fa parte di un gruppo di Active Directory**

  Se questa opzione è abilitata, la selezione includerà i dispositivi del gruppo Active Directory specificato nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

Attività di rete

Nella sezione **Attività di rete** è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base alle relative attività della rete:

- **Il dispositivo è un punto di distribuzione**

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione include i dispositivi che operano come punti di distribuzione.
  - **No**. I dispositivi che operano come punti di distribuzione non sono inclusi nella selezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- **Non eseguire la disconnessione da Administration Server**

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Abilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è selezionata.
  - **Disabilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è deselezionata.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- **Profilo connessione cambiato**

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **No**. La selezione non includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- **Ultima connessione ad Administration Server**

  È possibile utilizzare questa casella di controllo per impostare un criterio di ricerca per i dispositivi in base all'ora dell'ultima connessione ad Administration Server.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stata stabilita l'ultima connessione tra Network Agent installato nel dispositivo client e Administration Server. La selezione includerà i dispositivi che rientrano nell'intervallo specificato.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Rilevati nuovi dispositivi durante il polling della rete

  Cerca nuovi dispositivi rilevati dal polling della rete negli ultimi giorni.

  Se questa opzione è abilitata, la selezione includerà soltanto i nuovi dispositivi rilevati dalla device discovery nel numero di giorni specificato nel campo **Periodo di rilevamento (giorni)**.

  Se questa opzione è disabilitata, la selezione includerà tutti i dispositivi rilevati dalla device discovery.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il dispositivo è visibile

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. L'applicazione include nella selezione i dispositivi attualmente visibili nella rete.
  - **No**. L'applicazione include nella selezione i dispositivi attualmente invisibili nella rete.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Applicazione

Nella sezione **Applicazione** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'applicazione gestita selezionata:

- Nome applicazione

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome di un'applicazione Kaspersky.

  L'elenco contiene solo i nomi delle applicazioni con plug-in di gestione installati nella workstation dell'amministratore.

  Se non è selezionata alcuna applicazione, il criterio non verrà applicato.

- Versione applicazione

  Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al numero versione di un'applicazione Kaspersky.

  Se non è specificato alcun numero di versione, il criterio non verrà applicato.

- Nome aggiornamento critico

  Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome dell'applicazione o al numero del pacchetto di aggiornamento.

  Se il campo è vuoto, il criterio non verrà applicato.

- Ultimo aggiornamento dei moduli

  È possibile utilizzare questa opzione per impostare un criterio per la ricerca dei dispositivi in base all'ora dell'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stato eseguito l'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Il dispositivo è gestito tramite Kaspersky Security Center

  Nell'elenco a discesa è possibile includere nella selezione i dispositivi gestiti tramite Kaspersky Security Center:

  - **Sì**. L'applicazione include nella selezione i dispositivi gestiti tramite Kaspersky Security Center.
  - **No**. L'applicazione include nella selezione i dispositivi non gestiti tramite Kaspersky Security Center.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- L'applicazione di protezione è installata

  Nell'elenco a discesa è possibile includere nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione:

  - **Sì**. L'applicazione include nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione.
  - **No**. L'applicazione include nella selezione tutti i dispositivi in cui non è installata un'applicazione di protezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Sistema operativo

Nella sezione **Sistema operativo** è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base al tipo di sistema operativo.

- Versione del sistema operativo

  Se la casella di controllo è selezionata, è possibile selezionare un sistema operativo dall'elenco. I dispositivi in cui sono installati i sistemi operativi specificati saranno inclusi nei risultati della ricerca.

- Dimensioni in bit del sistema operativo

  Nell'elenco a discesa è possibile selezionare l'architettura del sistema operativo da cui dipenderà l'applicazione della regola di spostamento al dispositivo (**Sconosciuto**, **x86**, **AMD64** o **IA64**). Per impostazione predefinita, non è selezionata alcuna opzione nell'elenco, pertanto l'architettura del sistema operativo non è definita.

- **Versione Service Pack del sistema operativo**

  In questo campo è possibile specificare la versione del pacchetto del sistema operativo (nel formato *X.Y*), da cui dipenderà l'applicazione della regola di spostamento al dispositivo. Per impostazione predefinita, non è specificato alcun valore per la versione.

- **Build del sistema operativo**

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Numero di build del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un numero di build uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti i numeri di build ad eccezione di quello specificato.

- **ID di rilascio del sistema operativo**

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Identificatore della versione (ID) del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un ID di rilascio uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti gli ID di rilascio ad eccezione di quello specificato.

Stato dispositivo

Nella sezione **Stato dispositivo** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base alla descrizione dello stato dei dispositivi ottenuta da un'applicazione gestita:

- **Stato dispositivo**

  Elenco a discesa in cui è possibile selezionare uno degli stati del dispositivo: *OK*, *Critico* o *Avviso*.

- **Descrizione stato del dispositivo**

  In questo campo è possibile selezionare le caselle di controllo accanto alle condizioni che, se soddisfatte, assegnano al dispositivo uno dei seguenti stati: *OK*, *Critico* o *Avviso*.

- **Stato dispositivo definito dall'applicazione**

  Elenco a discesa in cui è possibile selezionare lo stato della protezione in tempo reale. I dispositivi con lo stato della protezione in tempo reale specificato vengono inclusi nella selezione.

Componenti della protezione

Nella sezione **Componenti della protezione** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base allo stato della protezione:

- **Data rilascio database**

  Se questa opzione è selezionata, è possibile eseguire la ricerca dei dispositivi client in base alla data di rilascio del database anti-virus. Nei campi di immissione è possibile impostare l'intervallo di tempo in base al quale eseguire la ricerca.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Ultima scansione**

  Se questa opzione è abilitata, è possibile eseguire la ricerca dei dispositivi client in base all'ora dell'ultima scansione malware. Nei campi di immissione è possibile specificare il periodo di tempo entro il quale è stata eseguita l'ultima scansione malware.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Numero totale di minacce rilevate**

  Se questa opzione è abilitata, è possibile eseguire la ricerca di dispositivi client in base al numero di virus rilevati. Nei campi di immissione è possibile impostare i valori di soglia inferiore e superiore per il numero di virus trovati.

  Per impostazione predefinita, questa opzione è disabilitata.

Registro delle applicazioni

Nella sezione **Registro delle applicazioni** è possibile impostare i criteri di ricerca dei dispositivi in base alle applicazioni installate:

- **Nome applicazione**

  Elenco a discesa da cui è possibile selezionare un'applicazione. I dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- **Versione applicazione**

  Campo di immissione in cui è possibile specificare la versione dell'applicazione selezionata.

- **Fornitore**

  Elenco a discesa da cui è possibile selezionare il produttore di un'applicazione installata nel dispositivo.

- **Stato applicazione**

  Elenco a discesa da cui è possibile selezionare lo stato di un'applicazione (*Installata*, *Non installata*). Verranno inclusi nella selezione i dispositivi in cui è installata o non è installata l'applicazione specificata, in base allo stato selezionato.

- **Trova per aggiornamento**

  Se questa opzione è abilitata, la ricerca verrà eseguita utilizzando i dettagli degli aggiornamenti per le applicazioni installate nei dispositivi. Dopo aver selezionato la casella di controllo, i campi **Nome applicazione**, **Versione applicazione** e **Stato applicazione** diventano rispettivamente **Nome aggiornamento**, **Versione aggiornamento** e **Stato**.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Nome applicazione di protezione incompatibile**

  Elenco a discesa da cui è possibile selezionare applicazioni di protezione di terze parti. Durante la ricerca, i dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- **Tag applicazione**

  Nell'elenco a discesa è possibile selezionare il tag di un'applicazione. Tutti i dispositivi che hanno applicazioni installate con il tag selezionato nella descrizione sono inclusi nella selezione dispositivi.

- **Applica ai dispositivi senza i tag specificati**

  Se questa opzione è abilitata, la selezione includerà i dispositivi con descrizioni che non contengono alcuno dei tag selezionati.

  Se questa opzione è disabilitata, il criterio non viene applicato.

  Per impostazione predefinita, questa opzione è disabilitata.

Registro hardware

Nella sezione **Registro hardware** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'hardware installato:

- **Dispositivo**

  Nell'elenco a discesa è possibile selezionare un tipo di unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- **Fornitore**

  Nell'elenco a discesa è possibile selezionare il nome di un produttore dell'unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- **Nome dispositivo**

  Nome del dispositivo nella rete Windows. Il dispositivo con il nome specificato verrà incluso nella selezione.

- **Descrizione**

  Descrizione del dispositivo o dell'unità hardware. I dispositivi con la descrizione specificata in questo campo verranno inclusi nella selezione.

  La descrizione di un dispositivo in qualsiasi formato può essere immessa nella finestra delle proprietà del dispositivo. Il campo supporta la ricerca full-text.

- **Produttore dispositivo**

  Nome del produttore del dispositivo. I dispositivi del produttore specificato in questo campo verranno inclusi nella selezione.

  È possibile inserire il nome del produttore nella finestra delle proprietà di un dispositivo.

- **Numero di serie**

  Tutte le unità hardware con il numero di serie specificato in questo campo verranno incluse nella selezione.

- **Numero di inventario**

  L'apparecchiatura con il numero di inventario specificato in questo campo verrà inclusa nella selezione.

- **Utente**

  Tutte le unità hardware dell'utente specificato in questo campo verranno incluse nella selezione.

- **Posizione**

  Posizione del dispositivo o dell'unità hardware (ad esempio nella sede principale o in una filiale). I computer o gli altri dispositivi distribuiti al percorso specificato in questo campo verranno inclusi nella selezione.

  È possibile descrivere il percorso di un dispositivo in qualsiasi formato nella finestra delle proprietà del dispositivo.

- **Frequenza CPU (MHz)**

  L'intervallo di frequenze di una CPU. I dispositivi con CPU corrispondenti all'intervallo di frequenze in questi campi (compresi) verranno inclusi nella selezione.

- **Core CPU virtuali**

  Intervallo del numero di core virtuali in una CPU. I dispositivi con CPU corrispondenti all'intervallo in questi campi (compresi) verranno inclusi nella selezione.

- **Volume disco rigido (GB)**

  Intervallo di valori per le dimensioni del disco rigido nel dispositivo. I dispositivi con dischi rigidi corrispondenti all'intervallo in questi campi di immissione (compresi) verranno inclusi nella selezione.

- **Dimensione RAM (MB)**

  Intervallo di valori per le dimensioni della RAM del dispositivo. I dispositivi con RAM corrispondenti all'intervallo presente in questi campi di immissione (compresi i valori specificati) verranno inclusi nella selezione.

Macchine virtuali

Nella sezione **Macchine virtuali** è possibile configurare i criteri per l'inclusione dei dispositivi nella selezione in base al fatto che siano macchine virtuali o che facciano parte di Microsoft Virtual Desktop Infrastructure (VDI):

- Questa è una macchina virtuale

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Non importante**.
  - **No**. I dispositivi che non sono macchine virtuali vengono trovati.
  - **Sì**. Vengono trovati i dispositivi che sono macchine virtuali.

- Tipo di macchina virtuale

  Nell'elenco a discesa è possibile selezionare il produttore della macchina virtuale.

  Questo elenco a discesa è disponibile se è selezionato il valore **Sì** o **Non importante** nell'elenco a discesa **Questa è una macchina virtuale**.

- Parte di Virtual Desktop Infrastructure

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Non importante**.
  - **No**. Vengono trovati i dispositivi che non fanno parte di Virtual Desktop Infrastructure.
  - **Sì**. Vengono trovati i dispositivi che fanno parte di Microsoft Virtual Desktop Infrastructure (VDI).

Vulnerabilità e aggiornamenti

Nella sezione **Vulnerabilità e aggiornamenti** è possibile specificare i criteri per l'inclusione dei dispositivi nella selezione in base all'origine di Windows Update:

WUA è passato ad Administration Server

È possibile selezionare una delle seguenti opzioni di ricerca nell'elenco a discesa:

- **Sì**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da Administration Server.
- **No**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da altre origini.

Utenti

Nella sezione **Utenti** è possibile impostare i criteri per l'inclusione dei dispositivi nella selezione in base agli account degli utenti che hanno eseguito l'accesso al sistema operativo.

- **Ultimo utente che ha eseguito l'accesso al sistema**

  Se questa opzione è abilitata, fare clic sul pulsante **Sfoglia** per specificare un account utente. I risultati della ricerca includeranno i dispositivi in cui l'utente specificato ha eseguito l'ultimo accesso al sistema.

- **Utente che ha eseguito l'accesso al sistema almeno una volta**

  Se questa opzione è abilitata, fare clic sul pulsante **Sfoglia** per specificare un account utente. I risultati della ricerca includeranno i dispositivi in cui l'utente specificato ha eseguito l'accesso al sistema almeno una volta.

Problemi che influiscono sullo stato nelle applicazioni gestite

Nella sezione **Problemi che influiscono sullo stato nelle applicazioni gestite** è possibile specificare i criteri per l'inclusione dei dispositivi nella selezione in base all'elenco dei possibili problemi rilevati da un'applicazione gestita. Se è presente almeno un problema selezionato in un dispositivo, il dispositivo verrà incluso nella selezione. Quando si seleziona un problema elencato per diverse applicazioni, è possibile selezionare automaticamente questo problema in tutti gli elenchi.

Descrizione stato del dispositivo

È possibile selezionare le caselle di controllo relative alle descrizioni degli stati dall'applicazione gestita. Alla ricezione di questi stati, i dispositivi verranno inclusi nella selezione. Quando si seleziona uno stato elencato per diverse applicazioni, è possibile selezionare automaticamente questo stato in tutti gli elenchi.

Stati dei componenti nelle applicazioni gestite

Nella sezione **Stati dei componenti nelle applicazioni gestite** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base agli stati dei componenti nelle applicazioni gestite:

- **Stato prevenzione fughe di dati**

  Cercare i dispositivi in base allo stato di prevenzione della perdita dei dati (*Sconosciuto, Arrestata, Avvio in corso, Sospesa, In esecuzione, Non riuscito*).

- **Stato protezione server di collaborazione**

  Cercare i dispositivi in base allo stato della protezione della collaborazione server (*Sconosciuto*, *Arrestata*, *Avvio in corso, Sospesa*, *In esecuzione*, *Non riuscito*).

- **Stato protezione anti-virus server di posta**

  Cercare i dispositivi in base allo stato della protezione dei server di posta (*Sconosciuto, Arrestata, Avvio in corso, Sospesa, In esecuzione, Non riuscito*).

- **Stato Endpoint Sensor**

  Cercare i dispositivi in base allo stato del componente Sensore Endpoint (*Sconosciuto, Arrestata, Avvio in corso, Sospesa, In esecuzione, Non riuscito*).

Criptaggio

Algoritmo di criptaggio

Algoritmo di cifratura a blocchi AES (Advanced Encryption Standard). Nell'elenco a discesa è possibile selezionare le dimensioni della chiave di criptaggio (56 bit, 128 bit, 192 bit o 256 bit).

Valori disponibili: *AES56*, *AES128*, *AES192* e *AES256*.

Segmenti cloud

Nella sezione **Segmenti cloud** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base ai rispettivi segmenti cloud:

- **Il dispositivo si trova in un segmento cloud**

  Se questa opzione è abilitata, è possibile fare clic sul pulsante **Sfoglia** per specificare il segmento in cui eseguire la ricerca.

  Se anche l'opzione **Includi gli oggetti figlio** è abilitata, la ricerca viene eseguita in tutti gli oggetti figlio del segmento specificato.

  I risultati di ricerca includono solo i dispositivi del segmento selezionato.

- **Dispositivo rilevato tramite l'API**

  Nell'elenco a discesa, è possibile selezionare se un dispositivo deve essere rilevato o meno dagli strumenti API:

  - **AWS**. Il dispositivo viene rilevato tramite l'API AWS, quindi si trova senz'altro nell'ambiente cloud AWS.
  - **Azure**. Il dispositivo viene rilevato tramite l'API Azure, quindi si trova senz'altro nell'ambiente cloud Azure.
  - **Google Cloud.** Il dispositivo viene rilevato tramite l'API Google, quindi si trova senz'altro nell'ambiente cloud Google.
  - **No**. Il dispositivo non può essere rilevato tramite l'API AWS, Azure o Google, ad esempio perché si trova all'esterno dell'ambiente cloud oppure si trova nell'ambiente cloud ma non può essere rilevato tramite un'API.
  - **Nessun valore**. Questa condizione non viene applicata.

Componenti dell'applicazione

Questa sezione contiene un elenco dei componenti delle applicazioni per cui sono installati plug-in di gestione corrispondenti in Administration Console.

Nella sezione **Componenti dell'applicazione** è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base agli stati e ai numeri di versione dei componenti che fanno riferimento all'applicazione selezionata:

- **Stato**

  Ricerca dei dispositivi in base allo stato dei componenti inviato da un'applicazione all'Administration Server. È possibile selezionare uno dei seguenti stati: *Nessun dato dal dispositivo*, *Arrestato*, *Avvio in corso*, *Sospeso*, *In esecuzione*, *Malfunzionamento* o *Non installato*. Se il componente selezionato dell'applicazione installata in un dispositivo gestito presenta lo stato specificato, il dispositivo viene incluso nella selezione dispositivi.

  Stati inviati dalle applicazioni:

  - *Avvio in corso* - Il componente è attualmente in fase di inizializzazione.
  - *In esecuzione* - Il componente è abilitato e correttamente in esecuzione.
  - *Sospeso* - Il componente è sospeso, ad esempio dopo che l'utente ha sospeso la protezione nell'applicazione gestita.
  - *Malfunzionamento* - Si è verificato un errore durante l'esecuzione del componente.
  - *Arrestato* - Il componente è disabilitato e al momento non è in esecuzione.
  - *Non installato* - L'utente non ha selezionato il componente per l'installazione durante la configurazione dell'installazione personalizzata dell'applicazione.

  A differenza degli altri stati, lo stato *Nessun dato dal dispositivo* non viene inviato dalle applicazioni. Questa opzione indica che le applicazioni non dispongono di alcuna informazione sullo stato del componente selezionato. Ciò può ad esempio verificarsi quando il componente selezionato non appartiene ad alcuna delle applicazioni installate nel dispositivo o quando il dispositivo è spento.

- **Versione**

  Ricerca dei dispositivi in base al numero di versione del componente selezionato nell'elenco. È possibile digitare un numero di versione, ad esempio `3.4.1.0`, e quindi specificare se il componente selezionato deve avere una versione uguale, precedente o successiva. È anche possibile configurare la ricerca di tutte le versioni ad eccezione di quella specificata.

Esportazione delle impostazioni di una selezione dispositivi in un file

Per esportare le impostazioni di una selezione dispositivi in un file di testo:

1. Nella struttura della console selezionare la cartella **Selezioni dispositivi**.
2. Nella scheda **Selezione** dell'area di lavoro fare clic sulla selezione dispositivi desiderata nell'elenco delle selezioni utente.

   Le impostazioni possono essere esportate solo dalle selezioni dispositivi create da un utente.

3. Fare clic sul pulsante **Esegui selezione**.

4. Nella scheda **Risultati selezione** fare clic sul pulsante **Esporta impostazioni**.

5. Nella finestra **Salva con nome** visualizzata specificare un nome per il file di esportazione delle impostazioni della selezione, selezionare una cartella in cui salvarlo, quindi fare clic sul pulsante **Salva**.

Le impostazioni della selezione dispositivi verranno salvate nel file specificato.

Creazione di una selezione dispositivi

Per creare una selezione dispositivi:

1. Nella struttura della console selezionare la cartella **Selezioni dispositivi**.

2. Nell'area di lavoro della cartella fare clic su **Avanzate** e selezionare **Crea selezione** nell'elenco a discesa.

3. Nella finestra **Nuova selezione dispositivi** visualizzata immettere il nome della nuova selezione, quindi fare clic su **OK**.

Nella struttura della console, nella cartella **Selezioni dispositivi**, verrà visualizzata una nuova cartella con il nome immesso. Per impostazione predefinita, la nuova selezione dispositivi comprende tutti i dispositivi inclusi nei gruppi di amministrazione dell'Administration Server su cui è stata creata la selezione. Per fare in modo che una selezione visualizzi solo i dispositivi che interessano l'utente nello specifico, configurare la selezione facendo clic sul pulsante **Proprietà selezione**.

Creazione di una selezione dispositivi in base a impostazioni importate

Per creare una selezione dispositivi in base a impostazioni importate:

1. Nella struttura della console selezionare la cartella **Selezioni dispositivi**.

2. Nell'area di lavoro della cartella fare clic sul pulsante **Avanzate** e selezionare **Importa selezione da file** nell'elenco a discesa.

3. Nella finestra visualizzata specificare il percorso del file da cui importare le impostazioni di selezione. Fare clic sul pulsante **Apri**.

Viene creata una voce **Nuova selezione** nella cartella **Selezioni dispositivi**. Le impostazioni della nuova selezione vengono importate dal file specificato.

Se una selezione denominata **Nuova selezione** è già presente nella cartella **Selezioni dispositivi**, al nome della selezione creata viene aggiunto un indice nel formato **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Rimozione di dispositivi dai gruppi di amministrazione in una selezione

Durante l'utilizzo di una selezione dispositivi, è possibile rimuovere i dispositivi dai gruppi di amministrazione in questa selezione senza passare ai gruppi di amministrazione da cui devono essere rimossi i dispositivi.

Per rimuovere dispositivi dai gruppi di amministrazione:

1. Nella struttura della console selezionare la cartella **Selezioni dispositivi**.
2. Selezionare i dispositivi da rimuovere utilizzando i tasti **MAIUSC** o **CTRL**.
3. Rimuovere i dispositivi selezionati dai gruppi di amministrazione in uno dei seguenti modi:
   - Selezionare **Elimina** nel menu di scelta rapida dei dispositivi selezionati.
   - Fare clic sul pulsante **Esegui azione** e selezionando **Rimuovi dal gruppo** nell'elenco a discesa.

I dispositivi selezionati verranno rimossi dai gruppi di amministrazione corrispondenti.

Monitoraggio dell'installazione e della disinstallazione delle applicazioni

È possibile monitorare l'installazione e la disinstallazione di applicazioni specifiche nei dispositivi gestiti, ad esempio un browser specifico. Per utilizzare questa funzionalità, è possibile aggiungere applicazioni dal registro delle applicazioni all'elenco delle applicazioni monitorate. Quando un'applicazione monitorata viene installata o disinstallata, Network Agent pubblica i rispettivi eventi: **Applicazione monitorata installata** o **Applicazione monitorata rimossa**. È possibile monitorare questi eventi utilizzando, ad esempio, selezioni eventi o rapporti.

È possibile monitorare questi eventi solo se sono archiviati nel database di Administration Server.

Per aggiungere un'applicazione all'elenco delle applicazioni monitorate:

1. Nella cartella **Avanzate** → **Gestione applicazioni** della struttura della console selezionare la sottocartella **Registro delle applicazioni**.
2. Sopra l'elenco delle applicazioni visualizzato, fare clic sul pulsante **Mostra la finestra delle proprietà del registro delle applicazioni**.
3. Nella finestra **Applicazioni monitorate** visualizzata fare clic sul pulsante **Aggiungi**.
4. Nella finestra **Seleziona nome applicazione** visualizzata selezionare le applicazioni dal registro delle applicazioni per cui si desidera monitorare l'installazione o la disinstallazione.
5. Nella finestra **Seleziona nome applicazione** fare clic sul pulsante **OK**.

In seguito alla configurazione dell'elenco delle applicazioni monitorate e all'installazione o disinstallazione di un'applicazione monitorata nei dispositivi gestiti dell'organizzazione, è possibile monitorare i rispettivi eventi, ad esempio utilizzando la selezione eventi Eventi recenti.

Eventi dei componenti di Kaspersky Security Center

Ogni componente Kaspersky Security Center dispone di uno specifico set di tipi di eventi. Questa sezione elenca i tipi di eventi che si verificano in Kaspersky Security Center Administration Server, Network Agent e iOS MDM Server. I tipi di eventi che si verificano nelle applicazioni Kaspersky non sono elencati in questa sezione.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Struttura dei dati della descrizione del tipo di evento

Per ogni tipo di evento, sono indicati il relativo nome visualizzato, l'identificatore (ID), il codice alfabetico, la descrizione e il periodo di archiviazione predefinito.

- **Nome visualizzato del tipo di evento**. Questo testo è visualizzato in Kaspersky Security Center durante la configurazione degli eventi e quando gli eventi si verificano.
- **ID del tipo di evento**. Questo codice numerico viene utilizzato durante l'elaborazione degli eventi tramite strumenti di terzi per l'analisi degli eventi.
- **Tipo di evento** (codice alfabetico). Questo codice viene utilizzato quando si esplorano e si elaborano gli eventi con le visualizzazione pubbliche disponibili nel database di Kaspersky Security Center e quando gli eventi vengono esportati in un sistema SIEM.
- **Descrizione**. Questo testo contiene le situazioni in cui si verifica un evento e come procedere in questo caso.
- **Periodo di archiviazione predefinito**. Rappresenta il numero di giorni per cui l'evento viene memorizzato nel database di Administration Server ed è visualizzato nell'elenco degli eventi in Administration Server. Al termine di questo periodo, l'evento viene eliminato. Se il valore per il periodo di archiviazione degli eventi è 0, gli eventi vengono rilevati ma non sono visualizzati nell'elenco degli eventi in Administration Server. Se è stato configurato il salvataggio di tali eventi nel registro eventi del sistema operativo, è possibile accedervi in tale posizione.

  È possibile modificare il periodo di archiviazione per gli eventi:

  - Administration Console: Impostazione del periodo di archiviazione per un evento
  - Kaspersky Security Center Web Console: Impostazione del periodo di archiviazione per un evento

Tra gli altri dati possono essere inclusi i seguenti campi:

- **event_id**: numero univoco dell'evento nel database, generato e assegnato automaticamente; da non confondere con l'**ID del tipo di evento**.
- **task_id**: l'ID dell'attività che ha causato l'evento (se presente)
- **criticità**: uno dei seguenti livelli di criticità (in ordine di criticità crescente):

  0) Livello di criticità non valido

  1) Informazioni

  2) Avviso

  3) Errore

  4) Critico

Eventi di Administration Server

Questa sezione contiene informazioni sugli eventi relativi ad Administration Server.

Eventi critici di Administration Server

La tabella seguente elenca i tipi di eventi di Kaspersky Security Center Administration Server con il livello di importanza **Critico**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Se è stata specificata la porta nella finestra delle proprietà di Administration Server in Administration Console, **Kaspersky Security Center pubblica le metriche** e gli eventi critici che devono essere ottenuti da Prometheus, un sistema per il monitoraggio e gli avvisi. Prometheus ottiene le metriche e gli eventi critici, quindi genera avvisi per ciascun evento.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
È stato superato il limite di licenze	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Una volta al giorno Kaspersky Security Center verifica se è stato superato un limite di licenze. Gli eventi di questo tipo si verificano quando Administration Server rileva il superamento di alcune limitazioni di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client e se il numero delle unità di licensing attualmente utilizzate coperte da una singola licenza supera il 110% del numero totale di unità coperte dalla licenza. Anche quando si verifica questo evento, i dispositivi client sono protetti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare i dispositivi non in uso. • Fornire una licenza per più dispositivi (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). Kaspersky Security Center determina le regole per generare gli eventi quando viene superato un limite di licenze.	180 giorni
Epidemia di virus	26 (per Protezione minacce file)	GNRL_EV_VIRUS_OUTBREAK	Gli eventi di questo tipo si verificano quando il numero di oggetti dannosi rilevati in più dispositivi gestiti supera il limite in un periodo limitato. È possibile rispondere all'evento nei seguenti modi: • Configurare la soglia nelle proprietà di Administration Server. • Creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.	180 giorni
Epidemia di virus	27 (per Protezione minacce di posta)	GNRL_EV_VIRUS_OUTBREAK	Gli eventi di questo tipo si verificano quando il numero di oggetti dannosi rilevati in più dispositivi gestiti supera il limite in un periodo limitato. È possibile rispondere all'evento nei seguenti modi: • Configurare la soglia nelle proprietà di Administration Server. • Creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.	180 giorni
Epidemia di virus	28 (per firewall)	GNRL_EV_VIRUS_OUTBREAK	Gli eventi di questo tipo si verificano quando il numero di oggetti dannosi rilevati in più dispositivi gestiti supera il limite in un periodo limitato. È possibile rispondere all'evento nei seguenti modi: • Configurare la soglia nelle proprietà di Administration Server. • Creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.	180 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Il dispositivo è diventato non gestito	4111	KLSRV_HOST_OUT_CONTROL	Eventi di questo tipo si verificano se un dispositivo gestito è visibile nella rete ma non si connette ad Administration Server da un periodo specifico. Determinare il motivo che impedisce il corretto funzionamento di Network Agent nel dispositivo. Le cause possibili includono i problemi di rete e la rimozione di Network Agent dal dispositivo.	180 giorni
Lo stato del dispositivo è Critico	4113	KLSRV_HOST_STATUS_CRITICAL	Eventi di questo tipo si verificano quando a un dispositivo gestito viene assegnato lo stato *Critico*. È possibile configurare le condizioni in cui lo stato del dispositivo diventa *Critico*.	180 giorni
Il file chiave è stato aggiunto alla lista vietati	4124	KLSRV_LICENSE_BLACKLISTED	Eventi di questo tipo si verificano quando Kaspersky ha aggiunto il codice di attivazione o il file chiave in uso alla lista vietati. Contattare il Servizio di assistenza tecnica per ulteriori dettagli.	180 giorni
Modalità con funzionalità limitate	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Eventi di questo tipo si verificano quando Kaspersky Security Center viene avviato con funzionalità di base, senza le funzionalità Vulnerability e patch management e Mobile Device Management. Di seguito sono riportati i motivi dell'evento e le risposte appropriate: • Il periodo licenza è scaduto. Fornire una licenza per utilizzare la modalità con funzionalità complete di Kaspersky Security Center (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). • Administration Server gestisce più dispositivi rispetto a quanto previsto dalla limitazione licenza. Spostare i dispositivi dai gruppi di amministrazione di un Administration Server a quelli di un altro Administration Server (se la limitazione licenza dell'altro Administration Server lo consente).	180 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
La licenza sta per scadere	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Eventi di questo tipo si verificano quando si avvicina la data di scadenza della licenza commerciale. Una volta al giorno Kaspersky Security Center verifica se si è in prossimità della data di scadenza della licenza. Gli eventi di questo tipo vengono pubblicati 30 giorni, 15 giorni, 5 giorni e 1 giorno prima della data di scadenza della licenza. Non è possibile modificare il numero di giorni. Se Administration Server è disattivato nel giorno specificato prima della data di scadenza della licenza, l'evento non verrà pubblicato fino al giorno successivo. Alla scadenza della licenza commerciale, Kaspersky Security Center fornisce solo le funzionalità di base. È possibile rispondere all'evento nei seguenti modi: • Verificare di aver aggiunto una chiave di licenza di riserva ad Administration Server. • Se si utilizza un abbonamento, assicurarsi di rinnovarlo. L'abbonamento illimitato viene rinnovato automaticamente se il pagamento al provider di servizi è stato effettuato anticipatamente entro il termine.	180 giorni
Il certificato è scaduto	4132	KLSRV_CERTIFICATE_EXPIRED	Eventi di questo tipo si verificano quando il certificato client nei dispositivi con certificato mobile scade.	180 giorni
Il certificato di Administration Server è scaduto.	6129	ServerCertificateExpired	Eventi di questo tipo si verificano quando scadono i certificati di Administration Server per i dispositivi mobili e i dispositivi UEFI. È necessario aggiornare il certificato scaduto.	180 giorni
Gli aggiornamenti per i moduli dell'applicazione Kaspersky sono stati revocati	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Eventi di questo tipo si verificano se gli aggiornamenti immediati sono stati revocati (per questi aggiornamenti viene visualizzato lo stato *Revocato*) dagli esperti di Kaspersky perché, ad esempio, devono essere aggiornati a una versione più recente. L'evento riguarda le patch di Kaspersky Security Center e non riguarda i moduli delle applicazioni gestite di Kaspersky. L'evento indica come motivo che gli aggiornamenti immediati non sono installati.	180 giorni
Controllo: esportazione in SIEM non riuscita	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Eventi di questo tipo si verificano quando l'esportazione degli eventi nel sistema SIEM non è riuscita a causa di un errore di connessione con il sistema SIEM.	180 giorni

Eventi di errore funzionale di Administration Server

La tabella seguente elenca i tipi di eventi di Kaspersky Security Center Administration Server con il livello di importanza **Errore funzionale**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di errore funzionale di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Errore di runtime	4125	KLSRV_RUNTIME_ERROR	Eventi di questo tipo si verificano a causa di problemi sconosciuti. La maggior parte delle volte si tratta di problemi DBMS, problemi di rete e altri problemi hardware e software. È possibile trovare i dettagli dell'evento nella descrizione dell'evento.	180 giorni
Limite di installazioni superato per uno dei gruppi di applicazioni concesse in licenza	4126	KLSRV_INVLICPROD_EXCEDED	Administration Server genera periodicamente eventi di questo tipo (ogni ora). Eventi di questo tipo si verificano se in Kaspersky Security Center si gestiscono chiavi di licenza di applicazioni di terze parti e se il numero di installazioni ha superato il limite impostato dalla chiave di licenza dell'applicazione di terze parti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare l'applicazione di terzi dai dispositivi in cui non è in uso l'applicazione. • Utilizzare una licenza di terzi per altri dispositivi. È possibile gestire le chiavi di licenza di applicazioni di terze parti utilizzando le funzionalità dei gruppi di applicazioni concesse in licenza. Un gruppo di applicazioni concesse in licenza include le applicazioni di terzi che soddisfano i criteri impostati dall'utente.	180 giorni
Impossibile eseguire il polling del segmento cloud	4143	KLSRV_KLCLOUD_SCAN_ERROR	Eventi di questo tipo si verificano quando Administration Server non riesce a eseguire il polling di un segmento di rete in un ambiente cloud. Leggere i dettagli nella descrizione dell'evento e rispondere di conseguenza.	Non archiviato
Impossibile copiare gli aggiornamenti nella cartella specificata	4123	KLSRV_UPD_REPL_FAIL	Eventi di questo tipo si verificano quando gli aggiornamenti software vengono copiati in una cartella condivisa aggiuntiva. È possibile rispondere all'evento nei seguenti modi: • Verificare che l'account utente utilizzato per ottenere l'accesso alla cartella disponga dell'autorizzazione di scrittura. • Verificare eventuali variazioni del nome utente e/o della password della cartella. • Verificare la connessione Internet poiché potrebbe essere la causa dell'evento. Seguire le istruzioni per l'aggiornamento dei database e dei moduli software.	180 giorni
Spazio su disco esaurito	4107	KLSRV_DISK_FULL	Eventi di questo tipo si verificano quando nel disco rigido del dispositivo in cui è installato Administration Server si esaurisce lo spazio disponibile. Liberare spazio su disco nel dispositivo.	180 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
La cartella condivisa non è disponibile	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Eventi di questo tipo si verificano se la cartella condivisa di Administration Server non è disponibile. È possibile rispondere all'evento nei seguenti modi: • Verificare che Administration Server (dove si trova la cartella condivisa) sia attivato e disponibile. • Verificare eventuali variazioni del nome utente e/o della password della cartella. • Verificare la connessione di rete.	180 giorni
Database di Administration Server non disponibile	4109	KLSRV_DATABASE_UNAVAILABLE	Eventi di questo tipo si verificano se il database di Administration Server diventa non disponibile. È possibile rispondere all'evento nei seguenti modi: • Verificare se è disponibile il server remoto in cui è installato SQL Server. • Visualizzare i log DBMS per scoprire il motivo della mancata disponibilità di Administration Server. A causa della manutenzione preventiva, un server remoto in cui è installato SQL Server potrebbe ad esempio non essere disponibile.	180 giorni
Spazio disponibile esaurito nel database di Administration Server	4110	KLSRV_DATABASE_FULL	Eventi di questo tipo si verificano quando non è disponibile spazio nel database di Administration Server. Administration Server non funziona quando il database ha raggiunto la capacità massima e non è possibile eseguire ulteriori registrazioni nel database. Di seguito sono riportate le cause di questo evento, a seconda del DBMS in uso, e le risposte appropriate all'evento: • Si utilizza il DBMS SQL Server Express Edition: Nella documentazione di SQL Server Express esaminare il limite relativo alle dimensioni del database per la versione utilizzata. È probabile che il database di Administration Server abbia superato il limite relativo alle dimensioni del database. Limitare il numero di eventi da archiviare nel database di Administration Server. Nel database di Administration Server sono presenti troppi eventi inviati dal componente Controllo Applicazioni. È possibile modificare le impostazioni del criterio di Kaspersky Endpoint Security for Windows relative all'archiviazione degli eventi di Controllo Applicazioni nel database di Administration Server. • Si utilizza un DBMS diverso da SQL Server Express Edition: Non limitare il numero di eventi da archiviare nel database di Administration Server. Ridurre l'elenco degli eventi da archiviare nel database di Administration Server. Rivedere le informazioni sulla selezione DBMS.	180 giorni

Eventi di avviso di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Administration Server con il livello di importanza **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
È stato rilevato un evento frequente		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Eventi di questo tipo si verificano quando Administration Server rileva un evento frequente in un dispositivo gestito. Per ulteriori dettagli, consultare la sezione seguente: Blocco degli eventi frequenti.	90 giorni
È stato superato il limite di licenze	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una volta al giorno Kaspersky Security Center verifica se è stato superato un limite di licenze. Gli eventi di questo tipo si verificano quando Administration Server rileva il superamento di alcune limitazioni di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client e se il numero delle unità di licensing attualmente utilizzate coperte da una singola licenza costituisce dal 100% al 110% del numero totale di unità coperte dalla licenza. Anche quando si verifica questo evento, i dispositivi client sono protetti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare i dispositivi non in uso. • Fornire una licenza per più dispositivi (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). Kaspersky Security Center determina le regole per generare gli eventi quando viene superato un limite di licenze.	90 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Il dispositivo è rimasto inattivo nella rete per molto tempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Eventi di questo tipo si verificano quando un dispositivo gestito risulta inattivo per un determinato periodo di tempo. Molto spesso ciò accade quando un dispositivo gestito viene disattivato. È possibile rispondere all'evento nei seguenti modi: • Rimuovere manualmente il dispositivo dall'elenco dei dispositivi gestiti. • Specificare l'intervallo di tempo dopo il quale viene creato l'evento **Il dispositivo è rimasto inattivo nella rete per molto tempo** utilizzando Administration Console o Kaspersky Security Center Web Console. • Specificare l'intervallo di tempo dopo il quale il dispositivo viene automaticamente rimosso dal gruppo utilizzando Administration Console o utilizzando Kaspersky Security Center Web Console.	90 giorni
Conflitto dei nomi di dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Eventi di questo tipo si verificano quando Administration Server considera due o più dispositivi gestiti come un unico dispositivo. Molto spesso questo accade quando un disco rigido clonato è stato utilizzato per la distribuzione del software nei dispositivi gestiti e senza eseguire il passaggio di Network Agent alla modalità di clonazione del disco dedicata in un dispositivo di riferimento. Per evitare questo problema, eseguire il passaggio di Network Agent alla modalità di clonazione del disco in un dispositivo di riferimento prima di clonare il disco rigido di questo dispositivo.	90 giorni
Lo stato del dispositivo è Avviso	4114	KLSRV_HOST_STATUS_WARNING	Eventi di questo tipo si verificano quando a un dispositivo gestito viene assegnato lo stato *Avviso*. È possibile configurare le condizioni in cui lo stato del dispositivo diventa *Avviso*.	90 giorni
Il limite di installazioni sta per essere superato per uno dei gruppi di applicazioni concesse in licenza	4127	KLSRV_INVLICPROD_FILLED	Eventi di questo tipo si verificano quando il numero di installazioni per applicazioni di terze parti incluse in un gruppo di applicazioni concesse in licenza raggiunge il 90% del valore massimo consentito specificato nelle proprietà della chiave di licenza. È possibile rispondere all'evento nei seguenti modi: • Se l'applicazione di terzi non è in uso in alcuni dei dispositivi gestiti, eliminare l'applicazione da questi dispositivi. • Se si prevede che il numero di installazioni per l'applicazione di terzi supererà il valore massimo consentito nell'immediato futuro, valutare la possibilità di ottenere in anticipo una licenza di terzi per un numero superiore di dispositivi. È possibile gestire le chiavi di licenza di applicazioni di terze parti utilizzando le funzionalità dei gruppi di applicazioni concesse in licenza.	90 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Il certificato è stato richiesto	4133	KLSRV_CERTIFICATE_REQUESTED	Eventi di questo tipo si verificano quando un certificato per Mobile Device Management non viene riemesso automaticamente. Di seguito sono elencate le possibili cause e le risposte appropriate all'evento: • È stata avviata la riemissione automatica per un certificato per il quale l'opzione **Riemetti automaticamente il certificato se possibile** è disabilitata. Ciò potrebbe essere dovuto a un errore che si è verificato durante la creazione del certificato. Potrebbe essere necessaria la riemissione manuale del certificato. • Se si utilizza un'integrazione con un'infrastruttura a chiave pubblica, la causa potrebbe essere un attributo SAM-Account-Name mancante dell'account utilizzato per l'integrazione con PKI e per l'emissione del certificato. Esaminare le proprietà dell'account.	90 giorni
Il certificato è stato rimosso	4134	KLSRV_CERTIFICATE_REMOVED	Eventi di questo tipo si verificano quando un amministratore rimuove qualsiasi tipo di certificato (generale, posta, VPN) per Mobile Device Management. Dopo aver rimosso un certificato, i dispositivi mobili connessi tramite questo certificato non riusciranno a connettersi ad Administration Server. Questo evento potrebbe essere utile quando si esaminano malfunzionamenti associati alla gestione dei dispositivi mobili.	90 giorni
Il certificato sta per scadere	6128	ServerCertificateExpiresSoon	Eventi di questo tipo si verificano quando scadono i certificati di Administration Server per i dispositivi mobili e i dispositivi UEFI. È necessario aggiornare il certificato scaduto.	90 giorni
Il certificato APNs è scaduto	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Eventi di questo tipo si verificano allo scadere di un certificato APNs. È necessario rinnovare manualmente il certificato APNs e installarlo in un server per dispositivi mobili MDM iOS.	Non archiviato
Il certificato APNs sta per scadere	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Eventi di questo tipo si verificano quando mancano meno di 14 giorni allo scadere del certificato APNs. Allo scadere del certificato APNs, è necessario rinnovare manualmente il certificato APNs e installarlo in un server per dispositivi mobili MDM iOS. È consigliabile pianificare il rinnovo del certificato APNs prima della data di scadenza.	Non archiviato

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Impossibile inviare il messaggio FCM al dispositivo mobile	4138	KLSRV_GCM_DEVICE_ERROR	Eventi di questo tipo si verificano quando Mobile Device Management è configurato per l'utilizzo di Firebase Cloud Messaging (FCM) per la connessione a dispositivi mobili gestiti con un sistema operativo Android e FCM Server non riesce a gestire alcune delle richieste ricevute da Administration Server. Questo vuol dire che alcuni dei dispositivi mobili gestiti non riceveranno una notifica push. Leggere il codice HTTP nei dettagli della descrizione dell'evento e rispondere di conseguenza. Per ulteriori informazioni sui codici HTTP ricevuti da FCM Server e sugli errori correlati, fare riferimento alla documentazione del servizio Firebase (vedere il capitolo "Codici di risposta dell'errore dei messaggi downstream").	90 giorni
Errore HTTP durante l'invio del messaggio FCM al server FCM	4139	KLSRV_GCM_HTTP_ERROR	Eventi di questo tipo si verificano quando Mobile Device Management è configurato per l'utilizzo di Firebase Cloud Messaging (FCM) per la connessione dei dispositivi mobili gestiti con il sistema operativo Android e FCM Server ripristina in Administration Server una richiesta con un codice HTTP diverso da 200 (OK). Di seguito sono elencate le possibili cause e le risposte appropriate all'evento: • Problemi sul lato server FCM. Leggere il codice HTTP nei dettagli della descrizione dell'evento e rispondere di conseguenza. Per ulteriori informazioni sui codici HTTP ricevuti da FCM Server e sugli errori correlati, fare riferimento alla documentazione del servizio Firebase (vedere il capitolo "Codici di risposta dell'errore dei messaggi downstream"). • Problemi sul lato server proxy (se si utilizza un server proxy). Leggere il codice HTTP nei dettagli della descrizione dell'evento e rispondere di conseguenza.	90 giorni
Impossibile inviare il messaggio FCM al server FCM	4140	KLSRV_GCM_GENERAL_ERROR	Eventi di questo tipo si verificano a causa di errori imprevisti sul lato Administration Server quando si utilizza il protocollo HTTP di Firebase Cloud Messaging. Leggere i dettagli nella descrizione dell'evento e rispondere di conseguenza. Se non si riesce a trovare autonomamente la soluzione a un problema, è consigliabile contattare il Servizio di assistenza tecnica Kaspersky.	90 giorni
Poco spazio libero nel disco rigido	4105	KLSRV_NO_SPACE_ON_VOLUMES	Eventi di questo tipo si verificano quando nel disco rigido del dispositivo in cui è installato Administration Server si esaurisce quasi totalmente lo spazio disponibile. Liberare spazio su disco nel dispositivo.	90 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Spazio libero insufficiente nel database di Administration Server	4106	KLSRV_NO_SPACE_IN_DATABASE	Eventi di questo tipo si verificano se lo spazio in Administration Server è troppo limitato. Se non si ovvierà alla situazione, il database di Administration Server raggiungerà in breve tempo la capacità massima e Administration Server non funzionerà. Di seguito sono riportate le cause di questo evento, a seconda del DBMS in uso, e le risposte appropriate all'evento. Si utilizza il DBMS SQL Server Express Edition: • Nella documentazione di SQL Server Express esaminare il limite relativo alle dimensioni del database per la versione utilizzata. È probabile che il database di Administration Server stia per raggiungere il limite relativo alle dimensioni del database. • Limitare il numero di eventi da archiviare nel database di Administration Server. • Nel database di Administration Server sono presenti troppi eventi inviati dal componente Controllo Applicazioni. È possibile modificare le impostazioni del criterio di Kaspersky Endpoint Security for Windows relative all'archiviazione degli eventi di Controllo Applicazioni nel database di Administration Server. Si utilizza un DBMS diverso da SQL Server Express Edition: • Non limitare il numero di eventi da archiviare nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server Rivedere le informazioni sulla selezione DBMS.	90 giorni
La connessione all'Administration Server secondario è stata interrotta	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Eventi di questo tipo si verificano quando una connessione all'Administration Server secondario viene interrotta. Leggere il registro eventi Kaspersky nel dispositivo in cui è installato l'Administration Server secondario e rispondere di conseguenza.	90 giorni
La connessione all'Administration Server primario è stata interrotta	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Eventi di questo tipo si verificano quando una connessione all'Administration Server primario viene interrotta. Leggere il registro eventi Kaspersky nel dispositivo in cui è installato l'Administration Server primario e rispondere di conseguenza.	90 giorni
Sono stati registrati nuovi aggiornamenti per i moduli dell'applicazione Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Eventi di questo tipo si verificano quando Administration Server registra nuovi aggiornamenti per il software Kaspersky installato nei dispositivi gestiti la cui installazione richiede l'approvazione. Approvare o rifiutare gli aggiornamenti utilizzando Administration Console o Kaspersky Security Center Web Console.	90 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Poiché è stato superato il limite relativo al numero di eventi nel database, è stata avviata l'eliminazione degli eventi	4145	KLSRV_EVP_DB_TRUNCATING	Eventi di questo tipo si verificano quando viene avviata l'eliminazione degli eventi precedenti dal database di Administration Server dopo il raggiungimento della capacità massima del database di Administration Server. È possibile rispondere all'evento nei seguenti modi: • Cambiare il numero massimo di eventi archiviati nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server	Non archiviato
Poiché è stato superato il limite relativo al numero di eventi nel database, gli eventi sono stati eliminati	4146	KLSRV_EVP_DB_TRUNCATED	Eventi di questo tipo si verificano dopo l'eliminazione degli eventi precedenti dal database di Administration Server in seguito al raggiungimento della capacità massima del database di Administration Server. È possibile rispondere all'evento nei seguenti modi: • Cambiare il numero massimo consentito di eventi archiviati nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server	Non archiviato
Controllo (test della connessione al server SIEM non riuscito)	5120	KLAUD_EV_SIEM_TEST_FAILED	Eventi di questo tipo si verificano quando una connessione di test al server SIEM non riesce.	30 giorni
Impossibile emettere il certificato automaticamente		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Questo evento si verifica in caso di errore durante la creazione di un certificato client per un dispositivo mobile (un dispositivo eseguito con un protocollo mobile).	90 giorni

Eventi informativi di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Administration Server con il livello di importanza **Informazioni**.

Eventi informativi di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito	Osservazioni
Utilizzo della chiave di licenza superiore al 90%	4097	KLSRV_EV_LICENSE_CHECK_90	30 giorni	
Nuovo dispositivo rilevato	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 giorni	
Il dispositivo è stato aggiunto automaticamente al gruppo	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 giorni	
Il dispositivo è stato spostato automaticamente in base a una regola	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 giorni	
Il dispositivo è stato rimosso dal gruppo poiché inattivo nella rete per molto tempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 giorni	

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito	Osservazioni
Sta per essere superato il limite di installazioni (è stato utilizzato più del 95%) per uno dei gruppi di applicazioni concesse in licenza	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 giorni	
Sono disponibili alcuni file da inviare a Kaspersky per l'analisi	4131	KLSRV_APS_FILE_APPEARED	30 giorni	
L'ID istanza FCM è stato modificato in questo dispositivo mobile	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 giorni	
Aggiornamenti copiati nella cartella specificata	4122	KLSRV_UPD_REPL_OK	30 giorni	
La connessione all'Administration Server secondario è stata stabilita	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 giorni	
La connessione all'Administration Server primario è stata stabilita	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 giorni	
I database sono stati aggiornati	4144	KLSRV_UPD_BASES_UPDATED	30 giorni	
Controllo: la connessione ad Administration Server è stata stabilita	4147	KLAUD_EV_SERVERCONNECT	30 giorni	
Controllo: l'oggetto è stato modificato	4148	KLAUD_EV_OBJECTMODIFY	30 giorni	Questo evento monitora le modifiche nei seguenti oggetti: • Gruppo di amministrazione • Gruppo di protezione • Utente • Pacchetto • Attività • Criterio • Server • Server virtuale
Controllo: lo stato dell'oggetto è stato modificato	4150	KLAUD_EV_TASK_STATE_CHANGED	30 giorni	Ad esempio, questo evento si verifica quando un'attività non è riuscita con un errore.
Controllo: le impostazioni del gruppo sono state modificate	4149	KLAUD_EV_ADMGROUP_CHANGED	30 giorni	
Controllo: la connessione ad Administration Server è stata terminata	4151	KLAUD_EV_SERVERDISCONNECT	30 giorni	
Controllo: le proprietà dell'oggetto sono state modificate	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 giorni	Questo evento monitora le modifiche nelle seguenti proprietà: • Utente • Licenza • Server • Server virtuale

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito	Osservazioni
Controllo: le autorizzazioni dell'utente sono state modificate	4153	KLAUD_EV_OBJECTACLMODIFIED	30 giorni	
Controllo: le chiavi di criptaggio sono state importate o esportate da Administration Server	5100	KLAUD_EV_DPEKEYSEXPORT	30 giorni	
Controllo (test della connessione al server SIEM riuscito)	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 giorni	Questo evento si verifica quando una connessione di test al server SIEM riesce.
Certificato di riserva creato		ServerReserveCertificateCreated	30 giorni	Questo evento si verifica quando è stato creato un certificato di Administration Server.
Certificato in rinnovo		ServerCertificateRenewed	30 giorni	Questo evento si verifica quando il certificato di Administration Server è stato rinnovato.
Certificato emesso automaticamente e correttamente		KLSRV_CERTIFICATE_AUTO_ISSUED	30 giorni	Questo evento si verifica quando è stato creato correttamente un certificato per un dispositivo mobile (un dispositivo eseguito con un protocollo mobile).

Gli eventi **Certificato di riserva creato, Certificato in rinnovo** e **Certificato emesso automaticamente e correttamente** vengono pubblicati automaticamente da Administration Server e visualizzati in Administration Console solo quando le operazioni corrispondenti a questi eventi vengono eseguite per i certificati di Administration Server per i dispositivi mobili e i dispositivi UEFI.

Eventi di Network Agent

Questa sezione contiene informazioni sugli eventi relativi a Network Agent.

Eventi di errore funzionale di Network Agent

La tabella seguente elenca i tipi di eventi di Kaspersky Security Center Network Agent con il livello di criticità **Errore funzionale**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di errore funzionale di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Errore durante l'installazione dell'aggiornamento	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Gli eventi di questo tipo si verificano se l'installazione automatica di aggiornamenti e patch per i componenti Kaspersky Security Center non è andata a buon fine. L'evento non riguarda gli aggiornamenti delle applicazioni gestite Kaspersky. Leggere la descrizione dell'evento. Un problema di Windows in Administration Server potrebbe essere la causa dell'evento. Se nella descrizione vengono menzionati problemi relativi alla configurazione di Windows, risolvere il problema.	30 giorni
Impossibile installare l'aggiornamento software di terze parti	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Gli eventi di questo tipo si verificano se sono in uso le funzionalità Vulnerability e patch management e Mobile Device Management e se l'aggiornamento del software di terze parti non è andato a buon fine. Verificare che il collegamento al software di terze parti sia valido. Leggere la descrizione dell'evento.	30 giorni
Impossibile installare gli aggiornamenti di Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Gli eventi di questo tipo si verificano se gli aggiornamenti di Windows non sono andati a buon fine. Configurare gli aggiornamenti di Windows in un criterio di Network Agent. Leggere la descrizione dell'evento. Cercare l'errore nella Microsoft Knowledge Base. Contattare il supporto tecnico Microsoft se non si riesce a risolvere autonomamente il problema.	30 giorni
Gestione degli utenti: errori	7723	KLNAG_EV_USR_MNG_ERR	Evento di avviso generale.	30 giorni
Impossibile ripristinare il valore di riferimento del file Sudoers	7726	KLNAG_EV_SUDOER_RESTORED_ERR	L'evento contiene la descrizione dell'errore di sostituzione del file sudoers.	30 giorni
Impossibile installare i certificati radice	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	L'evento contiene la descrizione dell'errore di installazione dei certificati.	30 giorni
Impossibile rimuovere i certificati radice	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	L'evento contiene la descrizione dell'errore di rimozione dei certificati.	30 giorni

Eventi di avviso di Network Agent

La tabella seguente elenca gli eventi di Kaspersky Security Center Network Agent con il livello di gravità **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
È stato restituito un avviso durante l'installazione dell'aggiornamento dei moduli software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 giorni
Installazione dell'aggiornamento software di terze parti completata con un avviso	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Installazione dell'aggiornamento software di terze parti rimandata	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 giorni
Si è verificato un problema di sicurezza	549	GNRL_EV_APP_INCIDENT_OCCURED	30 giorni
Proxy KSN avviato. Impossibile verificare la disponibilità di KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 giorni
Gestione degli utenti: avvisi	7722	KLNAG_EV_USR_MNG_WRN	30 giorni
Trovato file Sudoers che non corrisponde al valore di riferimento	7724	KLNAG_EV_SUDOER_DIFFERENT	30 giorni

Eventi informativi di Network Agent

La tabella seguente elenca gli eventi di Kaspersky Security Center Network Agent con il livello di gravità **Informazioni**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi informativi di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Installazione dell'aggiornamento per i moduli software completata	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 giorni
Installazione dell'aggiornamento dei moduli software avviata	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 giorni
Applicazione installata	7703	KLNAG_EV_INV_APP_INSTALLED	30 giorni
Applicazione rimossa	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 giorni
Applicazione monitorata installata	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 giorni
Applicazione monitorata rimossa	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 giorni
Applicazione di terze parti installata	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 giorni
Nuovo dispositivo aggiunto	7708	KLNAG_EV_DEVICE_ARRIVAL	30 giorni
Dispositivo rimosso	7709	KLNAG_EV_DEVICE_REMOVE	30 giorni
Nuovo dispositivo rilevato	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 giorni
Dispositivo autorizzato	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 giorni
Condivisione desktop Windows: file letto	7712	KLUSRLOG_EV_FILE_READ	30 giorni
Condivisione desktop Windows: file modificato	7713	KLUSRLOG_EV_FILE_MODIFIED	30 giorni
Condivisione desktop Windows: applicazione avviata	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 giorni
Condivisione desktop Windows: avviata	7715	KLUSRLOG_EV_WDS_BEGIN	30 giorni
Condivisione desktop Windows: arrestata	7716	KLUSRLOG_EV_WDS_END	30 giorni
Installazione dell'aggiornamento software di terze parti completata	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 giorni
Installazione dell'aggiornamento software di terze parti avviata	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Proxy KSN avviato. La verifica della disponibilità di KSN è stata completata	7719	KSNPROXY_STARTED_CON_CHK_OK	30 giorni
Proxy KSN arrestato	7720	KSNPROXY_STOPPED	30 giorni

Eventi di Server per dispositivi mobili MDM iOS

Questa sezione contiene informazioni sugli eventi relativi al server MDM iOS.

Eventi di errore funzionale di Server per dispositivi mobili MDM iOS

La tabella seguente elenca gli eventi del server per dispositivi mobili MDM iOS di Kaspersky Security Center con il livello di criticità **Errore funzionale**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di errore funzionale di Server per dispositivi mobili MDM iOS

Nome visualizzato del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Impossibile richiedere l'elenco dei profili	PROFILELIST_COMMAND_FAILED	30 giorni
Impossibile installare il profilo	INSTALLPROFILE_COMMAND_FAILED	30 giorni
Impossibile rimuovere il profilo	REMOVEPROFILE_COMMAND_FAILED	30 giorni
Impossibile richiedere l'elenco dei profili di provisioning	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 giorni
Impossibile installare il profilo di provisioning	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 giorni
Impossibile eliminare il profilo di provisioning	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 giorni
Impossibile richiedere l'elenco dei certificati digitali	CERTIFICATELIST_COMMAND_FAILED	30 giorni
Impossibile richiedere l'elenco di applicazioni installate	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 giorni
Impossibile richiedere le informazioni generali sul dispositivo mobile	DEVICEINFORMATION_COMMAND_FAILED	30 giorni
Impossibile richiedere le informazioni di protezione	SECURITYINFO_COMMAND_FAILED	30 giorni
Impossibile bloccare il dispositivo mobile	DEVICELOCK_COMMAND_FAILED	30 giorni
Impossibile reimpostare la password	CLEARPASSCODE_COMMAND_FAILED	30 giorni
Impossibile cancellare i dati dal dispositivo mobile	ERASEDEVICE_COMMAND_FAILED	30 giorni
Impossibile installare l'app	INSTALLAPPLICATION_COMMAND_FAILED	30 giorni
Impossibile impostare il codice di riscatto per l'app	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 giorni
Impossibile richiedere l'elenco delle app gestite	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 giorni
Impossibile rimuovere l'app gestita	REMOVEAPPLICATION_COMMAND_FAILED	30 giorni
Impostazioni roaming rifiutate	SETROAMINGSETTINGS_COMMAND_FAILED	30 giorni
Si è verificato un errore durante l'esecuzione dell'app	PRODUCT_FAILURE	30 giorni
Il risultato del comando contiene dati non validi	MALFORMED_COMMAND	30 giorni

Nome visualizzato del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Impossibile inviare la notifica push	SEND_PUSH_NOTIFICATION_FAILED	30 giorni
Impossibile inviare il comando	SEND_COMMAND_FAILED	30 giorni
Dispositivo non trovato	DEVICE_NOT_FOUND	30 giorni

Eventi di avviso di Server per dispositivi mobili MDM iOS

La tabella seguente elenca gli eventi di Server per dispositivi mobili MDM iOS di Kaspersky Security Center con il livello di gravità **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Server per dispositivi mobili MDM iOS

Nome visualizzato del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
È stato rilevato un tentativo di connessione di un dispositivo mobile	INACTICE_DEVICE_TRY_CONNECTED	30 giorni
Il profilo è stato rimosso	MDM_PROFILE_WAS_REMOVED	30 giorni
Tentativo di utilizzare un certificato client già in uso	CLIENT_CERT_ALREADY_IN_USE	30 giorni
È stato rilevato un dispositivo inattivo	FOUND_INACTIVE_DEVICE	30 giorni
È necessario il codice di riscatto	NEED_REDEMPTION_CODE	30 giorni
Profilo incluso in un criterio rimosso dal dispositivo	UMDM_PROFILE_WAS_REMOVED	30 giorni

Eventi informativi di Server per dispositivi mobili MDM iOS

La tabella seguente elenca gli eventi di Server per dispositivi mobili MDM iOS di Kaspersky Security Center con il livello di gravità **Informazioni**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi informativi di Server per dispositivi mobili MDM iOS

Nome visualizzato del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Un nuovo dispositivo mobile è stato connesso	NEW_DEVICE_CONNECTED	30 giorni
L'elenco dei profili è stato richiesto	PROFILELIST_COMMAND_SUCCESSFULL	30 giorni
Il profilo è stato installato	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 giorni
Il profilo è stato rimosso	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 giorni
L'elenco dei profili di provisioning è stato richiesto	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 giorni
L'installazione del profilo di provisioning è stata completata	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 giorni
La rimozione del profilo di provisioning è stata completata	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 giorni

Nome visualizzato del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
L'elenco dei certificati digitali è stato richiesto	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 giorni
L'elenco delle applicazioni installate è stato richiesto	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 giorni
Informazioni generali sul dispositivo mobile richieste	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 giorni
Le informazioni di protezione sono state richieste	SECURITYINFO_COMMAND_SUCCESSFULL	30 giorni
Il dispositivo mobile è stato bloccato	DEVICELOCK_COMMAND_SUCCESSFULL	30 giorni
La password è stata reimpostata	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 giorni
I dati sono stati cancellati dal dispositivo mobile	ERASEDEVICE_COMMAND_SUCCESSFULL	30 giorni
L'applicazione è stata installata	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 giorni
Il codice di riscatto è stato impostato per l'app	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 giorni
L'elenco delle app gestite è stato richiesto	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 giorni
L'app gestita è stata rimossa	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 giorni
Impostazioni roaming applicate	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 giorni

Blocco degli eventi frequenti

Questa sezione fornisce informazioni sulla gestione del blocco degli eventi frequenti, sulla rimozione del blocco degli eventi frequenti e sull'esportazione dell'elenco degli eventi frequenti in un file.

Informazioni sul blocco degli eventi frequenti

Un'applicazione gestita, ad esempio Kaspersky Endpoint Security for Windows, installata in uno o più dispositivi gestiti può inviare molti eventi dello stesso tipo ad Administration Server. La ricezione di eventi frequenti può sovraccaricare il database di Administration Server e sovrascrivere altri eventi. Administration Server inizia a bloccare gli eventi più frequenti quando il numero di tutti gli eventi ricevuti supera il limite specificato per il database.

Administration Server blocca la ricezione automatica degli eventi frequenti. Non è possibile bloccare autonomamente gli eventi frequenti o scegliere quali eventi bloccare.

Se si desidera scoprire se un evento è bloccato, è possibile verificare se questo evento è presente nella sezione **Blocco degli eventi frequenti** delle proprietà di Administration Server. Se l'evento è bloccato, è possibile eseguire le seguenti operazioni:

- Se si desidera impedire la sovrascrittura del database, è possibile continuare a bloccare la ricezione di questo tipo di eventi.
- Se ad esempio si desidera individuare il motivo dell'invio degli eventi frequenti ad Administration Server, è possibile sbloccare gli eventi frequenti e continuare a ricevere comunque gli eventi di questo tipo.
- Se si desidera continuare a ricevere gli eventi frequenti finché non vengono nuovamente bloccati, è possibile rimuovere dal blocco gli eventi frequenti.

Gestione del blocco degli eventi frequenti

Administration Server blocca automaticamente la ricezione degli eventi frequenti, ma è possibile interrompere il blocco e continuare a ricevere gli eventi frequenti. È inoltre possibile bloccare la ricezione degli eventi frequenti sbloccati in precedenza.

Per gestire il blocco degli eventi frequenti:

1. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server**, quindi selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server accedere al riquadro **Sezioni** e selezionare **Blocco degli eventi frequenti**.
3. Nella sezione **Blocco degli eventi frequenti**:
   - Selezionare le opzioni **Tipo di evento** degli eventi per cui si desidera bloccare la ricezione.
   - Deselezionare le opzioni **Tipo di evento** degli eventi che si desidera continuare a ricevere.
4. Fare clic sul pulsante **Applica**.
5. Fare clic sul pulsante **OK**.

Administration Server riceve gli eventi frequenti per i quali è stata deselezionata l'opzione **Tipo di evento** e blocca la ricezione degli eventi frequenti per i quali è stata selezionata l'opzione **Tipo di evento**.

Rimozione del blocco degli eventi frequenti

È possibile rimuovere il blocco per gli eventi frequenti e iniziare a riceverli fino a quando Administration Server bloccherà nuovamente questo tipo di eventi frequenti.

Per rimuovere il blocco degli eventi frequenti:

1. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server**, quindi selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server accedere al riquadro **Sezioni** e selezionare **Blocco degli eventi frequenti**.

3. Nella sezione **Blocco degli eventi frequenti** fare clic sulla riga dell'evento frequente per il quale si desidera rimuovere il blocco.

4. Fare clic sul pulsante **Elimina**.

L'evento frequente viene rimosso dall'elenco degli eventi frequenti. Administration Server riceverà gli eventi di questo tipo.

Esportazione di un elenco degli eventi frequenti in un file

Per esportare un elenco degli eventi frequenti in un file:

1. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server**, quindi selezionare **Proprietà**.

2. Nella finestra delle proprietà di Administration Server accedere al riquadro **Sezioni** e selezionare **Blocco degli eventi frequenti**.

3. Fare clic sul pulsante **Esporta in un file**.

4. Nella finestra **Salva con nome** visualizzata specificare il percorso del file in cui si desidera salvare l'elenco.

5. Fare clic sul pulsante **Salva**.

Tutti i record nell'elenco degli eventi frequenti vengono esportati in un file.

Controllo delle modifiche di stato delle macchine virtuali

Administration Server archivia le informazioni sullo stato dei dispositivi gestiti, come il registro hardware e l'elenco delle applicazioni installate, e le impostazioni di applicazioni gestite, attività e criteri. Se una macchina virtuale opera come dispositivo gestito, l'utente può ripristinarne lo stato in qualsiasi momento utilizzando uno snapshot della macchina virtuale creato in precedenza. Le informazioni sullo stato della macchina virtuale in Administration Server possono diventare obsolete.

Ad esempio, si supponga che alle 12:00 l'amministratore crei in Administration Server un criterio di protezione, di cui viene avviata l'esecuzione nella macchina virtuale VM_1 alle 12:01. Alle 12:30, l'utente della macchina virtuale VM_1 ne modifica lo stato ripristinandola da uno snapshot eseguito alle 11:00. Viene interrotta l'esecuzione del criterio di protezione nella macchina virtuale. Tuttavia, le informazioni obsolete archiviate in Administration Server indicano che il criterio di protezione nella macchina virtuale VM_1 continua.

Kaspersky Security Center aiuta a monitorare tutte le modifiche dello stato delle macchine virtuali.

Dopo ogni sincronizzazione con un dispositivo, Administration Server genera un ID univoco, che viene archiviato sia nel dispositivo che nell'Administration Server. Prima di avviare la sincronizzazione successiva, Administration Server confronta i valori di entrambi questi ID. Se i valori degli ID non corrispondono, Administration Server riconosce la macchina virtuale come ripristinata da uno snapshot. Administration Server reimposta tutte le impostazioni di criteri e attività attivi per la macchina virtuale e invia alla macchina virtuale i criteri aggiornati e l'elenco delle attività di gruppo.

Monitoraggio dello stato della protezione anti-virus tramite le informazioni del Registro di sistema

Per monitorare lo stato della protezione anti-virus in un dispositivo client utilizzando le informazioni registrate da Network Agent, a seconda del sistema operativo del dispositivo:

- Nei dispositivi che eseguono Windows:

  1. Aprire il Registro di sistema del dispositivo client (ad esempio, in locale, utilizzando il comando regedit nel menu **Start** → **Esegui**).

  2. Passare al seguente hive:

     - Per i sistemi a 32 bit:

       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - Per i sistemi a 64 bit:

       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     Nel Registro di sistema vengono visualizzate informazioni sullo stato della protezione anti-virus del dispositivo client.

- Nei dispositivi che eseguono Linux:

  - Le informazioni sono racchiuse in file di testo separati, uno per ciascun tipo di dati, disponibili in /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.

- Nei dispositivi che eseguono macOS:

  - Le informazioni sono racchiuse in file di testo separati, uno per ciascun tipo di dati, disponibili in /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

Lo stato della protezione anti-virus corrisponde ai valori delle chiavi descritti nella tabella seguente.

Chiavi del Registro di sistema e possibili valori

Chiave (tipo di dati)	Valore	Descrizione
`Protection_LastConnected (REG_SZ)`	DD-MM-YYYY HH-MM-SS	Data e ora (in formato UTC) dell'ultima connessione all'Administration Server
`Protection_AdmServer (REG_SZ)`	IP, nome DNS o nome NetBIOS	Nome dell'Administration Server che gestisce il dispositivo
`Protection_NagentVersion (REG_SZ)`	a.b.c.d	Numero della build di Network Agent installata nel dispositivo
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (patch1; patch2; ...; patchN)	Numero completo della versione di Network Agent (con patch) installata nel dispositivo
`Protection_HostId (REG_SZ)`	ID dispositivo	ID del dispositivo
`Protection_DynamicVM (REG_DWORD)`	0 — no 1 — yes	Network Agent è installato in modalità VDI dinamica
`Protection_AvInstalled (REG_DWORD)`	0 — no 1 — yes	Un'applicazione di protezione è installata nel dispositivo

Chiave (tipo di dati)	Valore	Descrizione
`Protection_AvRunning (REG_DWORD)`	0 — no 1 — yes	La protezione in tempo reale è abilitata nel dispositivo
`Protection_HasRtp (REG_DWORD)`	0 — no 1 — yes	Un componente per la protezione in tempo reale è installato
`Protection_RtpState (REG_DWORD)`	Stato protezione in tempo reale:	
	0	Sconosciuto
	1	Disabilitata
	2	Sospesa
	3	Avvio in corso
	4	Abilitata
	5	Abilitato con livello di protezione elevato (protezione massima)
	6	Abilitato con livello di protezione basso (velocità massima)
	7	Abilitato con impostazioni predefinite (opzione consigliata)
	8	Abilitato con impostazioni personalizzate
	9	Operazione non riuscita
`Protection_LastFscan (REG_SZ)`	DD-MM-YYYY HH-MM-SS	Data e ora (in formato UTC) dell'ultima scansione completa
`Protection_BasesDate (REG_SZ)`	DD-MM-YYYY HH-MM-SS	Data e ora (in formato UTC) di rilascio dei database dell'applicazione

Visualizzazione e configurazione delle azioni per i dispositivi inattivi

È possibile ottenere notifiche relative ai dispositivi client all'interno di un gruppo che risultano inattivi. È anche possibile eliminare automaticamente tali dispositivi.

Per visualizzare o configurare le azioni eseguite quando i dispositivi nel gruppo risultano inattivi:

1. Nella struttura della console fare clic con il pulsante destro del mouse sul nome del gruppo di amministrazione desiderato.
2. Nel menu di scelta rapida selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del gruppo di amministrazione.
3. Nella finestra **Proprietà**, passare alla sezione **Dispositivi**.

4. Se necessario, abilitare o disabilitare le seguenti opzioni:

- **Avvisa l'amministratore se il dispositivo è inattivo da più di (giorni)**

  Se questa opzione è abilitata, l'amministratore riceve le notifiche sui dispositivi inattivi. È possibile specificare l'intervallo di tempo al termine del quale verrà creato l'evento **Il dispositivo risulta inattivo nella rete da molto tempo**. L'intervallo di tempo predefinito è 7 giorni.

  Per impostazione predefinita, questa opzione è abilitata.

- **Rimuovi il dispositivo dal gruppo se è inattivo da più di (giorni)**

  Se questa opzione è abilitata, è possibile specificare l'intervallo di tempo al termine del quale il dispositivo viene rimosso automaticamente dal gruppo. L'intervallo di tempo predefinito è 60 giorni.

  Per impostazione predefinita, questa opzione è abilitata.

- **Eredita da gruppo padre**

  Le impostazioni di questa sezione saranno ereditate dal gruppo padre di cui fa parte il dispositivo client. Se questa opzione è abilitata, le impostazioni in **Attività dei dispositivi nella rete** sono bloccate dalle modifiche.

  Questa opzione è disponibile solo se il gruppo di amministrazione ha un gruppo padre.

  Per impostazione predefinita, questa opzione è abilitata.

- **Forza ereditarietà nei gruppi figlio**

  I valori delle impostazioni vengono distribuiti ai gruppi figlio, ma nelle proprietà dei gruppi figlio tali impostazioni sono bloccate.

  Per impostazione predefinita, questa opzione è disabilitata.

5. Fare clic su **OK**.

Le modifiche verranno salvate e applicate.

Disabilitazione degli annunci di Kaspersky

In Kaspersky Security Center Web Console la sezione Annunci Kaspersky (**Monitoraggio e generazione dei rapporti** → **Annunci Kaspersky**) consente di rimanere informati fornendo informazioni relative alla versione in uso di Kaspersky Security Center e alle applicazioni gestite installate nei dispositivi gestiti. Se non si desidera ricevere gli annunci di Kaspersky, è possibile disabilitare questa funzionalità.

Gli annunci Kaspersky includono due tipi di informazioni: annunci relativi alla sicurezza e annunci di marketing. È possibile disabilitare separatamente gli annunci di ciascun tipo.

Per disabilitare gli annunci relativi alla sicurezza:

1. Nella struttura della console selezionare l'Administration Server per cui si desidera disabilitare gli annunci relativi alla sicurezza.

2. Fare clic con il pulsante destro del mouse e, nel menu di scelta rapida visualizzato, selezionare **Proprietà**.

3. Nella finestra delle proprietà di Administration Server visualizzata, nella sezione **Annunci Kaspersky**, disabilitare l'opzione **Abilita la visualizzazione degli annunci Kaspersky in Kaspersky Security Center Web Console**.

4. Fare clic su **OK**.

Gli annunci di Kaspersky vengono disabilitati.

Gli annunci di marketing sono disabilitati per impostazione predefinita. Gli annunci di marketing vengono ricevuti solo se è stato abilitato Kaspersky Security Network (KSN). È possibile disabilitare questo tipo di annunci disabilitando KSN.

Regolazione di punti di distribuzione e gateway di connessione

Una struttura di gruppi di amministrazione in Kaspersky Security Center esegue le seguenti funzioni:

- Imposta l'ambito dei criteri

  È disponibile un metodo alternativo per l'applicazione delle impostazioni appropriate nei dispositivi, utilizzando i *profili criterio*. In questo caso, l'ambito dei criteri viene definito con tag, posizioni dei dispositivi nelle unità organizzative di Active Directory o appartenenza a gruppi di protezione di Active Directory.

- Imposta l'ambito delle attività di gruppo

  Esiste un approccio alla definizione dell'ambito delle attività di gruppo che non è basato su una gerarchia di gruppi di amministrazione: l'utilizzo di attività per selezioni dispositivi e di attività per dispositivi specifici.

- Imposta i diritti di accesso a dispositivi, Administration Server virtuali e Administration Server secondari

- Assegna i punti di distribuzione

Al momento della creazione della struttura dei gruppi di amministrazione, è necessario tenere conto della topologia della rete dell'organizzazione per l'assegnazione ottimale dei punti di distribuzione. La distribuzione ottimale dei punti di distribuzione consente di ridurre il traffico nella rete dell'organizzazione.

A seconda dello schema dell'organizzazione e della topologia di rete, le seguenti configurazioni standard possono essere applicate alla struttura dei gruppi di amministrazione:

- Singola sede

- Più sedi remote di piccole dimensioni

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Configurazione standard dei punti di distribuzione: singola sede

In una configurazione standard con una singola sede, tutti i dispositivi si trovano nella rete dell'organizzazione e sono visibili reciprocamente. La rete dell'organizzazione può comprendere diversi componenti (reti o segmenti di rete) connessi tramite canali con larghezza di banda ridotta.

Sono disponibili i seguenti metodi per creare la struttura dei gruppi di amministrazione:

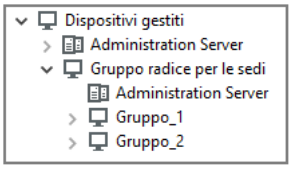
- Creazione della struttura dei gruppi di amministrazione tenendo conto della topologia di rete. La struttura dei gruppi di amministrazione potrebbe non riflettere la topologia di rete alla perfezione. Una corrispondenza tra i diversi componenti della rete e alcuni gruppi di amministrazione può essere sufficiente. È possibile utilizzare l'assegnazione automatica dei punti di distribuzione o assegnarli manualmente.

- Creazione della struttura dei gruppi di amministrazione senza tenere conto della topologia di rete. In questo caso è necessario disabilitare l'assegnazione automatica dei punti di distribuzione e quindi assegnare a uno o più dispositivi il ruolo di punti di distribuzione per un gruppo di amministrazione radice in ciascun componente della rete, ad esempio per il gruppo **Dispositivi gestiti**. Tutti i punti di distribuzione saranno allo stesso livello e avranno lo stesso ambito che comprende tutti i dispositivi della rete dell'organizzazione. In questo caso, tutti i Network Agent si connetteranno al punto di distribuzione con il percorso più vicino. Il percorso di un punto di distribuzione è monitorabile con l'utilità tracert.

Configurazione standard dei punti di distribuzione: più sedi remote di piccole dimensioni

Questa configurazione standard prevede la presenza di diverse sedi remote, che possono comunicare con la sede centrale via Internet. Ogni sede remota è situata dietro il NAT, ovvero la connessione da una sede remota all'altra non è possibile perché le sedi sono isolate tra loro.

La configurazione deve essere riflessa nella struttura dei gruppi di amministrazione: è necessario creare un gruppo di amministrazione distinto per ogni sede remota (i gruppi **Sede 1** e **Sede 2** nella figura seguente).



Le sedi remote sono incluse nella struttura dei gruppi di amministrazione

È necessario assegnare uno o più punti di distribuzione a ogni gruppo di amministrazione che corrisponde a una sede. I punti di distribuzione devono essere dispositivi nella sede remota con una quantità sufficiente di spazio libero su disco. I dispositivi distribuiti nel gruppo **Sede 1**, ad esempio, accederanno ai punti di distribuzione assegnati al gruppo di amministrazione **Sede 1**.

Se alcuni utenti si spostano fisicamente tra le sedi con i loro computer portatili, è necessario selezionare due o più dispositivi (oltre ai punti di distribuzione esistenti) in ogni sede remota e assegnare loro il ruolo di punti di distribuzione per un gruppo di amministrazione di primo livello (**Gruppo radice per le sedi** nella figura precedente).

Esempio: un computer portatile è distribuito nel gruppo di amministrazione **Sede 1** e quindi viene spostato fisicamente nella sede che corrisponde al gruppo di amministrazione **Sede 2**. Dopo lo spostamento del portatile, Network Agent tenta di accedere ai punti di distribuzione assegnati al gruppo **Sede 1**, ma tali punti di distribuzione non sono disponibili. Network Agent inizia quindi a tentare di accedere ai punti di distribuzione che sono stati assegnati al **Gruppo radice per le sedi**. Poiché le sedi remote sono isolate tra loro, i tentativi di accedere ai punti di distribuzione assegnati al gruppo di amministrazione **Gruppo radice per le sedi** avranno esito positivo solo quando Network Agent tenta di accedere ai punti di distribuzione nel gruppo **Sede 2**. In altre parole, il computer portatile rimarrà nel gruppo di amministrazione che corrisponde alla sede iniziale, ma utilizzerà il punto di distribuzione della sede in cui si trova fisicamente al momento.

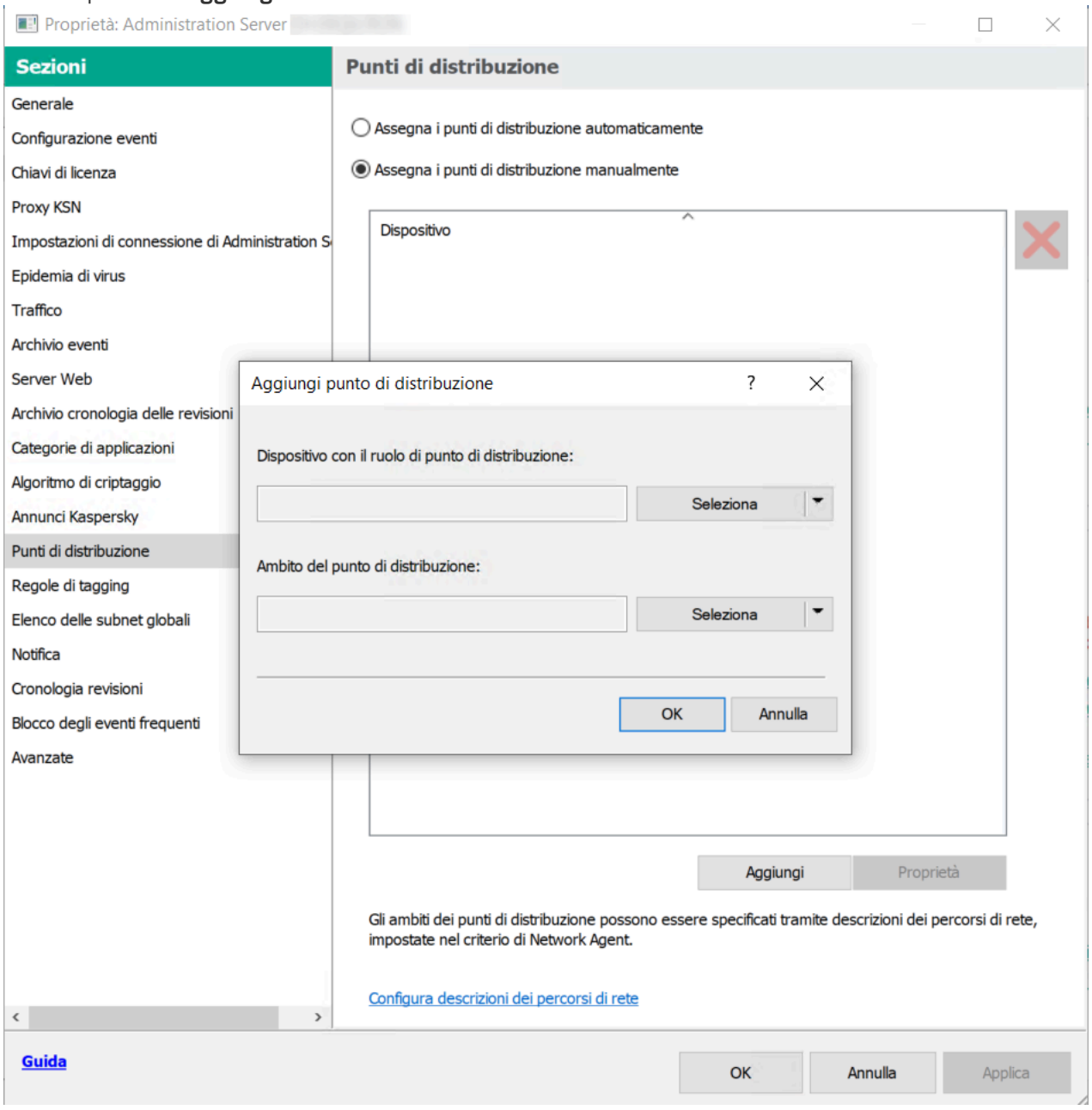
Assegnazione di un dispositivo gestito a cui assegnare il ruolo di punto di distribuzione

È possibile assegnare manualmente a un dispositivo il ruolo di punto di distribuzione per un gruppo di amministrazione e configurarlo come gateway di connessione in Administration Console.

Per assegnare un dispositivo come punto di distribuzione di un gruppo di amministrazione:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Nel menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server selezionare la sezione **Punti di distribuzione**.
4. Nella parte destra della finestra selezionare l'opzione **Assegna i punti di distribuzione manualmente**.

5. Fare clic sul pulsante **Aggiungi**.



Assegnazione manuale di un punto di distribuzione

Verrà visualizzata la finestra **Aggiungi punto di distribuzione**.

6. Nella finestra **Aggiungi punto di distribuzione** eseguire le seguenti azioni:

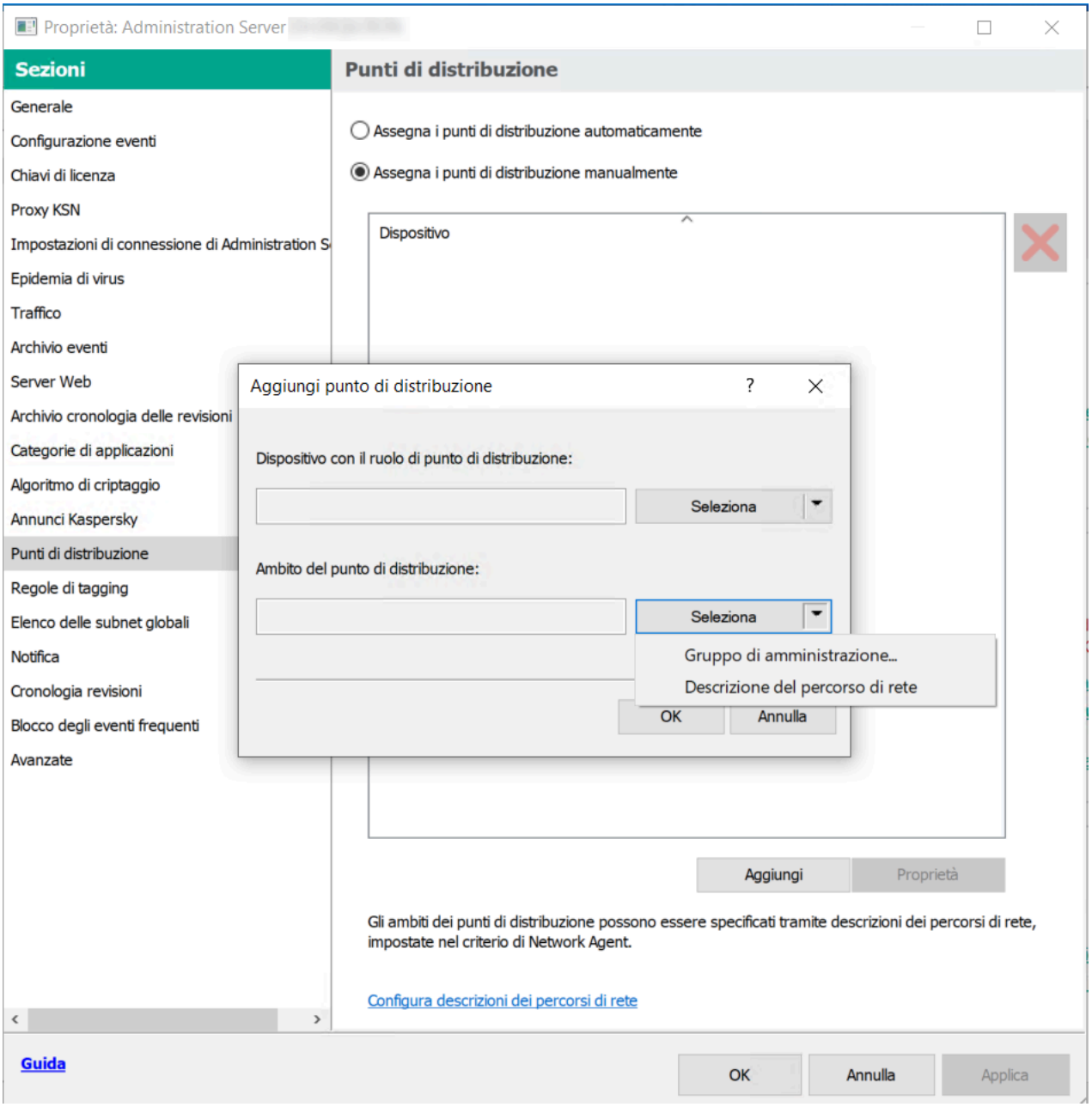
   a. In **Dispositivo con il ruolo di punto di distribuzione** fare clic sulla freccia verso il basso (▾) sul pulsante di divisione **Seleziona** e selezionare l'opzione **Aggiungi dispositivo dal gruppo**.

   b. Nella finestra **Seleziona dispositivi** visualizzata selezionare il dispositivo che fungerà da punto di distribuzione.

   c. In **Ambito del punto di distribuzione**, fare clic sulla freccia verso il basso ▾ sul pulsante di divisione **Seleziona**.

   d. Indicare i dispositivi specifici a cui il punto di distribuzione distribuirà gli aggiornamenti. È possibile specificare un gruppo di amministrazione o una descrizione del percorso di rete.

e. Fare clic su **OK** per chiudere la finestra **Aggiungi punto di distribuzione**.



Selezione dell'ambito del punto di distribuzione

Il punto di distribuzione aggiunto sarà visualizzato nell'elenco dei punti di distribuzione, nella sezione **Punti di distribuzione**.

Al primo dispositivo in cui è installato Network Agent che si connette all'Administration Server virtuale verrà assegnato automaticamente il ruolo di punto di distribuzione e questo verrà configurato come gateway di connessione.

Collegamento di un dispositivo Linux come gateway nella rete perimetrale

Per connettere un dispositivo Linux come gateway nella rete perimetrale:

1. Scaricare e installare Network Agent nel dispositivo Linux.

2. Eseguire lo script post-installazione e seguire la procedura guidata per impostare la configurazione dell'ambiente locale. Nel prompt dei comandi eseguire il seguente comando:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Nel passaggio in cui viene richiesta la modalità di Network Agent scegliere l'opzione **Usa come gateway di connessione**.

4. In Administration Console basata su MMC, nel menu di scelta rapida di Administration Server selezionare **Proprietà**.

5. Nella finestra delle proprietà di Administration Server che verrà visualizzata selezionare la sezione **Punti di distribuzione**.

6. Nella parte destra della finestra **Punti di distribuzione** visualizzata:

   a. Selezionare l'opzione **Assegna i punti di distribuzione manualmente**.

   b. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Aggiungi punto di distribuzione**.

7. Nella finestra **Aggiungi punto di distribuzione** eseguire le seguenti azioni:

   a. In **Dispositivo con il ruolo di punto di distribuzione**, fare clic sulla freccia verso il basso (▾) sul pulsante di divisione **Seleziona**, quindi selezionare l'opzione **Aggiungi gateway di connessione nella rete perimetrale in base all'indirizzo**.

   b. In **Ambito del punto di distribuzione**, fare clic sulla freccia verso il basso ▾ sul pulsante di divisione **Seleziona**.

   c. Indicare i dispositivi specifici a cui il punto di distribuzione distribuirà gli aggiornamenti. È possibile specificare un gruppo di amministrazione.

   d. Fare clic su **OK** per chiudere la finestra **Aggiungi punto di distribuzione**.

8. Il punto di distribuzione aggiunto sarà visualizzato nell'elenco dei punti di distribuzione, nella sezione **Punti di distribuzione**.

9. Eseguire l'utilità klnagchk per verificare se è stata configurata correttamente una connessione a Kaspersky Security Center. Nel prompt dei comandi eseguire:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. Nel menu principale, accedere a Kaspersky Security Center e individuare il dispositivo.

11. Nella finestra visualizzata fare clic sul <Nome dispositivo>.

12. Nell'elenco a discesa selezionare il collegamento **Sposta nel gruppo**.

13. Nella finestra **Seleziona gruppo** visualizzata fare clic sul collegamento **Punti di distribuzione**.

14. Fare clic su **OK**.

15. Riavviare il servizio Network Agent nel client Linux eseguendo il seguente comando nel prompt dei comandi:
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

Il collegamento di un dispositivo Linux come gateway nella rete perimetrale è stato completato.

Successivamente, è possibile connettere un dispositivo Linux ad Administration Server tramite il gateway di connessione configurato. Seguire queste procedure solo dopo aver completato lo scenario di installazione principale.

Collegamento di un dispositivo Linux ad Administration Server tramite un gateway di connessione

Un gateway di connessione consente di connettere i dispositivi client dalla rete perimetrale (DMZ) ad Administration Server. I dispositivi basati su Windows e Linux possono fungere da gateway di connessione. Dopo aver connesso e configurato il gateway di connessione, è possibile utilizzare questo gateway per connettere un dispositivo Linux ad Administration Server. Seguire la procedura riportata di seguito solo dopo aver completato lo scenario di installazione principale.

Per connettere un dispositivo Linux ad Administration Server tramite un gateway di connessione, eseguire le seguenti azioni in questo dispositivo:

1. Scaricare e installare Network Agent nel dispositivo Linux.

2. Eseguire lo script post-installazione di Network Agent eseguendo il seguente comando nel prompt dei comandi:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Nel passaggio in cui viene richiesta la modalità di Network Agent scegliere l'opzione **Esegui la connessione al server utilizzando il gateway di connessione** e immettere l'indirizzo del gateway di connessione.

4. Verificare la connessione con Kaspersky Security Center e il gateway di connessione utilizzando il seguente comando nel prompt dei comandi:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   L'indirizzo del gateway di connessione viene visualizzato nell'output.

La connessione di un dispositivo Linux ad Administration Server tramite un gateway di connessione è stata completata. È possibile utilizzare questo dispositivo per aggiornare la distribuzione, per l'installazione remota delle applicazioni e per recuperare informazioni sui dispositivi in rete.

Aggiunta di un gateway di connessione nella rete perimetrale come punto di distribuzione

Un gateway di connessione attende le connessioni da Administration Server anziché stabilire connessioni ad Administration Server. Questo significa che subito dopo l'installazione di un gateway di connessione in un dispositivo nella rete perimetrale, Administration Server non elenca il dispositivo tra i dispositivi gestiti. È pertanto necessaria una procedura speciale per garantire che Administration Server avvii una connessione al gateway di connessione.

Per aggiungere un dispositivo con un gateway di connessione come punto di distribuzione:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Nel menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server selezionare la sezione **Punti di distribuzione**.
4. Nella parte destra della finestra selezionare l'opzione **Assegna i punti di distribuzione manualmente**.
5. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Aggiungi punto di distribuzione**.
6. Nella finestra **Aggiungi punto di distribuzione** eseguire le seguenti azioni:

   a. In **Dispositivo con il ruolo di punto di distribuzione fare** clic sulla freccia verso il basso sul pulsante di divisione **Seleziona**, quindi selezionare l'opzione **Aggiungi gateway di connessione nella rete perimetrale in base all'indirizzo**.

   b. Nella finestra **Immettere l'indirizzo del gateway di connessione** visualizzata inserire l'indirizzo IP del gateway di connessione (o inserire il nome se il gateway di connessione è accessibile in base al nome).

   c. In **Ambito del punto di distribuzione**, fare clic sulla freccia verso il basso sul pulsante di divisione **Seleziona**.

   d. Indicare i dispositivi specifici a cui il punto di distribuzione distribuirà gli aggiornamenti. È possibile specificare un gruppo di amministrazione o una descrizione del percorso di rete.

      È consigliabile disporre di un gruppo separato per i dispositivi gestiti esterni.

Dopo l'esecuzione di queste azioni, l'elenco dei punti di distribuzione contiene una nuova voce denominata **Voce temporanea per il gateway di connessione**.

Administration Server tenta quasi immediatamente di connettersi al gateway di connessione all'indirizzo specificato. Se l'operazione va a buon fine, il nome della voce diventa il nome del dispositivo gateway di connessione. Questo processo richiede al massimo cinque minuti.

Mentre la voce temporanea per il gateway di connessione viene convertita in una voce denominata, il gateway di connessione viene visualizzato anche nel gruppo **Dispositivi non assegnati**.

Per aggiungere un gateway di connessione a una rete configurata in precedenza, reinstallare Network Agent nei dispositivi che si desidera connettere al gateway di connessione appena aggiunto.

Assegnazione automatica di punti di distribuzione

È consigliabile assegnare automaticamente i punti di distribuzione. Kaspersky Security Center selezionerà autonomamente a quali dispositivi assegnare i punti di distribuzione.

Per assegnare automaticamente i punti di distribuzione:

1. Aprire la finestra principale dell'applicazione.
2. Nella struttura della console selezionare il nodo con il nome dell'Administration Server per cui si desidera assegnare automaticamente i punti di distribuzione.
3. Dal menu di scelta rapida di Administration Server fare clic su **Proprietà**.
4. Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni** selezionare **Punti di distribuzione**.
5. Nella parte destra della finestra selezionare l'opzione **Assegna i punti di distribuzione automaticamente**.

   Se è abilitata l'assegnazione automatica dei dispositivi come punti di distribuzione, non è possibile configurare i punti di distribuzione manualmente, né modificare l'elenco dei punti di distribuzione.

6. Fare clic su **OK**.

Administration Server assegna e configura i punti di distribuzione automaticamente.

Informazioni sull'installazione locale di Network Agent in un dispositivo selezionato come punto di distribuzione

Per consentire al dispositivo selezionato come punto di distribuzione di comunicare direttamente con l'Administration Server virtuale per operare come gateway di connessione, Network Agent deve essere installato in locale nel dispositivo.

La procedura per l'installazione locale di Network Agent in un dispositivo definito come punto di distribuzione è identica a quella per l'installazione locale di Network Agent in qualsiasi dispositivo della rete.

Un dispositivo selezionato come punto di distribuzione deve soddisfare le seguenti condizioni:

- Durante l'installazione locale di Network Agent, specificare l'indirizzo di un Administration Server virtuale che gestisce il dispositivo nel campo **Indirizzo server** nella finestra dell'Installazione guidata di **Administration Server**. È possibile utilizzare sia l'indirizzo IP che il nome del dispositivo nella rete Windows.

  Per l'indirizzo dell'Administration Server virtuale viene utilizzato il seguente formato: <Indirizzo completo dell'Administration Server fisico che controlla il server virtuale>/<Nome dell'Administration Server virtuale>.

- In modo che possa operare come gateway di connessione, aprire tutte le porte del dispositivo necessarie per la comunicazione con l'Administration Server.

Dopo l'installazione nel dispositivo di Network Agent con le impostazioni specificate, Kaspersky Security Center esegue automaticamente le seguenti operazioni:

- Include il dispositivo nel gruppo **Dispositivi gestiti** dell'Administration Server virtuale.
- Assegna a questo dispositivo il ruolo di punto di distribuzione del gruppo **Dispositivi gestiti** dell'Administration Server virtuale.

È necessario (e sufficiente) eseguire l'installazione locale di Network Agent nel dispositivo a cui è assegnato il ruolo di punto di distribuzione per il gruppo **Dispositivi gestiti** nella rete dell'organizzazione. È possibile installare in remoto Network Agent nei dispositivi che operano come punti di distribuzione nei gruppi di amministrazione nidificati. A tale scopo, utilizzare il punto di distribuzione del gruppo **Dispositivi gestiti** come gateway di connessione.

Informazioni sull'utilizzo di un punto di distribuzione come gateway di connessione

Se l'Administration Server è esterno alla rete perimetrale (DMZ), i Network Agent appartenenti alla rete non potranno connettersi all'Administration Server.

Durante la connessione dell'Administration Server ai Network Agent, è possibile utilizzare un punto di distribuzione come gateway di connessione. Il punto di distribuzione apre una porta per stabilire la connessione ad Administration Server. Dopo l'avvio, l'Administration Server si connette a tale punto di distribuzione e mantiene la connessione per tutta la durata della sessione.

Alla ricezione di un segnale dall'Administration Server, il punto di distribuzione invia un segnale UDP ai Network Agent per consentire la connessione all'Administration Server. Quando i Network Agent ricevono il segnale, si connettono al punto di distribuzione, che provvede al trasferimento delle informazioni fra i Network Agent e Administration Server. Lo scambio di informazioni può avvenire su una rete IPv4 o IPv6.

È consigliabile utilizzare un dispositivo appositamente assegnato come gateway di connessione e coprire un massimo di 10.000 dispositivi client (compresi i dispositivi mobili) con il gateway di connessione.

Per aggiungere un gateway di connessione a una rete configurata in precedenza:

1. Installare Network Agent in modalità gateway di connessione.
2. Reinstallare Network Agent nei dispositivi che si desidera connettere al gateway di connessione appena aggiunto.

Aggiunta di intervalli IP all'elenco di intervalli sottoposti a polling da un punto di distribuzione

È possibile aggiungere un intervallo IP all'elenco degli intervalli sottoposti a polling da un punto di distribuzione.

Per aggiungere un intervallo IP all'elenco degli intervalli sottoposti a polling:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Nel menu di scelta rapida del nodo selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server che verrà visualizzata selezionare la sezione **Punti di distribuzione**.
4. Nell'elenco selezionare il punto di distribuzione desiderato e fare clic su **Proprietà**.
5. Nella finestra delle proprietà del punto di distribuizione visualizzata, nel riquadro sinistro **Sezioni**, selezionare **Device discovery** → **Intervalli IP**.
6. Selezionare la casella di controllo **Abilita polling intervalli**.
7. Fare clic sul pulsante **Aggiungi**.

   Il pulsante **Aggiungi** è attivo solo se si seleziona la casella di controllo **Abilita polling intervalli**.

   Verrà visualizzata la finestra **Intervallo IP**.
8. Nella finestra **Intervallo IP** immettere il nome del nuovo intervallo IP (il nome predefinito è Nuovo intervallo).
9. Fare clic sul pulsante **Aggiungi**.
10. Eseguire una delle seguenti operazioni:
    - Specificare l'intervallo IP utilizzando gli indirizzi iniziale e finale.
    - Specificare l'intervallo IP utilizzando l'indirizzo e la subnet mask.
    - Fare clic su **Sfoglia** e aggiungere una subnet dall'elenco globale delle subnet.
11. Fare clic su **OK**.
12. Fare clic su **OK** per aggiungere il nuovo intervallo con il nome specificato.

Il nuovo intervallo verrà visualizzato nell'elenco degli intervalli sottoposti a polling.

Utilizzo di un punto di distribuzione come server push

In Kaspersky Security Center un punto di distribuzione può fungere da server push per i dispositivi gestiti tramite il protocollo mobile e per i dispositivi gestiti da Network Agent. È ad esempio necessario abilitare un server push se si desidera forzare la sincronizzazione dei dispositivi KasperskyOS con Administration Server. Un server push ha lo stesso ambito dei dispositivi gestiti del punto di distribuzione in cui è abilitato il server push. Se sono stati assegnati più punti di distribuzione per lo stesso gruppo di amministrazione, è possibile abilitare il server push in ciascuno dei punti di distribuzione. In questo caso, Administration Server bilancia il carico tra i punti di distribuzione.

Un server push supporta il carico massimo di 50.000 connessioni simultanee.

È consigliabile utilizzare i punti di distribuzione come server push per garantire la continuità della connessione tra un dispositivo gestito e Administration Server. La continuità della connessione è necessaria per alcune operazioni, come l'esecuzione e l'arresto di attività locali, la ricezione di statistiche per un'applicazione gestita o la creazione di un tunnel. Se si utilizza un punto di distribuzione come server push, non è necessario utilizzare l'opzione **Non eseguire la disconnessione da Administration Server** nei dispositivi gestiti o inviare pacchetti alla porta UDP di Network Agent.

Per utilizzare un punto di distribuzione come server push:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Nel menu di scelta rapida del nodo selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server che verrà visualizzata selezionare la sezione **Punti di distribuzione**.
4. Nell'elenco selezionare il punto di distribuzione desiderato e fare clic su **Proprietà**.
5. Nella finestra delle proprietà del punto di distribuzione visualizzata, nella sezione **Generale** del riquadro **Sezioni** a sinistra, selezionare l'opzione **Usa questo punto di distribuzione come server push**.
6. Specificare il numero di porta del server push, cioè la porta nel punto di distribuzione che i dispositivi client utilizzeranno per la connessione.

   Per impostazione predefinita, viene utilizzata la porta 13295.
7. Fare clic sul pulsante **OK** per chiudere la finestra delle proprietà del punto di distribuzione.
8. Aprire la finestra delle impostazioni del criterio di Network Agent.
9. Nella sezione **Connettività** passare alla sottosezione **Rete**.
10. Nella sottosezione **Rete** selezionare l'opzione **Usa punto di distribuzione per forzare la connessione ad Administration Server**.
11. Fare clic sul pulsante **OK** per chiudere la finestra.

Il punto di distribuzione inizia a operare come server push. Adesso può inviare notifiche push ai dispositivi client.

Se si gestiscono dispositivi in cui è installato KasperskyOS o si prevede di farlo, è necessario utilizzare un punto di distribuzione come server push. È inoltre possibile utilizzare un punto di distribuzione come server push se si desidera inviare notifiche push ai dispositivi client.

Altre operazioni di routine

Questa sezione fornisce raccomandazioni sul funzionamento di routine di Kaspersky Security Center.

Gestione degli Administration Server

Questa sezione fornisce informazioni sull'utilizzo e sulla configurazione degli Administration Server.

Creazione di una gerarchia di Administration Server: l'aggiunta un Administration Server secondario

È possibile aggiungere un Administration Server come Administration Server secondario, configurando una gerarchia "primario/secondario". L'aggiunta di un Administration Server secondario è possibile indipendentemente dal fatto che l'Administration Server che si prevede di utilizzare come secondario sia disponibile per la connessione tramite Administration Console.

Quando si combinano due Administration Server in una gerarchia, verificare che la porta 13291 sia accessibile in entrambi gli Administration Server. La porta 13291 è necessaria per ricevere le connessioni da Administration Console ad Administration Server.

Connessione di un Administration Server come secondario in riferimento all'Administration Server primario

È possibile aggiungere un Administration Server come secondario connettendolo all'Administration Server primario tramite la porta 13000. Sarà necessario un dispositivo in cui è installato Administration Console da cui è possibile accedere alle porte TCP 13291 in entrambi gli Administration Server: presunto Administration Server primario e presunto Administration Server secondario.

Per aggiungere come secondario un Administration Server disponibile per la connessione tramite Administration Console:

1. Verificare che la porta 13000 del presunto Administration Server primario sia disponibile per la ricezione delle connessioni dagli Administration Server secondari.
2. Utilizzare Administration Console per eseguire la connessione al presunto Administration Server primario.
3. Selezionare il gruppo di amministrazione a cui si desidera aggiungere l'Administration Server secondario.
4. Nell'area di lavoro del nodo **Administration Server** del gruppo selezionato fare clic sul collegamento **Aggiungi Administration Server secondario**.

   Verrà avviata l'Aggiunta guidata Administration Server secondari.
5. Nel primo passaggio della procedura guidata (immissione dell'indirizzo dell'Administration Server aggiunto al gruppo), immettere il nome di rete del presunto Administration Server secondario.
6. Seguire le istruzioni della procedura guidata.

Verrà creata la gerarchia "primario/secondario". L'Administration Server primario riceverà la connessione dall'Administration Server secondario.

Se non si dispone di un dispositivo in cui è installato Administration Console da cui è possibile accedere alle porte TCP 13291 in entrambi gli Administration Server (se ad esempio il presunto Administration Server secondario è situato in una sede remota e l'amministratore di sistema di tale sede non può aprire l'accesso a Internet alla porta 13291 per motivi di sicurezza), sarà comunque possibile aggiungere un Administration Server secondario.

Per aggiungere come secondario un Administration Server non disponibile per la connessione tramite Administration Console:

1. Verificare che la porta 13000 del presunto Administration Server primario sia disponibile per la connessione dagli Administration Server secondari.

2. Scrivere il file di certificato del presunto Administration Server primario in un dispositivo esterno, ad esempio un'unità flash, o inviarlo all'amministratore di sistema della sede remota in cui si trova Administration Server.

   Il file di certificato dell'Administration Server si trova nello stesso Administration Server, in%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Scrivere il file di certificato del presunto Administration Server secondario in un dispositivo esterno, ad esempio un'unità flash. Se il presunto Administration Server secondario è situato in una sede remota, contattare l'amministratore di sistema di tale sede per richiedergli di inviare il certificato.

   Il file di certificato dell'Administration Server si trova nello stesso Administration Server, in%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. Utilizzare Administration Console per eseguire la connessione al presunto Administration Server primario.

5. Selezionare il gruppo di amministrazione a cui si desidera aggiungere l'Administration Server secondario.

6. Nell'area di lavoro del nodo **Administration Server** fare clic sul collegamento **Aggiungi Administration Server secondario**.

   Verrà avviata l'Aggiunta guidata Administration Server secondari.

7. Nel primo passaggio della procedura guidata (immissione dell'indirizzo) lasciare vuoto il campo **Indirizzo dell'Administration Server secondario (facoltativo)**.

8. Nella finestra **File di certificato dell'Administration Server secondario** fare clic sul pulsante **Sfoglia** e selezionare il file di certificato dell'Administration Server secondario salvato.

9. Al termine della procedura guidata, utilizzare un'istanza diversa di Administration Console per connettersi al presunto Administration Server secondario. Se tale Administration Server è situato in una sede remota, contattare l'amministratore di sistema di tale sede per richiedere la connessione al presunto Administration Server secondario ed eseguire i passaggi successivi previsti.

10. Dal menu di scelta rapida del nodo **Administration Server** selezionare **Proprietà**.

11. Nelle proprietà di Administration Server passare alla sezione **Avanzate** e quindi alla sottosezione **Gerarchia di Administration Server**.

12. Selezionare la casella di controllo **Questo Administration Server è secondario nella gerarchia**.

    I campi di immissione diventano disponibili per l'immissione e la modifica dei dati.

13. Nel campo **Indirizzo Administration Server primario** immettere il nome della rete del presunto Administration Server primario.

14. Selezionare il file precedentemente salvato con il certificato del presunto Administration Server primario facendo clic sul pulsante **Sfoglia**.

15. Fare clic su **OK**.

Verrà creata la gerarchia "primario/secondario". È possibile connettersi all'Administration Server secondario tramite Administration Console. L'Administration Server primario riceverà la connessione dall'Administration Server secondario.

Connessione dell'Administration Server primario a un Administration Server secondario

È possibile aggiungere un nuovo Administration Server come secondario in modo che l'Administration Server primario si connetta all'Administration Server secondario tramite la porta 13000. È consigliabile eseguire questa operazione se, ad esempio, si posiziona un Administration Server secondario nella rete perimetrale.

Sarà necessario un dispositivo in cui è installato Administration Console da cui è possibile accedere alle porte TCP 13291 in entrambi gli Administration Server: presunto Administration Server primario e presunto Administration Server secondario.

Per aggiungere un nuovo Administration Server come secondario e connetterlo all'Administration Server primario tramite la porta 13000:

1. Verificare che la porta 13000 del presunto Administration Server secondario sia disponibile per la ricezione delle connessioni dall'Administration Server primario.

2. Utilizzare Administration Console per eseguire la connessione al presunto Administration Server primario.

3. Selezionare il gruppo di amministrazione a cui si desidera aggiungere l'Administration Server secondario.

4. Nell'area di lavoro del nodo **Administration Server** del gruppo di amministrazione attinente fare clic sul collegamento **Aggiungi Administration Server secondario**.

   Verrà avviata l'Aggiunta guidata Administration Server secondari.

5. Nel primo passaggio della procedura guidata (immissione dell'indirizzo dell'Administration Server da aggiungere al gruppo) immettere il nome della rete del presunto Administration Server secondario e selezionare la casella di controllo **Connetti l'Administration Server primario all'Administration Server secondario nella rete perimetrale**.

6. Se si esegue la connessione al presunto Administration Server secondario utilizzando un server proxy, durante il primo passaggio della procedura guidata selezionare la casella di controllo **Usa server proxy** e specificare le impostazioni di connessione.

7. Seguire le istruzioni della procedura guidata.

Verrà creata la gerarchia di Administration Server. L'Administration Server secondario riceverà la connessione dall'Administration Server primario.

Connessione a un Administration Server e passaggio da un Administration Server all'altro

Dopo l'avvio, Kaspersky Security Center tenta di connettersi a un Administration Server. Se sono disponibili diversi Administration Server nella rete, l'applicazione richiede quello a cui è stata eseguita la connessione durante la sessione precedente di Kaspersky Security Center.

Se l'applicazione viene avviata per la prima volta dopo l'installazione, tenta di connettersi all'Administration Server specificato durante l'installazione di Kaspersky Security Center.

Una volta stabilita la connessione a un Administration Server, la struttura delle cartelle di tale server viene visualizzata nella struttura della console.

Se alla struttura della console sono stati aggiunti diversi Administration Server, è possibile passare da uno all'altro.

Administration Console è necessario per l'utilizzo di ogni Administration Server. Prima della prima connessione a un nuovo Administration Server, verificare che la porta 13291, utilizzata per ricevere le connessioni da Administration Console, sia aperta, così come tutte le porte rimanenti necessarie per la comunicazione tra Administration Server e gli altri componenti di Kaspersky Security Center.

Per passare a un Administration Server diverso:

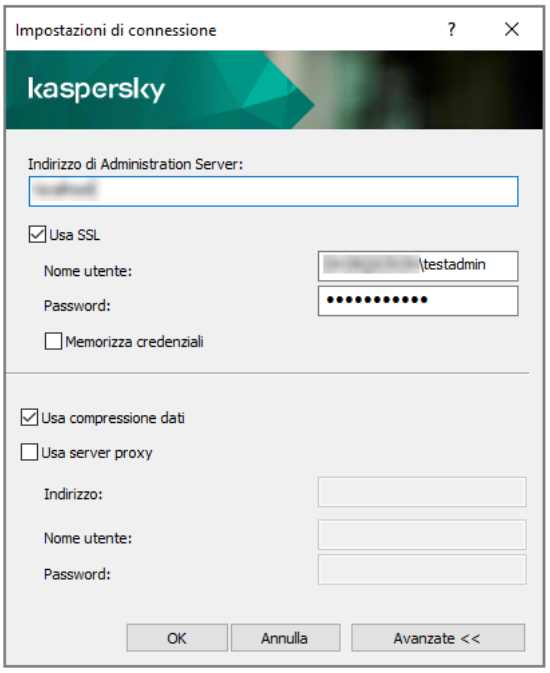
1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nel menu di scelta rapida del nodo selezionare **Connetti ad Administration Server**.

3. Nella finestra **Impostazioni di connessione** visualizzata specificare nel campo **Indirizzo di Administration Server** il nome dell'Administration Server a cui si desidera connettersi. È possibile specificare un indirizzo IP o il nome di un dispositivo in una rete Windows come nome dell'Administration Server. È possibile fare clic sul pulsante **Avanzate** per configurare la connessione ad Administration Server (vedere la figura seguente).

   Per connettersi ad Administration Server tramite una porta diversa da quella predefinita, immettere un valore nel campo **Indirizzo di Administration Server** nel formato <Nome Administration Server>:<Porta>.

   Per connettersi a un Administration Server virtuale, immettere un valore nel campo **Indirizzo di Administration Server** nel formato <indirizzo di Administration Server>/<nome server virtuale>.

   L'accesso ad Administration Server non è consentito agli utenti che non dispongono dei diritti di **Lettura**.



Connessione ad Administration Server

4. Fare clic su **OK** per completare il passaggio tra i server.

   Dopo la connessione ad Administration Server, viene aggiornata la struttura delle cartelle del nodo corrispondente nella struttura della console.

Diritti di accesso ad Administration Server e ai relativi oggetti

Durante l'installazione di Kaspersky Security Center vengono creati automaticamente i gruppi **KLAdmins** e **KLOperators**. A questi gruppi vengono concesse le autorizzazioni per la connessione ad Administration Server e per l'elaborazione dei relativi oggetti.

A seconda del tipo di account utilizzato per l'installazione di Kaspersky Security Center, i gruppi **KLAdmins** e **KLOperators** vengono creati come segue:

- Se l'applicazione è installata tramite un account utente incluso in un dominio, i gruppi vengono creati sia nel dominio che include l'Administration Server che nell'Administration Server stesso.
- Se l'applicazione è installata tramite un account di sistema, i gruppi vengono creati soltanto nell'Administration Server.

È possibile visualizzare i gruppi **KLAdmins** e **KLOperators** e modificare i privilegi di accesso degli utenti che appartengono ai gruppi **KLAdmins** e **KLOperators** utilizzando gli strumenti di amministrazione standard del sistema operativo.

Al gruppo **KLAdmins** sono concessi tutti i diritti di accesso, mentre al gruppo **KLOperators** vengono concessi soltanto i diritti di lettura ed esecuzione. I diritti concessi al gruppo **KLAdmins** sono bloccati.

Gli utenti appartenenti al gruppo **KLAdmins** sono denominati *Amministratori di Kaspersky Security Center*, gli utenti del gruppo **KLOperators** sono denominati *Operatori di Kaspersky Security Center*.

Oltre che agli utenti inclusi nel gruppo **KLAdmins**, i diritti di amministratore di Kaspersky Security Center vengono concessi agli amministratori locali dei dispositivi in cui è installato Administration Server.

Gli amministratori locali possono essere esclusi dall'elenco degli utenti che dispongono di diritti di amministratore di Kaspersky Security Center.

Tutte le operazioni avviate dagli amministratori di Kaspersky Security Center verranno eseguite utilizzando i diritti dell'account di Administration Server.

Per ciascun Administration Server della rete è possibile creare uno specifico gruppo **KLAdmins**, che disporrà dei diritti necessari solo per tale Administration Server.

Se si includono dispositivi appartenenti allo stesso dominio in gruppi di amministrazione di differenti Administration Server, l'amministratore del dominio sarà un amministratore di Kaspersky Security Center per tutti i gruppi. Il gruppo **KLAdmins** è lo stesso per questi gruppi di amministrazione e viene creato durante l'installazione del primo Administration Server. Tutte le operazioni avviate dall'amministratore di Kaspersky Security Center vengono eseguite utilizzando i diritti dell'account dell'Administration Server per cui sono state avviate tali operazioni.

In seguito all'installazione dell'applicazione, un amministratore di Kaspersky Security Center può eseguire le seguenti operazioni:

- Modificare i diritti concessi ai gruppi **KLOperators**.
- Concedere i diritti di accesso alle funzionalità di Kaspersky Security Center ad altri utenti e gruppi di sicurezza registrati sulla workstation dell'amministratore.
- Assegnare diritti di accesso utente in ogni gruppo di amministrazione.

L'amministratore di Kaspersky Security Center può assegnare diritti di accesso a ogni gruppo di amministrazione o ad altri oggetti di Administration Server nella sezione **Protezione** della finestra delle proprietà dell'oggetto selezionato.

È possibile tracciare l'attività dell'utente utilizzando i record sugli eventi durante l'esecuzione di Administration Server. I record degli eventi sono visualizzati nel nodo **Administration Server** della scheda **Eventi**. Questi eventi hanno livello di importanza **Eventi informativi** e i tipi di eventi iniziano con "**Controllo**".

Condizioni per la connessione a un Administration Server tramite Internet

Se un Administration Server è remoto, ovvero all'esterno di una rete aziendale, i dispositivi client vi si connettono tramite Internet.

Per la connessione dei dispositivi client a un Administration Server via Internet, devono essere soddisfatte le seguenti condizioni:

- L'Administration Server remoto deve disporre di un indirizzo IP esterno e la porta in entrata 13000 deve rimanere aperta (per la connessione dei Network Agent). È consigliabile aprire anche la porta UDP 13000 (per la ricezione delle notifiche sullo spegnimento dei dispositivi).
- I Network Agent devono essere installati nei dispositivi.
- Quando si installa Network Agent nei dispositivi, è necessario specificare l'indirizzo IP esterno dell'Administration Server remoto. Se per l'installazione viene utilizzato un pacchetto di installazione, l'indirizzo IP esterno deve essere specificato manualmente nelle proprietà del pacchetto di installazione, nella sezione **Impostazioni**.
- Per utilizzare l'Administration Server remoto al fine di gestire le applicazioni e le attività di un dispositivo, nella sezione **Generale** della finestra delle proprietà di tale dispositivo selezionare la casella di controllo **Non eseguire la disconnessione da Administration Server**. Dopo avere selezionato la casella di controllo, attendere la sincronizzazione di Administration Server con il dispositivo remoto. Il numero di dispositivi client che mantengono una connessione permanente con un Administration Server non può essere superiore a 300.

Per aumentare le prestazioni delle attività generate da un Administration Server remoto, è possibile aprire la porta 15000 in un dispositivo. In questo caso, per eseguire un'attività, l'Administration Server invia uno speciale pacchetto a Network Agent tramite la porta 15000 senza attendere il completamento della sincronizzazione con il dispositivo.

Connessione criptata a un Administration Server

Sia lo scambio dei dati tra i dispositivi client e Administration Server che la connessione di Administration Console ad Administration Server possono essere eseguiti tramite il protocollo TLS (Transport Layer Security). Il protocollo TLS consente l'identificazione delle parti che interagiscono, il criptaggio dei dati trasferiti e la loro protezione dalle modifiche durante il trasferimento. Il protocollo TLS utilizza chiavi pubbliche per l'autenticazione delle parti che interagiscono e per il criptaggio dei dati.

Autenticazione dell'Administration Server quando un dispositivo è connesso

Quando un dispositivo client si connette ad Administration Server per la prima volta, Network Agent nel dispositivo scarica una copia del certificato di Administration Server e la salva in locale.

> Se si installa Network Agent su un dispositivo in locale, è possibile selezionare manualmente il certificato di Administration Server.

La copia scaricata del certificato viene utilizzata per verificare i diritti e le autorizzazioni di Administration Server durante le connessioni successive.

Durante le sessioni successive, Network Agent richiede il certificato di Administration Server a ogni connessione del dispositivo al server e lo confronta con la copia locale. Se le copie non corrispondono, l'accesso del dispositivo ad Administration Server non è consentito.

Autenticazione di Administration Server durante la connessione di Administration Console

Durante la prima connessione ad Administration Server, Administration Console richiede il certificato di Administration Server e lo salva in locale nella workstation dell'amministratore. In seguito, ogni volta che Administration Console tenta di connettersi ad Administration Server, quest'ultimo viene identificato in base alla copia del certificato.

Se il certificato di Administration Server non corrisponde alla copia memorizzata nella workstation dell'amministratore, Administration Console richiede di confermare la connessione ad Administration Server con il nome specificato e di scaricare un nuovo certificato. Una volta stabilita la connessione, Administration Console salva una copia del nuovo certificato di Administration Server, che verrà utilizzata per identificare Administration Server in futuro.

Configurazione di una lista di indirizzi IP consentiti per la connessione ad Administration Server

Per impostazione predefinita, gli utenti possono accedere a Kaspersky Security Center da qualsiasi dispositivo in cui possono aprire Kaspersky Security Center Web Console (di seguito denominato Web Console) o in cui è installata Administration Console basata su MMC. Tuttavia, è possibile configurare Administration Server in modo che gli utenti possano connettersi ad esso solo da dispositivi con indirizzi IP consentiti. In questo caso, anche se un utente malintenzionato ruba un account Kaspersky Security Center, egli non sarà in grado di accedere a Kaspersky Security Center perché l'indirizzo IP del suo dispositivo non è presente nella lista consentiti.

L'indirizzo IP viene verificato quando un utente accede a Kaspersky Security Center o esegue un'applicazione che interagisce con Administration Server tramite Kaspersky Security Center OpenAPI. In questo momento, il dispositivo di un utente tenta di stabilire una connessione con Administration Server. Se l'indirizzo IP del dispositivo non è presente nella lista consentiti, si verifica un errore di autenticazione e l'evento KLAUD_EV_SERVERCONNECT informa l'utente che non è stata stabilita una connessione con Administration Server.

Requisiti per una lista di indirizzi IP consentiti

Gli indirizzi IP vengono verificati solo quando le seguenti applicazioni tentano di connettersi ad Administration Server:

- Web Console Server

  Se si accede a Web Console su un dispositivo e Web Console Server è installato in un altro dispositivo, è possibile configurare un firewall sul dispositivo in cui è installato Web Console Server utilizzando gli strumenti standard del sistema operativo. Quindi, se qualcuno tenta di accedere a Web Console, un firewall contribuisce a prevenire l'interferenza di intrusi.

- Administration Console
- Applicazioni che interagiscono con Administration Server tramite oggetti di automazione klakaut
- Applicazioni che interagiscono con Administration Server tramite OpenAPI, come Kaspersky Anti Targeted Attack Platform o Kaspersky Security for Virtualization

Specificare quindi gli indirizzi dei dispositivi in cui sono installate le applicazioni sopra elencate.

È possibile impostare indirizzi IPv4 e IPv6. Non è possibile specificare intervalli di indirizzi IP.

Come stabilire una lista di indirizzi IP consentiti

Se non è stata impostata una lista consentiti in precedenza, seguire le istruzioni di seguito.

Per stabilire una lista di indirizzi IP consentiti per accedere a Kaspersky Security Center:

1. Nel dispositivo Administration Server eseguire il prompt dei comandi con un account che disponga dei diritti di amministratore.

2. Sostituire la directory corrente con la cartella di installazione di Kaspersky Security Center (in genere, <Disco>:\Programmi (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Immettere il comando seguente, utilizzando i diritti di amministratore:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<Indirizzi IP>" -t s`

   Specificare gli indirizzi IP che soddisfano i requisiti sopra elencati. I diversi indirizzi IP devono essere separati da un punto e virgola.

   Esempio di come consentire a un solo dispositivo di connettersi ad Administration Server:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Esempio di come consentire a più dispositivi di connettersi ad Administration Server:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 198.51.100.0; 203.0.113.0" -t s`

4. Riavviare il servizio Administration Server.

È possibile verificare se è stata configurata correttamente la lista di indirizzi IP consentiti nel Registro eventi Kaspersky in Administration Server.

Come modificare una lista di indirizzi IP consentiti

È possibile modificare una lista consentiti seguendo i passaggi previsti per la relativa creazione. A tale scopo, eseguire lo stesso comando e specificare una nuova lista consentiti:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<Indirizzi IP>" -t s
```

Se si desidera eliminare alcuni indirizzi IP dalla lista consentiti, riscriverla. Ad esempio, la lista consentiti include i seguenti indirizzi IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. Si desidera eliminare l'indirizzo IP 198.51.100.0. A tale scopo, immettere il seguente comando nel prompt dei comandi:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Non dimenticare di riavviare il servizio Administration Server.

Come reimpostare una lista di indirizzi IP consentiti configurata

Per reimpostare una lista di indirizzi IP consentiti già configurata:

1. Immettere il seguente comando nel prompt dei comandi, utilizzando i diritti di amministratore:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Riavviare il servizio Administration Server.

Successivamente, gli indirizzi IP non vengono più verificati.

Utilizzo dell'utilità klscflag per chiudere la porta 13291

La porta 13291 nell'Administration Server viene utilizzata per ricevere connessioni da Administration Console. Questa porta è aperta per impostazione predefinita. Se non si desidera utilizzare la Administration Console basata su MMC o l'utilità klakaut, è possibile chiudere questa porta utilizzando l'utilità klscflag. Questa utilità modifica il valore del parametro KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Per chiudere la porta 13291:

1. Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

2. Eseguire il comando seguente nella riga di comando:
   `klscflag -ssvset -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`

3. Riavviare il servizio Kaspersky Security Center Administration Server.

   La porta 13291 è chiusa.

Per verificare se la porta 13291 è stata chiusa correttamente:

Eseguire il comando seguente nella riga di comando:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Questo comando restituisce il seguente risultato:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

Il valore `false` indica che la porta è chiusa. In caso contrario, viene visualizzato il valore `true`.

Disconnessione da un Administration Server

Per disconnettersi da un Administration Server:

1. Nella struttura della console selezionare il nodo che corrisponde all'Administration Server da disconnettere.

2. Nel menu di scelta rapida del nodo selezionare **Disconnetti da Administration Server**.

Aggiunta di un Administration Server alla struttura della console

Per aggiungere un Administration Server alla struttura della console:

1. Nella finestra principale di Kaspersky Security Center selezionare nella struttura della console il nodo **Kaspersky Security Center**.
2. Nel menu di scelta rapida del nodo selezionare **Nuovo → Administration Server**.

Nella struttura della console viene creato un nodo denominato **Administration Server - <nome dispositivo> (Non connesso)**, da cui sarà possibile connettersi a qualsiasi Administration Server nella rete.

Rimozione di un Administration Server dalla struttura della console

Per rimuovere un Administration Server dalla struttura della console:

1. Nella struttura della console selezionare il nodo che corrisponde all'Administration Server da rimuovere.
2. Nel menu di scelta rapida del nodo selezionare **Rimuovi**.

Aggiunta di un Administration Server virtuale alla struttura della console

Per aggiungere un Administration Server virtuale alla struttura della console:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server per cui è necessario creare un Administration Server virtuale.
2. Nel nodo Administration Server selezionare la cartella **Administration Server**.
3. Nell'area di lavoro della cartella **Administration Server** fare clic sul collegamento **Aggiungi Administration Server virtuale**.

   Verrà avviata l'Aggiunta guidata nuovo Administration Server virtuale.
4. Nella finestra **Nome Administration Server virtuale** specificare il nome dell'Administration Server virtuale da creare.

   Il nome di un Administration Server virtuale non può superare i 255 caratteri e non può includere caratteri speciali (ad esempio "*<>?\:|).

5. Nella finestra **Immettere l'indirizzo per la connessione del dispositivo all'Administration Server virtuale** specificare l'indirizzo di connessione del dispositivo

   L'indirizzo di connessione di un Administration Server virtuale è l'indirizzo di rete attraverso il quale i dispositivi si connetteranno al Server. L'indirizzo di connessione comprende due parti: l'indirizzo di rete di un Administration Server fisico e il nome di un Administration Server virtuale, separati da una barra. Il nome dell'Administration Server virtuale verrà sostituito automaticamente. L'indirizzo specificato verrà utilizzato nell'Administration Server virtuale come indirizzo predefinito nei pacchetti di installazione di Network Agent.

6. Nella finestra **Creare l'account amministratore dell'Administration Server virtuale** assegnare a un utente dell'elenco il ruolo di amministratore del Server virtuale oppure aggiungere un nuovo account amministratore facendo clic sul pulsante **Crea**.

   È possibile specificare più account.

Nella struttura della console viene creato un nodo denominato **Administration Server <nome dell'Administration Server virtuale>**.

Modifica di un account del servizio di Administration Server. Utilità klsrvswch

Se è necessario modificare l'account del servizio di Administration Server impostato durante l'installazione di Kaspersky Security Center, è possibile utilizzare un'utilità denominata klsrvswch progettata per la modifica dell'account di Administration Server.

Durante l'installazione di Kaspersky Security Center, l'utilità viene copiata automaticamente nella cartella di installazione dell'applicazione.

È possibile avviare l'utilità un numero di volte illimitato.

> È necessario avviare l'utilità klsrvswch nel dispositivo Administration Server con l'account con diritti di amministratore utilizzato per installare Administration Server.

L'utilità klsrvswch consente di modificare il tipo di account. Se ad esempio si utilizza un account locale, è possibile modificarlo in un account di dominio o in un account del servizio gestito (e viceversa). L'utilità klsrvswch non consente di modificare il tipo di account in account del servizio gestito di gruppo (gMSA).

> In Windows Vista e nelle versioni successive di Windows non è possibile utilizzare un account LocalSystem per Administration Server. In queste versioni di Windows l'opzione di **Account LocalSystem** è inattiva.

Per modificare un account del servizio di Administration Server in un account di dominio:

1. Avviare l'utilità klsrvswch dalla cartella di installazione di Kaspersky Security Center. Il percorso di installazione predefinito: <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Questa azione avvia la procedura guidata per la modifica dell'account del servizio di Administration Server. Seguire le istruzioni della procedura guidata.

2. Nella finestra **Account del servizio di Administration Server** selezionare **Account LocalSystem**.

Al termine della procedura guidata, la modifica dell'account Administration Server viene completata. Il servizio Administration Server verrà avviato tramite l'*account LocalSystem* e utilizzando le relative credenziali.

Per il corretto funzionamento di Kaspersky Security Center, l'account utilizzato per avviare il servizio Administration Server deve disporre di diritti di amministratore per la risorsa in cui è contenuto il database di Administration Server.

Per modificare un account del servizio di Administration Server in un account utente o un account del servizio gestito:

1. Avviare l'utilità klsrvswch dalla cartella di installazione di Kaspersky Security Center. Il percorso di installazione predefinito: <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   Questa azione avvia la procedura guidata per la modifica dell'account del servizio di Administration Server. Seguire le istruzioni della procedura guidata.

2. Nella finestra **Account del servizio di Administration Server** selezionare **Account personalizzato**.

3. Fare clic sul pulsante **Trova**.

   Verrà visualizzata la finestra **Seleziona utente**.

4. Nella finestra **Seleziona utente** fare clic sul pulsante **Tipi di oggetto**.

5. Nell'elenco dei tipi di oggetto selezionare **Utenti** (per un account utente) o **Account servizio** (per un account del servizio gestito) e fare clic su **OK**.

6. Nel campo Nome oggetto immettere il nome (o una parte del nome) dell'account e fare clic su **Controlla nomi**.

7. Nell'elenco dei nomi corrispondenti selezionare il nome desiderato, quindi fare clic su **OK**.

8. Se è stato selezionato **Account servizio**, nella finestra **Password account** lasciare vuoti i campi **Password** e **Conferma password**. Se è stato selezionato **Utenti**, immettere una nuova password per l'utente e confermarla.

L'account del servizio di Administration Server verrà modificato nell'account selezionato.

Quando si utilizza Microsoft SQL Server in una modalità che presuppone l'autenticazione degli account utente con gli strumenti di Microsoft Windows, deve essere concesso l'accesso al database. L'account utente deve avere lo stato di proprietario del database Kaspersky Security Center. Per impostazione predefinita, viene utilizzato lo schema dbo.

Modifica delle credenziali del DBMS

Potrebbe essere necessario modificare le credenziali del DBMS, ad esempio per eseguire una rotazione delle credenziali per motivi di sicurezza.

Per modificare le credenziali del DBMS in un ambiente Windows tramite l'utilità klsrvswch.exe:

1. Avviare l'utilità klsrvswch disponibile nella cartella di installazione di Kaspersky Security Center. Il percorso di installazione predefinito: <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

   È necessario avviare l'utilità klsrvswch nel dispositivo Administration Server con l'account con diritti di amministratore utilizzato per installare Administration Server.

2. Fare clic sul pulsante **Avanti** della procedura guidata fino al passaggio **Modifica credenziali di accesso DBMS**.

3. Al passaggio **Modifica credenziali di accesso DBMS** della procedura guidata, effettuare le seguenti operazioni:

   Il passaggio **Modifica credenziali di accesso DBMS** della procedura guidata viene ignorato se viene utilizzata l'autenticazione di Windows.

   - Selezionare l'opzione **Applica nuove credenziali**.
   - Specificare un nuovo nome per l'account nel campo **Account**.
   - Specificare una nuova password per l'account nel campo **Password**.
   - Specificare la nuova password nel campo **Conferma password**.

   È necessario specificare le credenziali di un account esistente nel DBMS.

4. Fare clic sul pulsante **Avanti**.

Al termine della procedura guidata, le credenziali del DBMS vengono modificate.

L'utilità klsrvswch può essere utilizzata solo per modificare la password dell'account per l'autenticazione SQL. La modifica del metodo di autorizzazione non è supportata. Per modificare il metodo di autorizzazione, reinstallare Administration Server e specificare le impostazioni desiderate.

Modifica della cartella condivisa di Administration Server

La cartella condivisa di Administration Server viene specificata durante l'installazione di Administration Server. È possibile modificare il percorso della cartella condivisa, nelle proprietà dell'Administration Server.

Per modificare la cartella condivisa:

1. Creare una cartella di condivisione di rete e configurare le autorizzazioni per la condivisione e la struttura delle cartelle per consentire il controllo completo per il sottogruppo **Tutti**.

2. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server** e selezionare **Proprietà**.

3. Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni**, selezionare **Avanzate**, quindi selezionare **Cartella condivisa di Administration Server**.

4. Nella sezione **Cartella condivisa di Administration Server**, fare clic sul pulsante **Cambia**.

5. Selezionare la cartella che si desidera utilizzare come condivisa.

6. Fare clic sul pulsante **OK** per chiudere la finestra delle proprietà di Administration Server.

7. Assegnare i diritti di lettura per il sottogruppo **Everyone** per la cartella selezionata come condivisa.

Risoluzione dei problemi relativi ai nodi di Administration Server

La struttura della console nel riquadro sinistro di Administration Console contiene nodi di Administration Server. È possibile aggiungere tutti gli Administration Server necessari nella struttura della console.

L'elenco dei nodi di Administration Server nella struttura della console è memorizzato in una copia shadow di un file msc tramite Microsoft Management Console. La copia shadow del file è disponibile nella cartella %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ nel dispositivo in cui è installato Administration Console. Per ogni nodo di Administration Server il file contiene le seguenti informazioni:

- Indirizzo di Administration Server
- Numero di porta
- Se TLS è in uso

  Questo parametro dipende dal numero della porta utilizzata per la connessione di Administration Console ad Administration Server.
- Nome utente
- Certificato di Administration Server

Risoluzione dei problemi

Quando Administration Console si connette ad Administration Server, il certificato archiviato in locale viene confrontato con il certificato di Administration Server. Se i certificati non corrispondono, Administration Console genera un errore. Ad esempio, una mancata corrispondenza dei certificati può verificarsi quando si sostituisce il certificato di Administration Server. In questo caso, creare nuovamente il nodo di Administration Server nella console.

Per ricreare un nodo di Administration Server:

1. Chiudere la finestra Kaspersky Security Center Administration Console.

2. Eliminare il file di Kaspersky Security Center 15.1 all'indirizzo %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.

3. Eseguire Kaspersky Security Center Administration Console.

   Viene richiesto di connettersi ad Administration Server e accettare il certificato esistente.

4. Eseguire una delle seguenti operazioni:

   - Accettare il certificato esistente facendo clic sul pulsante **Sì**.
   - Per specificare il certificato, fare clic sul pulsante **No**, quindi passare al file di certificato da utilizzare per l'autenticazione di Administration Server.

Il problema relativo al certificato è stato risolto. È possibile utilizzare Administration Console per connettersi con l'Administration Server.

Visualizzazione e modifica delle impostazioni di un Administration Server

È possibile regolare le impostazioni di un Administration Server nella finestra delle proprietà di tale server.

Per aprire la finestra Proprietà: Administration Server,

Selezionare **Proprietà** nel menu di scelta rapida del nodo Administration Server nella struttura della console.

Regolazione delle impostazioni generali di un Administration Server

È possibile regolare le impostazioni generali di Administration Server nelle sezioni **Generale**, **Impostazioni di connessione di Administration Server**, **Archivio eventi** e **Sicurezza** della finestra Proprietà di Administration Server.

La sezione **Sicurezza** non è visualizzata nella finestra delle proprietà di Administration Server se la visualizzazione è stata disabilitata nell'interfaccia di Administration Console.

*Per abilitare la visualizzazione della sezione **Sicurezza** in Administration Console:*

1. Nella struttura della console selezionare l'Administration Server desiderato.
2. Nel menu **Visualizza** della finestra principale dell'applicazione selezionare **Configura interfaccia**.
3. Nella finestra **Configura interfaccia** visualizzata selezionare la casella di controllo **Visualizza le sezioni delle impostazioni di protezione** e fare clic su **OK**.
4. Nella finestra con il messaggio dell'applicazione fare clic su **OK**.

La sezione **Sicurezza** verrà visualizzata nella finestra della proprietà di Administration Server.

Impostazioni dell'interfaccia di Administration Console

È possibile regolare le impostazioni dell'interfaccia di Administration Console per visualizzare o nascondere i controlli dell'interfaccia utente relativi alle seguenti funzionalità:

- Vulnerability e patch management
- Criptaggio e protezione dei dati
- Impostazioni di controllo endpoint
- Mobile Device Management
- Administration Server secondari
- Sezioni delle impostazioni di protezione

Per configurare le impostazioni dell'interfaccia di Administration Console:

1. Nella struttura della console selezionare l'Administration Server desiderato.
2. Nel menu **Visualizza** della finestra principale dell'applicazione selezionare **Configura interfaccia**.
3. Nella finestra **Configura interfaccia** visualizzata selezionare le caselle di controllo accanto alle funzionalità che si desidera visualizzare e fare clic su **OK**.
4. Nella finestra con il messaggio dell'applicazione fare clic su **OK**.

Le funzionalità selezionate verranno visualizzate nell'interfaccia di Administration Console.

Elaborazione e archiviazione di eventi in Administration Server

Le informazioni sugli eventi che si verificano durante l'esecuzione dell'applicazione e dei dispositivi gestiti vengono salvate nel database di Administration Server. A ogni evento è attribuito un determinato tipo e un livello di criticità (*Evento critico*, *Errore funzionale*, *Avviso* o *informazioni*). A seconda delle condizioni in cui si è verificato un evento, l'applicazione può assegnare diversi livelli di criticità a eventi dello stesso tipo.

È possibile visualizzare i tipi e i livelli di criticità assegnati agli eventi nella sezione **Configurazione eventi** della finestra delle proprietà di Administration Server. Nella sezione **Configurazione eventi** è anche possibile configurare l'elaborazione di ogni evento da parte di Administration Server:

- Registrazione degli eventi in Administration Server e nei registri eventi del sistema operativo in un dispositivo e in Administration Server.
- Metodo utilizzato per notificare un evento all'amministratore (ad esempio, un SMS o un messaggio e-mail).

Nella sezione **Archivio eventi** della finestra delle proprietà di Administration Server è possibile modificare le impostazioni per l'archiviazione degli eventi nel database di Administration Server, limitando il numero di record degli eventi e il periodo di archiviazione dei record. Quando si specifica il numero massimo di eventi, l'applicazione calcola approssimativamente la quantità di spazio di archiviazione necessario per il numero specificato. È possibile utilizzare questo calcolo approssimativo per valutare se è necessario liberare spazio su disco per evitare l'overflow del database. La capacità predefinita del database di Administration Server è di 400.000 eventi. La capacità massima consigliata del database è di 45 milioni di eventi.

L'applicazione controlla il database ogni 10 minuti. Se il numero di eventi raggiunge il valore massimo specificato più 10.000, l'applicazione elimina gli eventi meno recenti in modo che rimanga solo il numero massimo di eventi specificato.

Quando l'Administration Server elimina gli eventi meno recenti, non può salvare i nuovi eventi nel database. Durante questo periodo di tempo, le informazioni sugli eventi rifiutati vengono scritte nel registro eventi Kaspersky. I nuovi eventi vengono accodati e quindi salvati nel database al termine dell'operazione di eliminazione.

È possibile modificare le impostazioni di qualsiasi attività per salvare gli eventi relativi all'avanzamento dell'attività oppure salvare solo i risultati dell'esecuzione dell'attività. In tal modo si riduce il numero di eventi nel database, si aumenta la velocità di esecuzione degli scenari associati all'analisi della tabella degli eventi nel database e si limita il rischio che gli eventi critici vengano sovrascritti da un ampio numero di eventi.

Visualizzazione del registro delle connessioni all'Administration Server

È possibile salvare in un file di registro la cronologia delle connessioni e dei tentativi di connessione all'Administration Server durante l'esecuzione. Le informazioni nel file consentono di tenere traccia non solo delle connessioni nell'infrastruttura di rete, ma anche dei tentativi non autorizzati di accesso ad Administration Server.

Per registrare gli eventi di connessione all'Administration Server:

1. Nella struttura della console selezionare l'Administration Server per cui si desidera abilitare la registrazione degli eventi di connessione.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà visualizzata, nella sezione **Impostazioni di connessione di Administration Server**, selezionare la sottosezione **Porte di connessione**.
4. Abilitare l'opzione **Registra eventi di connessione ad Administration Server**.
5. Fare clic sul pulsante **OK** per chiudere la finestra delle proprietà di Administration Server.

Tutti gli ulteriori eventi di connessione in entrata all'Administration Server, i risultati di autenticazione e gli errori SSL verranno salvati nel file %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Controllo delle epidemie di virus

Kaspersky Security Center consente di rispondere velocemente alle minacce di epidemie di virus. I rischi di epidemie di virus vengono valutati monitorando l'attività dei virus nei dispositivi.

È possibile configurare le regole di valutazione per le minacce di epidemie di virus e le azioni da eseguire qualora se ne verifichi una. A tale scopo, utilizzare la sezione **Epidemia di virus** della finestra delle proprietà di Administration Server.

È possibile specificare la procedura di notifica per l'evento *Epidemia di virus* nella sezione **Configurazione eventi** della finestra delle proprietà di Administration Server, nella finestra delle proprietà dell'evento *Epidemia di virus*.

L'evento *Epidemia di virus* viene generato in caso di rilevamento di eventi *Rilevato un oggetto dannoso* durante l'esecuzione delle applicazioni di protezione. È pertanto necessario salvare le informazioni su tutti gli eventi *Rilevato un oggetto dannoso* in Administration Server per essere in grado di riconoscere le epidemie di virus.

È possibile specificare le impostazioni per il salvataggio delle informazioni su qualsiasi evento *Rilevato un oggetto dannoso* nei criteri delle applicazioni di protezione.

Durante il conteggio degli eventi *Rilevato un oggetto dannoso*, vengono prese in considerazione solo le informazioni provenienti dai dispositivi client dell'Administration Server primario. Le informazioni provenienti dagli Administration Server secondari non vengono considerate. L'evento *Epidemia di virus* è configurato individualmente per ogni server secondario.

Limitazione del traffico

Per ridurre il volume del traffico all'interno di una rete, l'applicazione offre la possibilità di limitare la velocità del trasferimento dati a un Administration Server da subnet IP e intervalli IP specificati.

È possibile creare e configurare regole di limitazione del traffico nella sezione **Traffico** della finestra delle proprietà di Administration Server.

Per creare una regola di limitazione del traffico:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server per cui si desidera creare una regola di limitazione del traffico.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server selezionare la sezione **Traffico**.
4. Fare clic sul pulsante **Aggiungi**.
5. Nella finestra **Nuova regola** specificare le seguenti impostazioni:

   Nella sezione **Intervallo IP per limitare il traffico** selezionare il metodo che verrà utilizzato per definire la subnet o l'intervallo per cui la velocità di trasferimento dei dati sarà limitata, quindi immettere i valori delle impostazioni per il metodo selezionato. Selezionare uno dei seguenti metodi:

   - **Specifica l'intervallo utilizzando l'indirizzo e la maschera di rete**

     Il traffico viene limitato in base alle impostazioni delle subnet. Specificare l'indirizzo della subnet e la subnet mask per la determinazione dell'intervallo in cui limitare il traffico.

     È inoltre possibile fare clic su **Sfoglia** per aggiungere subnet dall'elenco globale delle subnet.

   - **Specifica l'intervallo utilizzando l'indirizzo iniziale e l'indirizzo finale**

     Il traffico viene limitato in base a un intervallo di indirizzi IP. Specificare l'intervallo di indirizzi IP nei campi di immissione **Inizio** e **Fine**.

     Questa opzione è selezionata per impostazione predefinita.

   Nella sezione **Limite traffico** è possibile definire le seguenti impostazioni per la limitazione della velocità di trasferimento dei dati:

   - **Intervallo**

     Intervallo di tempo durante il quale le limitazioni del traffico saranno applicate. Nei campi di immissione è possibile specificare i limiti dell'intervallo di tempo.

   - **Limite (KB/s)**

     Velocità massima totale di trasferimento dei dati in entrata e in uscita dell'Administration Server. Le limitazioni del traffico saranno effettive solo nell'intervallo specificato nel campo **Intervallo**.

   - **Limita il traffico per il tempo rimanente (KB/s)**

     Il traffico sarà limitato non solo durante l'intervallo specificato nel campo **Intervallo**, ma anche in altri orari.

     Per impostazione predefinita, questa casella di controllo è deselezionata. Il valore di questo campo potrebbe non corrispondere al valore del campo **Limite (KB/s)**.

Le regole di limitazione del traffico influiscono principalmente sul trasferimento dei file. Queste regole non si applicano al traffico generato dalla sincronizzazione tra Administration Server e Network Agent o tra gli Administration Server primari e secondari.

Configurazione di Server Web

Il server Web è progettato per la pubblicazione di pacchetti di installazione indipendenti, profili MDM iOS e file in una cartella condivisa.

È possibile definire le impostazioni per la connessione del server Web ad Administration Server e impostare un certificato del server Web nella sezione **Server Web** della finestra delle proprietà di Administration Server.

Utilizzo di utenti interni

Gli account degli *utenti interni* vengono utilizzati per operare con gli Administration Server virtuali. Kaspersky Security Center concede agli utenti interni dell'applicazione diritti equivalenti a quelli degli utenti reali.

Gli account degli utenti interni vengono creati e utilizzati solo in Kaspersky Security Center. Nessun dato relativo agli utenti interni viene trasferito al sistema operativo. Kaspersky Security Center esegue l'autenticazione degli utenti interni.

È possibile configurare gli account degli utenti interni nella cartella **Account utente** della struttura della console.

Backup e ripristino delle impostazioni di Administration Server

Il backup delle impostazioni di Administration Server e del relativo database viene eseguito tramite l'attività di backup e l'utilità klbackup. Una copia di backup include tutte le impostazioni e gli oggetti principali relativi ad Administration Server, come certificati, chiavi primarie per il criptaggio delle unità nei dispositivi gestiti, chiavi per varie licenze, struttura dei gruppi di amministrazione con tutti i relativi contenuti, attività, criteri e così via. Con una copia di backup è possibile ripristinare il funzionamento di un Administration Server il prima possibile, un'operazione che richiede da una decina di minuti a un paio d'ore.

Se non è disponibile una copia di backup, un errore può comportare la perdita dei certificati e di tutte le impostazioni di Administration Server. In tal caso, sarà necessario riconfigurare completamente Kaspersky Security Center ed eseguire di nuovo la distribuzione iniziale di Network Agent nella rete dell'organizzazione. Andranno inoltre perse tutte le chiavi primarie per il criptaggio delle unità nei dispositivi gestiti, con il rischio di una perdita irrevocabile dei dati criptati nei dispositivi con Kaspersky Endpoint Security. Pertanto, non dimenticare di eseguire periodicamente backup di Administration Server utilizzando l'attività di backup standard.

L'Avvio rapido guidato crea l'attività di backup per le impostazioni di Administration Server e ne configura l'esecuzione quotidiana, alle 4:00. Le copie di backup vengono salvate per impostazione predefinita nella cartella %ALLUSERSPROFILE%\Application Data\KasperskySC.

Se si utilizza come DBMS un'istanza di Microsoft SQL Server installata in un altro dispositivo, è necessario modificare l'attività di backup specificando un percorso UNC, accessibile in scrittura sia dal servizio Administration Server che dal servizio SQL Server, come cartella per l'archiviazione delle copie di backup. Questo requisito deriva da una speciale funzionalità di backup nel DBMS Microsoft SQL Server.

Se si utilizza come DBMS un'istanza locale di Microsoft SQL Server, è anche consigliabile salvare copie di backup su un supporto dedicato per proteggerle dal danneggiamento insieme con Administration Server.

Poiché una copia di backup contiene dati importanti, l'attività di backup e l'utilità klbackup forniscono funzionalità di protezione tramite password delle copie di backup. Per impostazione predefinita, l'attività di backup viene creata con una password vuota. È necessario impostare una password nelle proprietà dell'attività di backup. Il mancato rispetto di questo requisito causa una situazione in cui tutte le chiavi dei certificati di Administration Server, le chiavi per le licenze e le chiavi primarie per il criptaggio delle unità nei dispositivi gestiti restano non criptate.

In aggiunta al backup periodico, è anche necessario creare una copia di backup prima di ogni modifica significativa, inclusa l'installazione di upgrade e patch di Administration Server.

Se si utilizza Microsoft SQL Server come DBMS, è possibile ridurre al minimo le dimensioni delle copie di backup. A tale scopo, abilitare l'opzione **Comprimi backup** nelle impostazioni di SQL Server.

Il ripristino da una copia di backup viene eseguito con l'utilità klbackup in un'istanza funzionante di Administration Server che è stata appena installata e con la stessa versione (o una versione successiva) di quella per cui è stata creata la copia di backup.

L'istanza di Administration Server in cui deve essere eseguito il ripristino deve utilizzare un DBMS dello stesso tipo (ad esempio, SQL Server o MariaDB) e della stessa versione o successiva. La versione di Administration Server può essere la stessa (con una patch identica o successiva) o una versione successiva.

In questa sezione sono descritti gli scenari standard per il ripristino delle impostazioni e degli oggetti di Administration Server.

Utilizzo di uno snapshot del file system per ridurre la durata del backup

In Kaspersky Security Center 15.1, il tempo di inattività di Administration Server durante il backup è stato ridotto rispetto alle versioni precedenti. Inoltre, è stata aggiunta la funzionalità **Usa snapshot del file system per il backup dei dati** alle impostazioni delle attività. Questa funzionalità consente una riduzione aggiuntiva del tempo di inattività grazie all'utilità klbackup, che crea una copia shadow del disco durante il backup (in pochi secondi) e contemporaneamente esegue la copia del database (questa operazione richiede al massimo alcuni minuti). Quando klbackup crea una copia shadow del disco e una copia del database, l'utilità rende l'Administration Server nuovamente disponibile per la connessione.

È possibile utilizzare la funzionalità per la creazione di snapshot del file system solo se sono soddisfatte queste due condizioni:

- La cartella condivisa di Administration Server e la cartella %ALLUSERSPROFILE%\KasperskyLab si trovano nello stesso disco logico e sono cartelle locali in riferimento all'Administration Server.
- La cartella %ALLUSERSPROFILE%\KasperskyLab non contiene collegamenti simbolici che sono stati creati manualmente.

Se una di queste condizioni non può essere soddisfatta, non utilizzare la funzionalità. In questo caso, l'applicazione restituisce un messaggio di errore in risposta a qualsiasi tentativo di creare uno snapshot del file system.

Per utilizzare la funzionalità, è necessario disporre di un account a cui è stata concessa l'autorizzazione per la creazione di snapshot del disco logico che contiene la cartella %ALLUSERSPROFILE%. Tenere presente che l'account del servizio Administration Server non dispone di questo tipo di autorizzazione.

Per utilizzare la funzionalità per la creazione di snapshot del file system per ridurre la durata del backup:

1. Nella sezione **Attività** selezionare l'attività di backup.
2. Nel menu di scelta rapida selezionare **Proprietà**.

3. Nella finestra delle proprietà dell'attività visualizzata selezionare la sezione **Impostazioni**.

4. Selezionare la casella di controllo **Usa snapshot del file system per il backup dei dati**.

5. Nei campi **Nome utente** e **Password** immettere il nome e la password di un account che dispone dell'autorizzazione per la creazione di snapshot del disco logico che contiene la cartella %ALLUSERSPROFILE%.

6. Fare clic su **Applica**.

A ogni successivo avvio dell'attività di backup, l'utilità klbackup creerà snapshot del file system, riducendo il tempo di inattività dell'Administration Server durante l'esecuzione dell'attività.

Un dispositivo con Administration Server è inutilizzabile

Se un dispositivo con Administration Server risulta inutilizzabile a causa di un errore, è consigliabile eseguire le seguenti operazioni:

- Al nuovo Administration Server deve essere assegnato lo stesso indirizzo: nome NetBIOS, FQDN o IP statico (a seconda dell'elemento impostato al momento della distribuzione dei Network Agent).

- Installare Administration Server utilizzando un DBMS dello stesso tipo e della stessa versione (o di una versione successiva). È possibile installare la stessa versione del server (con una patch identica o successiva) o una versione successiva. Dopo installazione, non eseguire la configurazione iniziale tramite la procedura guidata.

- Nel menu **Start**, eseguire l'utilità klbackup e quindi eseguire il ripristino.

Le impostazioni di Administration Server o il database sono danneggiati

Se Administration Server risulta inutilizzabile perché le impostazioni o il database sono danneggiati (ad esempio, in seguito a una sovralimentazione), è consigliabile utilizzare il seguente scenario di ripristino:

1. Eseguire la scansione del file system nel dispositivo danneggiato.

2. Disinstallare la versione inutilizzabile di Administration Server.

3. Reinstallare Administration Server utilizzando un DBMS dello stesso tipo e della stessa versione (o di una versione successiva). È possibile installare la stessa versione del server (con una patch identica o successiva) o una versione successiva. Dopo installazione, non eseguire la configurazione iniziale tramite la procedura guidata.

4. Dal menu **Start** eseguire l'utilità klbackup e quindi eseguire il ripristino.

Non è consentito ripristinare Administration Server in un modo diverso dall'utilizzo dell'utilità klbackup.

Qualsiasi tentativo di ripristinare Administration Server tramite software di terze parti causerà inevitabilmente la mancata sincronizzazione dei dati nei nodi dell'applicazione Kaspersky Security Center distribuita e, di conseguenza, impedirà il corretto funzionamento dell'applicazione.

Backup e ripristino dei dati di Administration Server

Il backup dei dati consente di spostare un Administration Server da un dispositivo all'altro senza perdite di dati. Tramite il backup, è possibile ripristinare i dati quando si sposta il database di Administration Server su un altro dispositivo o quando si esegue l'aggiornamento a una versione più recente di Kaspersky Security Center. Inoltre, è possibile utilizzare il backup dei dati per spostare i dati di Administration Server da Kaspersky Security Center Windows sotto la gestione di Kaspersky Security Center Linux (lo spostamento dei dati da Kaspersky Security Center Linux a Kaspersky Security Center Windows non è supportato).

Non viene eseguito il backup dei plug-in di gestione installati. Dopo aver ripristinato i dati di Administration Server da una copia di backup, è necessario scaricare e reinstallare i plug-in per le applicazioni gestite.

Prima di eseguire il backup dei dati di Administration Server, verificare se al gruppo di amministrazione è stato aggiunto un Administration Server virtuale. Se viene aggiunto un Administration Server virtuale, assicurarsi che a questo Administration Server virtuale sia assegnato un amministratore prima del backup. Non è possibile concedere all'amministratore i diritti di accesso all'Administration Server virtuale dopo il backup. Tenere presente che se le credenziali dell'account amministratore vengono smarrite, non sarà possibile assegnare un nuovo amministratore all'Administration Server virtuale.

Per eseguire il backup o il ripristino di un cluster di failover di Kaspersky Security Center, è necessario arrestare l'intero cluster per la manutenzione e quindi riavviarlo al termine del backup o del ripristino.

È possibile creare una copia di backup dei dati di Administration Server in uno dei seguenti modi:

- Creando ed eseguendo un'attività di backup dei dati tramite Administration Console.
- Eseguendo l'utilità klbackup nel dispositivo in cui è installato Administration Server. Questa utilità è inclusa nel kit di distribuzione di Kaspersky Security Center. Dopo l'installazione di Administration Server, l'utilità è disponibile nella radice della cartella di destinazione specificata durante l'installazione dell'applicazione.

I seguenti dati vengono salvati nella copia di backup di Administration Server:

- Database di Administration Server (criteri, attività, impostazioni delle applicazioni, eventi salvati in Administration Server).
- Dettagli sulla configurazione della struttura dei gruppi di amministrazione e dei dispositivi client.
- Archivio dei pacchetti di distribuzione delle applicazioni per l'installazione remota.
- Certificato di Administration Server.
- Contenuto della cartella *Updates*.

  Per impostazione predefinita, il percorso della cartella è C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Il ripristino dei dati di Administration Server è possibile solo tramite l'utilità klbackup. È necessario eseguire Il ripristino di un'istanza funzionante di Administration Server che è stata appena installata e con la stessa versione (o una versione successiva) di quella per cui è stata creata la copia di backup.

Attività Backup dei dati di Administration Server

Creazione di un'attività Backup dei dati di Administration Server

L'attività di backup è un'attività di Administration Server; viene creata tramite l'Avvio rapido guidato. Se un'attività di backup creata dall'Avvio rapido guidato è stata eliminata, è possibile crearne una manualmente.

Per creare un'attività Backup dei dati di Administration Server:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Avviare la creazione dell'attività in uno dei seguenti modi:
   - Selezionando **Nuovo** → **Attività** nel menu di scelta rapida della cartella **Attività** nella struttura della console.
   - Facendo clic sul pulsante **Crea attività** nell'area di lavoro.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata. Nella finestra **Selezionare il tipo di attività** della procedura guidata selezionare il tipo di attività **Backup dei dati di Administration Server**.

L'attività **Backup dei dati di Administration Server** può essere creata solo in una singola copia. Se l'attività di backup dei dati di Administration Server è stata già creata per l'Administration Server, non viene visualizzata nella finestra di selezione del tipo di attività della Creazione guidata attività di backup di Administration Server.

Configurazione dell'attività Backup dei dati di Administration Server

Dopo aver creato un'attività di backup, è possibile configurare le impostazioni dell'attività.

Per configurare l'attività Backup dei dati di Administration Server:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Nel menu di scelta rapida di **Backup dei dati di Administration Server**, selezionare **Proprietà**.

Verrà visualizzata la finestra delle proprietà dell'attività *Backup dei dati di Administration Server*. Sono disponibili le seguenti proprietà:

- **Generale**

  Nella sezione **Generale**, è possibile specificare il nome dell'attività, visualizzare la data di creazione dell'attività, la data dell'ultimo comando, lo stato dell'avvio dell'attività e i risultati dell'attività.

- **Notifica**

  Nella sezione **Notifica**, è possibile specificare le impostazioni per l'archiviazione degli eventi correlati ai risultati dell'esecuzione delle attività, nonché configurare le notifiche sui risultati dell'esecuzione delle attività.

- **Pianificazione**

  Nella sezione **Pianificazione**, è possibile specificare una pianificazione per l'avvio dell'attività.

- **Destinazione**

  Nella sezione **Destinazione**, è possibile specificare il percorso della cartella per l'archiviazione delle copie di backup dei dati di Administration Server.

- **Impostazioni**

  Nella sezione **Impostazioni**, è possibile impostare la password di protezione del backup e il numero di copie di backup, se necessario.

  È inoltre possibile creare una copia replicata del disco logico in cui è archiviata la cartella %ALLUSERSPROFILE% e copiare il database di Administration Server. A tale scopo, è necessario abilitare l'opzione **Usa snapshot del file system per il backup dei dati**, quindi specificare il nome e la password di un account che dispone dell'autorizzazione per creare snapshot.

- **Sicurezza**

  Nella sezione **Sicurezza** è possibile concedere a utenti e gruppi le autorizzazioni per eseguire operazioni su Administration Server. Se l'opzione **Eredita le impostazioni da Administration Server** è abilitata, le impostazioni di protezione dell'attività vengono ereditate da Administration Server.

  Se questa opzione è disabilitata, è possibile configurare le impostazioni di protezione per l'attività. È possibile assegnare un ruolo a un utente o un gruppo di utenti o assegnare autorizzazioni a un utente o un gruppo di utenti, come applicabile per l'attività.

  Per impostazione predefinita, l'opzione **Eredita le impostazioni da Administration Server** è abilitata.

- **Cronologia revisioni**

  Nella sezione **Cronologia revisioni**, è possibile tenere traccia della modifica dell'attività. Ogni volta che si salvano le modifiche apportate all'attività, viene creata una revisione.

Utilità per il backup e il ripristino dei dati (klbackup)

È possibile copiare i dati di Administration Server a scopo di backup e per il ripristino in un secondo momento tramite l'utilità klbackup, inclusa nel kit di distribuzione di Kaspersky Security Center.

L'utilità klbackup può essere eseguita in due modalità:

- Interattiva
- Automatica

Backup e ripristino dei dati in modalità interattiva

Il ripristino dei dati di Administration Server da una copia di backup creata utilizzando l'utilità klbackup in modalità interattiva potrebbe verificarsi con un errore. Se è stata installata la patch 15.1.0.20748-pf2 per Administration Server e quindi è stata creata una copia di backup utilizzando l'utilità klbackup con l'opzione **Esegui migrazione del database** disabilitata, si verifica un errore durante il ripristino di questa copia (per tutti i DBMS, ad eccezione di MySQL e MariaDB). Se è installata la patch 15.1.0.20748-pf2 per Administration Server e si desidera creare una copia di backup senza eseguire la migrazione a un altro DBMS, utilizzare un'attività di backup dei dati o eseguire l'utilità klbackup dalla riga di comando.

Per creare una copia di backup dei dati di Administration Server in modalità interattiva:

1. Eseguire l'utilità klbackup disponibile nella cartella di installazione di Kaspersky Security Center.

   Verrà avviata la Procedura guidata di backup e ripristino.

2. Nella prima finestra della procedura guidata selezionare **Esegui il backup dei dati di Administration Server**.

   Se si seleziona l'opzione **Esegui il ripristino o il backup solo del certificato di Administration Server**, verrà salvata solo una copia di backup del certificato e della chiave privata di Administration Server. Il backup del certificato e della chiave privata di Administration Server può essere utile quando si esegue la migrazione da Administration Server di Kaspersky Security Center Windows ad Administration Server di Kaspersky Security Center Linux. È inoltre possibile eseguire la migrazione dei dispositivi gestiti tra gli Administration Server di Kaspersky Security Center Linux, nonché tra gli Administration Server di Kaspersky Security Center Windows. Per ulteriori informazioni, consultare Utilizzo dell'utilità klbackup per cambiare i dispositivi gestiti sotto la gestione di un altro Administration Server.

   Fare clic su **Avanti**.

3. Nella finestra successiva della procedura guidata, specificare le seguenti opzioni:

- **Cartella di destinazione del backup**
- **Esegui la migrazione del database**

  Abilitare questa opzione se al momento si archiviano i dati di Administration Server in un database di Microsoft SQL Server ed è necessario eseguirne la migrazione in uno dei seguenti database: MySQL o MariaDB, PostgreSQL o Postgres Pro, Azure SQL. Per impostazione predefinita, questa opzione è disabilitata.

  - **Esegui la migrazione al formato MySQL/MariaDB**

    Abilitare questa opzione se al momento si utilizza SQL Server come DBMS per Administration Server e si desidera migrare i dati da SQL Server al DBMS di MySQL o MariaDB. Kaspersky Security Center creerà un backup compatibile con MySQL e MariaDB. Successivamente, è possibile ripristinare i dati dal backup in MySQL o MariaDB.

  - **Esegui la migrazione a Postgres**

    Abilitare questa opzione se al momento si utilizza SQL Server come DBMS per Administration Server e si desidera migrare i dati da SQL Server al DBMS di PostgreSQL o Postgres Pro. Kaspersky Security Center creerà un backup compatibile con PostgreSQL e Postgres Pro. Successivamente, è possibile ripristinare i dati dal backup in PostgreSQL o Postgres Pro.

    Questa opzione diventa disponibile se si invia una richiesta all'Assistenza tecnica di Kaspersky e si installa la patch 15.1.0.20748-pf2 per Administration Server o si esegue l'aggiornamento a Kaspersky Security Center Windows versione 15.1.0.22239.

  - **Esegui la migrazione al formato Azure**

    Abilitare questa opzione se al momento si utilizza SQL Server come DBMS per Administration Server e si desidera migrare i dati da SQL Server al DBMS di Azure SQL. Kaspersky Security Center creerà un backup compatibile con Azure SQL. Successivamente, è possibile ripristinare i dati dal backup in Azure SQL.

- **Includi la data e l'ora correnti nel nome della cartella di destinazione del backup**
- **Password per il backup**

4. Fare clic sul pulsante **Avanti** per avviare il backup.

5. Se si utilizza un database in un ambiente cloud come Amazon Web Services (AWS) o Microsoft Azure, nella finestra **Accedere all'archivio online** compilare i seguenti campi:

   - Per AWS:

     - **Nome del bucket S3**

       Nome del bucket S3 che è stato creato per il backup.

     - **ID chiave di accesso**

       L'ID chiave (sequenza di caratteri alfanumerici) è stato ricevuto al momento della creazione dell'account utente IAM per l'utilizzo dell'istanza di archiviazione del bucket S3.

       Il campo è disponibile se è stato selezionato il database RDS in un bucket S3.

     - **Chiave segreta**

       Chiave segreta ricevuta con l'ID chiave di accesso al momento della creazione dell'account utente IAM.

       I caratteri della chiave segreta sono visualizzati come asterischi. Quando si inizia a immettere la chiave segreta, viene visualizzato il pulsante **Mostra**. Tenere premuto questo pulsante per visualizzare i caratteri immessi.

       Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

   - Per Microsoft Azure:

     - **Nome dell'account di archiviazione Azure**

       È stato creato il nome dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

     - **ID sottoscrizione Azure**

       La sottoscrizione è stata creata dall'utente nel portale di Azure.

     - **Password Azure**

       La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

       I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

     - **ID applicazione Azure**

L'ID applicazione è stato creato dall'utente nel portale di Azure.

È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

- **Nome del server SQL Azure**

  Il nome e il gruppo di risorse sono disponibili nelle proprietà del server SQL Azure.

- **Gruppo di risorse del server SQL Azure**

  Il nome e il gruppo di risorse sono disponibili nelle proprietà del server SQL Azure.

- **Chiave di accesso all'archivio Azure**

  Disponibile nelle proprietà dell'account di archiviazione, nella sezione Chiavi di accesso. È possibile utilizzare qualsiasi chiave (chiave1 o chiave2).

Per ripristinare i dati di Administration Server in modalità interattiva:

1. Eseguire l'utilità klbackup disponibile nella cartella di installazione di Kaspersky Security Center. Avviare klbackup con lo stesso account utilizzato per l'installazione di Administration Server. Si consiglia di eseguire l'utilità su un Administration Server appena installato.

   Verrà avviata la Procedura guidata di backup e ripristino.

2. Nella prima finestra della procedura guidata selezionare **Ripristina dati di Administration Server**, quindi fare clic su **Avanti**.

   Se si seleziona l'opzione **Esegui il ripristino o il backup solo del certificato di Administration Server**, il certificato e la chiave di privata di Administration Server verrà solo ripristinato.

   Quando si esegue l'utilità klbackup nel nodo del cluster di failover inattivo, verrà richiesto di selezionare una delle opzioni: specificare il certificato di Administration Server o recuperare automaticamente i dati da Administration Server.

3. Nella finestra **Ripristinare le impostazioni** della procedura guidata:

   - Specificare la cartella che contiene una copia di backup dei dati di Administration Server.

     Se si utilizza un ambiente cloud come AWS o Azure, specificare l'indirizzo dell'archiviazione. Assicurarsi inoltre che il file si chiami backup.zip.

   - Specificare la password che è stata immessa durante il backup dei dati.

     Al momento del ripristino dei dati, è necessario specificare la stessa password che è stata immessa durante il backup. Se il percorso di una cartella condivisa è stato modificato dopo il backup, controllare l'esecuzione delle attività che utilizzano i dati ripristinati (attività di ripristino e attività di installazione remota). Se necessario, modificare le impostazioni di queste attività. Durante il ripristino dei dati da un file di backup, nessun utente deve accedere alla cartella condivisa di Administration Server. L'account con cui viene avviata l'utilità klbackup deve avere accesso completo alla cartella condivisa.

4. Fare clic sul pulsante **Avanti** per ripristinare i dati.

Backup e ripristino dei dati in modalità automatica

Per creare una copia di backup o eseguire il ripristino dei dati di Administration Server in modalità automatica:

Eseguire klbackup con il set di chiavi desiderato dalla riga di comando del dispositivo in cui è installato Administration Server.

I flag di Network Agent non vengono ripristinati quando si utilizza l'utilità klbackup. È necessario configurare manualmente i flag di Network Agent.

L'istanza di Administration Server in cui deve essere eseguito il ripristino deve utilizzare un DBMS dello stesso tipo. La versione di Administration Server può essere la stessa (con una patch identica o successiva) o una versione successiva.

Sintassi della riga di comando per l'utilità:

```
klbackup -path <backup path> [-linux_path <percorso di backup SQL Server backup path>]
[-node_cert <percorso certificato>] [-logfile <file di registro>] [-use_ts]|[-restore]
[-password <password>] [-cert_only] [-online] [-migrate postgres]
```

Se non viene specificata alcuna password nella riga di comando dell'utilità klbackup, verrà richiesto di immetterla nella modalità interattiva.

Descrizioni delle chiavi:

- `-path <percorso di backup>`: salvare le informazioni nella cartella di backup specificata o utilizzare i dati nella cartella di backup per il ripristino (parametro obbligatorio).

  È necessario concedere all'account del server database e all'utilità klbackup le autorizzazioni per la modifica dei dati nella cartella di backup.

- `-linux_path <percorso di backup di SQL Server>`: percorso locale della cartella con i dati di backup per SQL Server in Linux.

  È necessario concedere all'account del server database e all'utilità klbackup le autorizzazioni per la modifica dei dati nella cartella di backup di SQL Server.

- `-node_cert <percorso del certificato>`: file del certificato del server per configurare il nodo del cluster di failover inattivo dopo il ripristino. Se non è impostato, verrà recuperato automaticamente dal server.

  Quando si esegue l'utilità klbackup nel nodo del cluster di failover inattivo, utilizzare questa chiave per specificare il percorso del certificato del server.

- `-logfile <file di registro>`: salvare un rapporto sul backup e il ripristino dei dati di Administration Server.

- `-use_ts` — Quando si salvano i dati, copiare le informazioni nella cartella di backup, nella sottocartella con un nome nel formato `klbackup YYYY-MM-DD # HH-MM-SS`, che include la data corrente e l'ora dell'operazione in UTC. Se la chiave non è specificata, le informazioni vengono salvate nella radice della cartella di backup.

  Quando si tenta di salvare le informazioni in una cartella in cui è già presente una copia di backup, viene visualizzato un messaggio di errore. Le informazioni non vengono aggiornate.

  La disponibilità della chiave `-use_ts` consente la gestione di un archivio dei dati di Administration Server. Ad esempio, se la chiave `-path` indica la cartella `C:\KLBackups`, nella cartella `klbackup 2022/6/19 # 11-30-18` vengono archiviate le informazioni sullo stato dell'Administration Server in data 19 giugno 2022 alle 11:30:18.

- `-restore` — Ripristinare i dati di Administration Server. Il ripristino dei dati viene eseguito in base alle informazioni contenute nella cartella di backup. Se non è disponibile nessuna chiave, viene eseguito il backup dei dati nella cartella di backup.

- `-password <password>`: password per proteggere i dati sensibili.

  Non è possibile recuperare una password dimenticata. Non sono disponibili requisiti per la password. La lunghezza della password è illimitata ed è possibile anche la lunghezza zero (nessuna password).

  Al momento del ripristino dei dati, è necessario specificare la stessa password che è stata immessa durante il backup. Se il percorso di una cartella condivisa è stato modificato dopo il backup, controllare l'esecuzione delle attività che utilizzano i dati ripristinati (attività di ripristino e attività di installazione remota). Se necessario, modificare le impostazioni di queste attività. Durante il ripristino dei dati da un file di backup, nessun utente deve accedere alla cartella condivisa di Administration Server. L'account con cui viene avviata l'utilità klbackup deve avere accesso completo alla cartella condivisa. Si consiglia di eseguire l'utilità su un Administration Server appena installato.

- `-cert_only` — Salvare o ripristinare solo il certificato e la chiave privata di Administration Server.

  Questo flag può essere utile quando si esegue la migrazione da Administration Server di Kaspersky Security Center Windows ad Administration Server di Kaspersky Security Center Linux. È inoltre possibile eseguire la migrazione dei dispositivi gestiti tra gli Administration Server di Kaspersky Security Center Linux, nonché tra gli Administration Server di Kaspersky Security Center Windows.

- `-online`: eseguire il backup dei dati di Administration Server creando uno snapshot del volume per ridurre al minimo il tempo offline di Administration Server. Quando si utilizza l'utilità per recuperare i dati, questa opzione viene ignorata. Non utilizzare questo flag durante la creazione di un backup per la migrazione a un DBMS diverso.

- -archive 0: mantiene i dati del server come file semplici. Per impostazione predefinita (`-archive 1`), i dati del server sono archiviati in un file di archivio.

- `-migrate mysql`: crea un backup dei dati di Administration Server archiviati nel database SQL Server compatibile con MySQL (incluso MariaDB). È possibile ripristinare i dati dal backup in MySQL.

- `-migrate postgres`: crea un backup dei dati di Administration Server archiviati nel database SQL Server compatibile con PostgreSQL e Postgres Pro. È possibile ripristinare i dati dal backup in PostgreSQL o Postgres Pro. Utilizzare questo contrassegno quando si esegue la migrazione a Kaspersky Security Center Linux tramite il backup dei dati di Administration Server.

  Questa opzione diventa disponibile se si invia una richiesta all'Assistenza tecnica di Kaspersky e si installa la patch 15.1.0.20748-pf2 per Administration Server o si esegue l'aggiornamento a Kaspersky Security Center Windows versione 15.1.0.22239.

Utilizzo dell'utilità klbackup per cambiare i dispositivi gestiti sotto la gestione di un altro Administration Server

L'utilità klbackup consente di cambiare i dispositivi sotto la gestione di un altro Administration Server. È possibile modificare l'Administration Server di Kaspersky Security Center Windows in Kaspersky Security Center Linux Administration Server utilizzando l'utilità klbackup quando si esegue la migrazione. È inoltre possibile eseguire la migrazione dei dispositivi gestiti tra gli Administration Server di Kaspersky Security Center Linux, nonché tra gli Administration Server di Kaspersky Security Center Windows.

Per cambiare i dispositivi sotto la gestione di un altro Administration Server utilizzando l'utilità klbackup:

1. Nel dispositivo precedente, creare una copia di backup del certificato e della chiave privata di Administration Server.

   È possibile creare una copia di backup in uno dei seguenti modi:

   - Tramite l'interfaccia dell'utilità klbackup (solo per Kaspersky Security Center Windows Administration Server)

     Eseguire l'utilità klbackup situata nella cartella di installazione di Kaspersky Security Center, quindi creare un backup utilizzando l'opzione **Esegui il ripristino o il backup solo del certificato di Administration Server**.

   - Utilizzando il prompt dei comandi (per Kaspersky Security Center Windows e Kaspersky Security Center Linux Administration Server versione 15.1 o successiva)

     Eseguire l'utilità klbackup con la chiave `-cert_only` dalla riga di comando, per creare una copia di backup del certificato e della chiave privata di Administration Server:

     ```
     klbackup -path percorso della copia di backup del certificato di Administration Server > -cert_only
     ```

2. Nel dispositivo precedente, disconnettere Administration Server dalla rete.

3. Assegnare lo stesso indirizzo al dispositivo con un altro Administration Server.

   È possibile assegnare al nuovo Administration Server il nome NetBIOS, l'FQDN e l'indirizzo IP statico. Dipende dall'indirizzo di Administration Server impostato nel pacchetto di installazione di Network Agent al momento della distribuzione dei Network Agent. In alternativa, è possibile utilizzare l'indirizzo di connessione che determina l'Administration Server a cui Network Agent si connette (è possibile ottenere questo indirizzo nei dispositivi gestiti utilizzando l'utilità klnagchk).

4. In un dispositivo con un altro Administration Server, ripristinare il certificato e la chiave privata di Administration Server dalla copia di backup.

   È possibile ripristinare una copia di backup in uno dei seguenti modi:

   - Tramite l'interfaccia dell'utilità klbackup (solo per Kaspersky Security Center Windows Administration Server)

     Eseguire l'utilità klbackup, quindi ripristinare un backup utilizzando l'opzione **Esegui il ripristino o il backup solo del certificato di Administration Server**.

   - Utilizzando il prompt dei comandi (per Kaspersky Security Center Windows e Kaspersky Security Center Linux Administration Server versione 15.1 o successiva)

     Eseguire l'utilità klbackup con la chiave `-cert_only` dalla riga di comando, per ripristinare una copia di backup del certificato e della chiave privata di Administration Server:

     ```
     klbackup -path < percorso della copia di backup del certificato di Administration Server > -restore -cert_only
     ```

I dispositivi gestiti vengono inseriti nella gestione di un altro Administration Server. È possibile passare a questo Administration Server e verificare che i dispositivi gestiti siano visibili nella rete e che Network Agent sia installato e in esecuzione (il valore *Sì* nelle colonne **Visibile**, **Network Agent installato** e **Network Agent è in esecuzione**).

Backup e ripristino dei dati di Administration Server quando si utilizza MySQL o MariaDB

È possibile utilizzare un backup dei dati per eseguire la migrazione dei dati di Administration Server da Kaspersky Security Center Windows con la gestione di Kaspersky Security Center Linux. La migrazione tramite il backup dei dati di Administration Server è supportata solo per la migrazione a Kaspersky Security Center Linux 15.2 o versioni successive da qualsiasi versione supportata di Kaspersky Security Center Windows.

Se si utilizza MySQL o MariaDB come DBMS per Kaspersky Security Center Windows e Kaspersky Security Center Linux, il parametro `lower_case_table_names` deve corrispondere per il DBMS corrente e quello nuovo. In caso contrario, la migrazione dei dati di Administration Server verrà eseguita in modo errato.

Prima di eseguire il backup dei dati di Administration Server in Kaspersky Security Center Windows, controllare il valore del parametro `lower_case_table_names`. Se prima non si specifica questo parametro durante l'installazione del DBMS, viene utilizzato il valore del parametro predefinito. Il valore predefinito del parametro `lower_case_table_names` per Windows è `1`.

Durante l'installazione di MySQL o MariaDB for Kaspersky Security Center Linux, impostare il parametro `lower_case_table_names` sullo stesso valore specificato per questo parametro per Windows utilizzando le istruzioni del sito Web di MySQL. Se non si specifica questo parametro, viene utilizzato il valore del parametro predefinito. Per i sistemi operativi basati su Linux, il valore predefinito del parametro `lower_case_table_names` è diverso dal valore predefinito per Windows.

Se si desidera installare MySQL 8.0, la specifica del parametro `lower_case_table_names` in base a questa istruzione potrebbe non funzionare. In questo caso, è prima necessario installare MySQL 5.7, specificare il parametro `lower_case_table_names` utilizzando l'istruzione, quindi eseguire l'upgrade di MySQL 5.7 a MySQL 8.0. Se il parametro `lower_case_table_names` non corrisponde per il DBMS corrente e quello nuovo, i dati di Administration Server verranno ripristinati in modo errato.

Ottimizzazione del backup e ripristino dei dati di Administration Server

Per ottimizzare il backup e il ripristino dei dati di Administration Server per ridurre i tempi di inattività di Administration Server, eseguire una delle seguenti operazioni:

- Abilitare l'opzione **Usa snapshot del file system per il backup dei dati**.

  Per maggiori dettagli, fare riferimento al seguente articolo: Utilizzo di uno snapshot del file system per ridurre la durata del backup.

- Configurare i seguenti flag:

  Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

  - `KLSRV_BKP_FILES`: suddivide il file di database in più file più piccoli, da 2 a 32. Ciò può accelerare il backup e il ripristino se le prestazioni del DBMS sono limitate dalla CPU.

    Esempio:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_FILES -t d -v 2
    ```

  - `KLSRV_BKP_BACKUP_EXTRA_PARS`: specifica i parametri `COMPRESSION` and `MAXTRANSFERSIZE`. Ciò può velocizzare il backup se le prestazioni del DBMS sono limitate dall'input/output dei file.

    Esempio:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_BACKUP_EXTRA_PARS -t s -v "COMPRESSION,
    MAXTRANSFERSIZE = 4194304"
    ```

  - `KLSRV_BKP_RESTORE_EXTRA_PARS`: specifica il parametro `MAXTRANSFERSIZE`. Ciò può velocizzare il ripristino se le prestazioni del DBMS sono limitate dall'input/output dei file.

    Esempio:

    ```
    klscflag -fset -pv klserver -n KLSRV_BKP_RESTORE_EXTRA_PARS -t s -v "MAXTRANSFERSIZE
    = 4194304"
    ```

  - `KLSRV_BKP_ONLINE_DB_BACKUP`: rimuove i tempi di inattività di Administration Server durante il backup. Disponibile solo per i seguenti DBMS:

    - PostgreSQL, Postgres Pro.

    - SQL Server con modello di ripristino completo. Per ulteriori dettagli, consultare la documentazione di PostgreSQL. Quando si abilita il flag `KLSRV_BKP_ONLINE_DB_BACKUP`, il DBMS di SQL Server passa automaticamente al modello di ripristino completo.

    Esempio:

    ```
    klscflag.exe -fset -pv klserver -n KLSRV_BKP_ONLINE_DB_BACKUP -t d -v 1
    ```

Spostamento di Administration Server in un altro dispositivo

Se è necessario utilizzare Administration Server in un nuovo dispositivo, è possibile spostarlo in uno dei seguenti modi:

- Spostare Administration Server e il server di database in un nuovo dispositivo (il server di database può essere installato nel nuovo dispositivo insieme ad Administration Server o in un altro dispositivo).
- Mantenere il server di database nel dispositivo precedente e spostare solo Administration Server in un nuovo dispositivo.

Per spostare Administration Server in un nuovo dispositivo:

1. Nel dispositivo precedente creare un backup dei dati di Administration Server.

   A tale scopo, è possibile eseguire l'attività di backup dei dati tramite Administration Console o eseguire l'utilità klbackup.

   > Se si utilizza SQL Server come DBMS per Administration Server, è possibile migrare i dati da SQL Server al DBMS di MySQL o MariaDB. A tale scopo, eseguire l'utilità klbackup in modalità interattiva per creare un backup dei dati. Abilitare l'opzione **Esegui la migrazione al formato MySQL/MariaDB** nella finestra **Impostazioni backup** della procedura guidata di backup e ripristino. Kaspersky Security Center creerà un backup compatibile con MySQL e MariaDB. Successivamente, è possibile ripristinare i dati dal backup in MySQL o MariaDB.

   > È inoltre possibile abilitare l'opzione **Esegui la migrazione al formato Azure** se si desidera migrare i dati da SQL Server al DBMS di Azure SQL.

2. Nel dispositivo precedente, disconnettere Administration Server dalla rete.

3. Selezionare un nuovo dispositivo in cui installare Administration Server. Assicurarsi che l'hardware e il software nel dispositivo selezionato soddisfino i requisiti per Administration Server, Administration Console e Network Agent. Controllare inoltre che le porte utilizzate in Administration Server siano disponibili.

4. Assegnare lo stesso indirizzo al nuovo dispositivo.

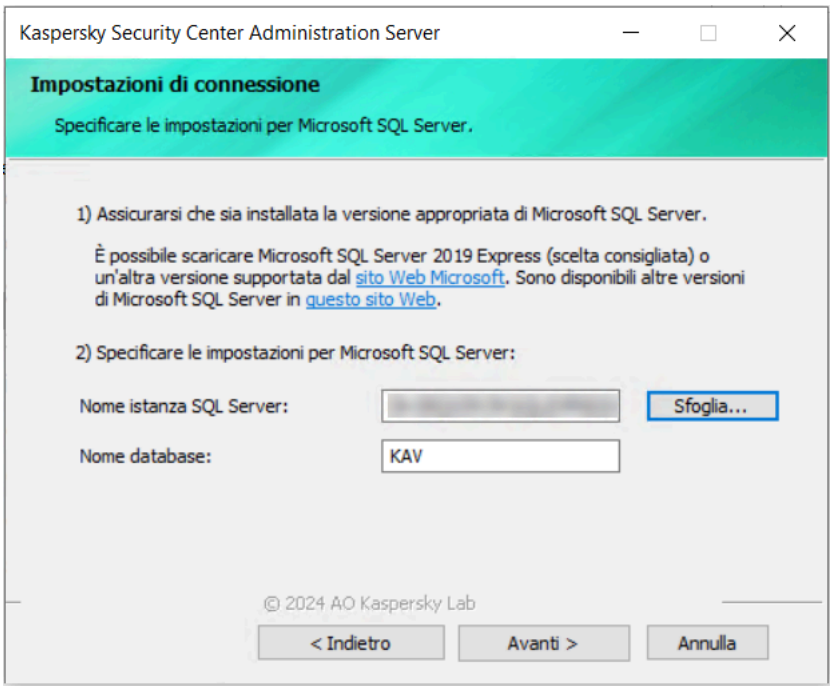
   È possibile assegnare al nuovo Administration Server il nome NetBIOS, l'FQDN e l'indirizzo IP statico. Dipende dall'indirizzo di Administration Server impostato nel pacchetto di installazione di Network Agent al momento della distribuzione dei Network Agent. In alternativa, è possibile utilizzare l'indirizzo di connessione che determina l'Administration Server a cui Network Agent si connette (è possibile ottenere questo indirizzo nei dispositivi gestiti utilizzando l'utilità klnagchk).

5. Se nececessario, in un altro dispositivo installare il sistema di gestione database (DBMS) che verrà utilizzato da Administration Server.

   Il database può essere installato nel nuovo dispositivo insieme ad Administration Server o in un altro dispositivo. Verificare che questo dispositivo soddisfi i requisiti hardware e software. Quando si seleziona un DBMS, tenere in considerazione il numero di dispositivi coperti da Administration Server.

6. Eseguire l'installazione dell'Administration Server nel nuovo dispositivo.

7. Durante l'installazione dell'Administration Server, configurare le impostazioni di connessione al server di database.



Esempio della finestra Impostazioni di connessione per Microsoft SQL Server

A seconda di dove è necessario individuare il server del database, eseguire una delle seguenti operazioni:

- **Mantenimento del server del database nel dispositivo precedente**

  1. Fare clic sul pulsante **Sfoglia** accanto al campo **Nome istanza SQL Server**, quindi selezionare il nome del dispositivo precedente nell'elenco visualizzato.

     Si noti che il dispositivo precedente deve essere disponibile per la connessione con il nuovo Administration Server.

  2. Immettere il nome del database precedente nel campo **Nome database**.

- **Spostare il server del database in un altro dispositivo**

  1. Fare clic sul pulsante **Sfoglia** accanto al campo **Nome istanza SQL Server**, quindi selezionare il nome del dispositivo nell'elenco visualizzato.

  2. Immettere il nuovo nome nel campo **Nome database**.

     Si noti che il nuovo nome del database deve corrispondere al nome del database del dispositivo precedente. I nomi dei database devono essere identici, in modo da poter utilizzare il backup di Administration Server. Il nome predefinito del database è *KAV*.

8. Al termine dell'installazione ripristinare i dati di Administration Server nel nuovo dispositivo utilizzando l'utilità klbackup.

   Se si utilizza SQL Server come DBMS nei dispositivi precedenti e nuovi, tenere presente che la versione di SQL Server installata nel nuovo dispositivo deve essere uguale o successiva alla versione di SQL Server installata nel dispositivo precedente. In caso contrario non è possibile recuperare i dati di Administration Server nel nuovo dispositivo.

9. Aprire Administration Console e connettersi all'Administration Server.

10. Verificare che tutti i dispositivi gestiti vengano collegati ad Administration Server.

11. Disinstallare Administration Server e il server del database dal dispositivo precedente.

È inoltre possibile utilizzare Kaspersky Security Center Web Console per spostare Administration Server e il server di un database in un altro dispositivo.

Prevenzione dei conflitti tra più Administration Server

Se sono presenti più Administration Server nella rete, tali server possono visualizzare gli stessi dispositivi client. Ciò può ad esempio causare l'installazione da parte di Administration Server di un'applicazione che era già installata da un altro Administration Server e altri conflitti. Per impedire che un'applicazione venga installata in un dispositivo gestito da un altro Administration Server, è necessario abilitare l'opzione **Installa solo nei dispositivi gestiti tramite questo Administration Server** nelle proprietà dell'attività *Installa l'applicazione in remoto*.

Se si abilita l'opzione **Installa solo nei dispositivi gestiti tramite questo Administration Server** e quindi si esegue l'attività *Installa l'applicazione in remoto*, verrà eseguito un controllo per determinare se i dispositivi sono gestiti da un altro Administration Server. Per i dispositivi gestiti da un altro Administration Server, il valore dell'attributo **Gestito da un altro Administration Server** verrà impostato su `true`. L'attività *Installa l'applicazione in remoto* non verrà applicata a questi dispositivi.

I valori dell'attributo **Gestito da un altro Administration Server** vengono visualizzati nella colonna **Gestito da un altro Administration Server** nell'elenco dei dispositivi gestiti e nell'elenco dei dispositivi non assegnati.

È anche possibile utilizzare la proprietà **Gestito da un altro Administration Server** come criterio per i seguenti scopi:

- Ricerca di dispositivi
- Selezioni dispositivi
- Regole di spostamento dei dispositivi
- Regole di tagging automatico

Per ripristinare l'attributo Gestito da un altro Administration Server:

1. Nel menu principale di Kaspersky Security Center Web Console, passare a **Individuazione e distribuzione** → **Dispositivi non assegnati**.

2. Selezionare il dispositivo richiesto, quindi fare clic sul pulsante **Rimuovere l'attributo Gestito da un altro Administration Server**.

L'attributo **Gestito da un altro Administration Server** viene reimpostato.

Gestione dei gruppi di amministrazione

Questa sezione contiene informazioni su come gestire i gruppi di amministrazione.

È possibile eseguire le seguenti azioni sui gruppi di amministrazione:

- Aggiungere un numero illimitato di gruppi nidificati a qualsiasi livello della gerarchia dei gruppi di amministrazione.
- Aggiungere dispositivi ai gruppi di amministrazione.
- Modificare la gerarchia dei gruppi di amministrazione spostando singoli dispositivi e interi gruppi in altri gruppi.
- Rimuovere gruppi nidificati e dispositivi dai gruppi di amministrazione.
- Aggiungere Administration Server secondari e virtuali ai gruppi di amministrazione.
- Spostare dispositivi dai gruppi di amministrazione di un Administration Server a quelli di un altro server.
- Definire le applicazioni Kaspersky da installare automaticamente nei dispositivi inclusi in un gruppo.

È possibile eseguire queste azioni solo se si dispone dell'autorizzazione **Modifica** nell'area **Gestione dei gruppi di amministrazione** per i gruppi di amministrazione che si desidera gestire (o per l'Administration Server a cui appartengono questi gruppi).

Creazione dei gruppi di amministrazione

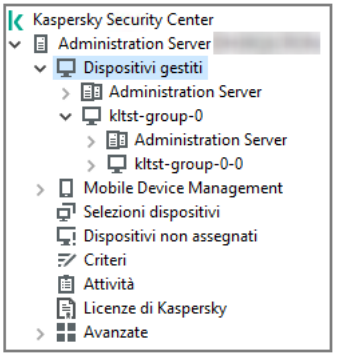
La gerarchia dei gruppi di amministrazione viene creata nella finestra principale dell'applicazione di Kaspersky Security Center, nella cartella **Dispositivi gestiti**. I gruppi di amministrazione sono visualizzati come cartelle nella struttura della console (vedere la figura seguente).

Subito dopo l'installazione di Kaspersky Security Center, la cartella **Dispositivi gestiti** contiene solo una cartella **Administration Server** vuota.

Le impostazioni dell'interfaccia utente determinano se la cartella **Administration Server** appare nella struttura della console. Per visualizzare questa cartella, nella barra dei menu selezionare **Visualizza → Configura interfaccia** e, nella finestra **Configura interfaccia** visualizzata, selezionare la casella di controllo **Visualizza Administration Server secondari**.

Durante la creazione di una gerarchia di gruppi di amministrazione, è possibile aggiungere dispositivi e macchine virtuali alla cartella **Dispositivi gestiti**, nonché aggiungere gruppi nidificati. Gli Administration Server secondari e virtuali possono essere aggiunti alla cartella **Administration Server**.

Come nel caso della cartella **Dispositivi gestiti**, ogni gruppo creato inizialmente contiene solo una cartella **Administration Server** vuota e destinata alla gestione degli Administration Server secondari e virtuali del gruppo. Le informazioni sui criteri e sulle attività per questo gruppo e le informazioni sui dispositivi inclusi in questo gruppo vengono visualizzate nelle schede con i nomi corrispondenti nell'area di lavoro del gruppo.



Visualizzazione della gerarchia di gruppi di amministrazione

Per creare un gruppo di amministrazione:

1. Nella struttura della console espandere la cartella **Dispositivi gestiti**.
2. Se si desidera creare un sottogruppo in un gruppo di amministrazione esistente, nella cartella **Dispositivi gestiti** selezionare una sottocartella corrispondente al gruppo che deve includere il nuovo gruppo di amministrazione.

   Se si crea un nuovo gruppo di amministrazione di primo livello, è possibile ignorare questo passaggio.
3. Avviare la creazione del gruppo di amministrazione in uno dei seguenti modi:
   - Utilizzando il comando **Nuovo→ Gruppo** nel menu di scelta rapida.
   - Facendo clic sul pulsante **Nuovo gruppo** nell'area di lavoro della finestra principale dell'applicazione, nella scheda **Dispositivi**.
4. Nella finestra **Nome gruppo** visualizzata immettere un nome per il gruppo, quindi fare clic su **OK**.

   Una nuova cartella del gruppo di amministrazione con il nome specificato verrà visualizzata nella struttura della console.

L'applicazione consente di creare una gerarchia di gruppi di amministrazione basata sulla struttura di Active Directory o sulla struttura della rete di dominio. È inoltre possibile creare una struttura di gruppi a partire da un file di testo.

Per creare una struttura di gruppi di amministrazione:

1. Nella struttura della console selezionare la cartella **Dispositivi gestiti**.
2. Nel menu di scelta rapida della cartella **Dispositivi gestiti** selezionare **Tutte le attività → Nuova struttura di gruppi**.

   Verrà avviata la Creazione guidata nuova struttura dei gruppi di amministrazione. Seguire le istruzioni della procedura guidata.

Spostamento di gruppi di amministrazione

È possibile spostare i gruppi di amministrazione nidificati all'interno della gerarchia dei gruppi.

Un gruppo di amministrazione viene spostato con tutti i gruppi nidificati, gli Administration Server secondari, i dispositivi, i criteri e le attività di gruppo. Il sistema applica al gruppo tutte le impostazioni che corrispondono alla nuova posizione nella gerarchia dei gruppi di amministrazione.

Il nome del gruppo deve essere univoco all'interno del livello della gerarchia. Se un gruppo con lo stesso nome esiste già nella cartella in cui si sposta il gruppo di amministrazione, è necessario cambiare il nome di quest'ultimo. Se non si modifica il nome del gruppo spostato, dopo lo spostamento al nome viene aggiunto un indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Non è possibile rinominare il gruppo **Dispositivi gestiti** perché si tratta di un elemento predefinito di Administration Console.

Per spostare un gruppo in un'altra cartella nella struttura della console:

1. Selezionare un gruppo da spostare nella struttura della console.
2. Eseguire una delle seguenti operazioni:
   - Spostare il gruppo utilizzando il menu di scelta rapida:
     1. Selezionare **Taglia** nel menu di scelta rapida del gruppo.
     2. Selezionare **Incolla** dal menu di scelta rapida del gruppo di amministrazione in cui si desidera spostare il gruppo selezionato.
   - Spostare il gruppo utilizzando il menu principale dell'applicazione:
     a. Nel menu principale selezionare **Azione** → **Taglia**.
     b. Selezionare nella struttura della console il gruppo di amministrazione in cui si desidera spostare il gruppo selezionato.
     c. Nel menu principale selezionare **Azione** → **Incolla**.
   - Spostare il gruppo in un altro gruppo nella struttura della console utilizzando il mouse.

Eliminazione di gruppi di amministrazione

È possibile eliminare un gruppo di amministrazione se non contiene Administration Server secondari, gruppi nidificati o dispositivi client e purché per tale gruppo di amministrazione non siano stati creati attività o criteri di gruppo.

Prima di eliminare un gruppo di amministrazione, è necessario rimuovere da tale gruppo tutti gli Administration Server secondari, i gruppi nidificati e i dispositivi client.

Per eliminare un gruppo:

1. Selezionare un gruppo di amministrazione nella struttura della console.
2. Eseguire una delle seguenti operazioni:
   - Selezionare **Elimina** nel menu di scelta rapida del gruppo.
   - Nel menu principale dell'applicazione selezionare **Azione** → **Elimina**.
   - Premere **CANC**.

Creazione automatica di una struttura di gruppi di amministrazione

Kaspersky Security Center consente di creare una struttura di gruppi di amministrazione utilizzando la Creazione guidata gerarchia di gruppi.

La procedura guidata crea una struttura di gruppi di amministrazione basata sui seguenti dati:

- Strutture di gruppi di lavoro e domini Windows
- Strutture di gruppi di Active Directory
- Contenuti di un file di testo creato manualmente dall'amministratore

Quando viene generato il file di testo, devono essere soddisfatte le seguenti condizioni:

- Il nome di ogni nuovo gruppo deve iniziare con una nuova riga e il delimitatore deve iniziare con un'interruzione di riga. Le righe vuote vengono ignorate.

  Esempio:
  Ufficio 1
  Ufficio 2
  Ufficio 3
  Nel gruppo di destinazione verranno creati tre gruppi al primo livello della gerarchia.

- Il nome del gruppo nidificato deve essere immesso utilizzando una barra (/).

  Esempio:
  Ufficio 1/Divisione 1/Reparto 1/Gruppo 1
  Nel gruppo di destinazione verranno creati quattro sottogruppi nidificati l'uno nell'altro.

- Per creare più gruppi nidificati allo stesso livello della gerarchia, è necessario specificare il "percorso completo del gruppo".

  Esempio:
  Ufficio 1/Divisione 1/Reparto 1
  Ufficio 1/Divisione 2/Reparto 1
  Ufficio 1/Divisione 3/Reparto 1
  Ufficio 1/Divisione 4/Reparto 1
  Nel gruppo di destinazione verrà creato un solo gruppo al primo livello della gerarchia, che includerà quattro gruppi nidificati allo stesso livello della gerarchia: "Divisione 1", "Divisione 2", "Divisione 3" e "Divisione 4". Ognuno di questi gruppi includerà il gruppo "Reparto 1".

La creazione della gerarchia dei gruppi di amministrazione utilizzando la procedura guidata non influisce sull'integrità della rete: invece di sostituire i gruppi esistenti, vengono aggiunti nuovi gruppi. Un dispositivo client non può essere incluso una seconda volta in un gruppo di amministrazione perché il dispositivo è rimosso dal gruppo **Dispositivi non assegnati** quando viene spostato nel gruppo di amministrazione.

Se, durante la creazione della struttura dei gruppi di amministrazione, un dispositivo non è stato incluso nel gruppo **Dispositivi non assegnati** per qualche motivo (ad esempio, perché era spento o disconnesso dalla rete), il dispositivo non verrà spostato automaticamente nel gruppo di amministrazione. Al termine della procedura guidata, è possibile aggiungere manualmente i dispositivi ai gruppi di amministrazione.

Per avviare la creazione automatica di una struttura di gruppi di amministrazione:

1. Selezionare la cartella **Dispositivi gestiti** nella struttura della console.
2. Nel menu di scelta rapida della cartella **Dispositivi gestiti** selezionare **Tutte le attività** → **Nuova struttura di gruppi**.

   Verrà avviata la Creazione guidata nuova struttura dei gruppi di amministrazione. Seguire le istruzioni della procedura guidata.

Installazione automatica delle applicazioni nei dispositivi di un gruppo di amministrazione

È possibile specificare i pacchetti di installazione da utilizzare per l'installazione remota delle applicazioni Kaspersky nei dispositivi client in un gruppo di amministrazione.

Per configurare l'installazione automatica delle applicazioni nei dispositivi di un gruppo di amministrazione:

1. Nella struttura della console selezionare il gruppo di amministrazione desiderato.
2. Aprire la finestra delle proprietà del gruppo di amministrazione.
3. Nel riquadro **Sezioni** selezionare **Installazione automatica** e nell'area di lavoro selezionare i pacchetti di installazione delle applicazioni da installare nei dispositivi.
4. Fare clic su **OK**.

   Le attività di gruppo vengono create. Queste attività vengono eseguite nei dispositivi client subito dopo essere stati aggiunti al gruppo di amministrazione.

Se per un'applicazione vengono selezionati più pacchetti di installazione per l'installazione automatica, l'attività di installazione viene creata solo per la versione più recente dell'applicazione.

Gestione dei dispositivi client

Questa sezione contiene informazioni sull'utilizzo dei dispositivi client.

Connessione dei dispositivi client ad Administration Server

La connessione del dispositivo client all'Administration Server viene stabilita attraverso il Network Agent installato nel dispositivo client.

Quando un dispositivo client effettua la connessione ad Administration Server, vengono eseguite le seguenti operazioni:

- Sincronizzazione automatica dei dati:
  - Sincronizzazione dell'elenco delle applicazioni installate nel dispositivo client.
  - Sincronizzazione di criteri, impostazioni dell'applicazione, attività e impostazioni delle attività.
- Recupero di informazioni aggiornate sulle condizioni delle applicazioni e di statistiche sull'esecuzione delle applicazioni e delle attività da parte di Administration Server.
- Invio all'Administration Server delle informazioni sugli eventi per l'elaborazione.

La sincronizzazione automatica dei dati viene eseguita periodicamente, in base alle impostazioni di Network Agent (ad esempio, ogni 15 minuti). È possibile specificare l'intervallo di connessione manualmente.

Le informazioni su un evento vengono inviate ad Administration Server non appena si verificano.

> Se un Administration Server è remoto, ovvero all'esterno di una rete aziendale, i dispositivi client vi si connettono tramite Internet.

Per la connessione dei dispositivi client a un Administration Server via Internet, devono essere soddisfatte le seguenti condizioni:

- L'Administration Server remoto deve disporre di un indirizzo IP esterno e la porta in entrata 13000 deve rimanere aperta (per la connessione dei Network Agent). È consigliabile aprire anche la porta UDP 13000 (per la ricezione delle notifiche sullo spegnimento dei dispositivi).
- I Network Agent devono essere installati nei dispositivi.
- Quando si installa Network Agent nei dispositivi, è necessario specificare l'indirizzo IP esterno dell'Administration Server remoto. Se per l'installazione viene utilizzato un pacchetto di installazione, l'indirizzo IP esterno deve essere specificato manualmente nelle proprietà del pacchetto di installazione, nella sezione **Impostazioni**.
- Per utilizzare l'Administration Server remoto al fine di gestire le applicazioni e le attività di un dispositivo, nella sezione **Generale** della finestra delle proprietà di tale dispositivo selezionare la casella di controllo **Non eseguire la disconnessione da Administration Server**. Dopo avere selezionato la casella di controllo, attendere la sincronizzazione di Administration Server con il dispositivo remoto. Il numero di dispositivi client che mantengono una connessione permanente con un Administration Server non può essere superiore a 300.

Per aumentare le prestazioni delle attività generate da un Administration Server remoto, è possibile aprire la porta 15000 in un dispositivo. In questo caso, per eseguire un'attività, l'Administration Server invia uno speciale pacchetto a Network Agent tramite la porta 15000 senza attendere il completamento della sincronizzazione con il dispositivo.

Kaspersky Security Center consente di configurare la connessione tra un dispositivo client e Administration Server in modo che la connessione rimanga attiva dopo che tutte le operazioni sono state completate. Una connessione senza interruzioni è necessaria quando occorre un monitoraggio in tempo reale dello stato delle applicazioni e Administration Server non è in grado di stabilire una connessione al client per qualche motivo (ad esempio, la connessione è protetta da un firewall, l'apertura di porte nel dispositivo client non è consentita o l'indirizzo IP del dispositivo client è sconosciuto). È possibile stabilire una connessione senza interruzioni tra un dispositivo client e Administration Server nella sezione **Generale** della finestra delle proprietà del dispositivo.

È consigliabile stabilire una connessione senza interruzioni con i dispositivi più importanti. Il numero totale di connessioni mantenute contemporaneamente da Administration Server è limitato a 300.

In caso di sincronizzazione manuale, il sistema utilizza un metodo di connessione ausiliario, per cui la connessione viene avviata da Administration Server. Prima di stabilire la connessione in un dispositivo client, è necessario aprire la porta UDP. Administration Server invia una richiesta di connessione alla porta UDP del dispositivo client. In risposta, verrà verificato il certificato di Administration Server. Se il certificato di Administration Server corrisponde alla copia archiviata nel dispositivo client, viene stabilita la connessione.

L'avvio manuale della sincronizzazione è inoltre utilizzato per ottenere informazioni aggiornate sulle condizioni delle applicazioni, l'esecuzione delle attività e le statistiche sul funzionamento delle applicazioni.

Connessione manuale di un dispositivo client ad Administration Server. Utilità Klmover

Se è necessario eseguire manualmente la connessione di un dispositivo client ad Administration Server, è possibile utilizzare l'utilità klmover nel dispositivo client.

Quando si installa Network Agent su un dispositivo client, l'utilità viene automaticamente copiata nella cartella di installazione di Network Agent.

Per connettere manualmente un dispositivo client ad Administration Server utilizzando l'utilità klmover:

Nel dispositivo avviare l'utilità klmover dalla riga di comando.

Quando viene avviata dalla riga di comando, l'utilità klmover può eseguire le seguenti operazioni (a seconda delle chiavi in uso):

- Connette Network Agent ad Administration Server con le impostazioni specificate.
- Memorizza i risultati dell'operazione nel file del registro eventi o li visualizza sullo schermo.

Non è possibile utilizzare l'utilità klmover per i dispositivi client connessi ad Administration Server tramite gateway di connessione. Per tali dispositivi è necessario riconfigurare Network Agent o reinstallarlo e specificare il gateway di connessione.

Sintassi della riga di comando per l'utilità:

```
klmover [-logfile <nome file>] [-address <indirizzo server>] [-pn <numero porta>] [-
ps <numero porta SSL>] [-nossl] [-cert <percorso del file di certificato>] [-silent]
[-dupfix] [-virtserv] [-cloningmode]
```

I diritti di amministratore sono necessari per eseguire l'utilità.

Descrizioni delle chiavi:

- `-logfile <nome file>`: ,emorizza i risultati dell'esecuzione dell'utilità in un file di registro.

  Per impostazione predefinita, le informazioni vengono salvate nel flusso di output standard (stdout). Se la chiave non è in uso, i risultati e i messaggi di errore sono visualizzati sullo schermo.

- `-address <indirizzo server>`: indirizzo dell'Administration Server a cui connettersi.

  È possibile specificare un indirizzo IP, il nome NetBIOS o il nome DNS di un dispositivo come indirizzo.

- `-pn <numero porta>`: numero della porta tramite la quale viene stabilita la connessione non criptata ad Administration Server.

  Il numero di porta predefinito è 14000.

- `-ps <numero porta SSL>`: numero della porta SSL tramite la quale viene stabilita la connessione criptata ad Administration Server utilizzando il protocollo SSL.

  Il numero di porta predefinito è 13000.

- `-nossl`: utilizza la connessione non criptata ad Administration Server.

  Se la chiave non è in uso, Network Agent è connesso ad Administration Server tramite il protocollo SSL criptato.

- `-cert <percorso del file di certificato>`: utilizza il file di certificato specificato per l'autenticazione di accesso ad Administration Server.

  Se la chiave non è in uso, Network Agent riceve un certificato alla prima connessione ad Administration Server.

- `-silent`: esegue l'utilità in modalità automatica.

  L'utilizzo della chiave potrebbe ad esempio essere utile se l'utilità viene avviata dallo script di accesso alla registrazione dell'utente.

- `-dupfix`: l'opzione è utilizzata se Network Agent è stato installato tramite un metodo diverso da quello usuale (con il pacchetto di distribuzione), ad esempio ripristinandolo da un'immagine disco ISO.

- `-virtserv`: nome dell'Administration Server virtuale.

- `-cloningmode`: modalità di clonazione del disco di Network Agent.

  Utilizzare uno dei seguenti parametri per configurare la modalità di clonazione del disco:

  - `-cloningmode`: richiede lo stato della modalità di clonazione del disco.
  - `-cloningmode 1`: abilita la modalità di clonazione del disco.
  - `-cloningmode 0`: disabilita la modalità di clonazione del disco.

- `-nauninstpwd <password>`: la chiave viene utilizzata per specificare la password di disinstallazione di Network Agent.

  La chiave non è obbligatoria.

Ad esempio, per connettere Network Agent ad Administration Server, eseguire il seguente comando:

```
klmover -address kscserver.mycompany.com -logfile klmover.log
```

Tunneling della connessione tra un dispositivo client e Administration Server

Kaspersky Security Center consente il tunneling delle connessioni TCP da Administration Console tramite l'Administration Server e quindi tramite Network Agent su una porta specificata in un dispositivo gestito. Il tunneling è progettato per la connessione di un'applicazione client su un dispositivo con Administration Console installato a una porta TCP in un dispositivo gestito, se non è possibile la connessione diretta tra Administration Console e il dispositivo di destinazione.

Il tunneling viene ad esempio utilizzato per le connessioni a un desktop remoto, sia per connettersi a una sessione esistente che per creare una nuova sessione remota.

È anche possibile abilitare il tunneling utilizzando strumenti esterni. L'amministratore può ad esempio eseguire l'utilità putty, il client VNC e altri strumenti in questo modo.

Il tunneling della connessione tra un dispositivo client remoto e Administration Server è richiesto se la porta utilizzata per la connessione ad Administration Server non è disponibile nel dispositivo. La porta nel dispositivo potrebbe non essere disponibile nei seguenti casi:

- Il dispositivo remoto è connesso a una rete locale che utilizza il meccanismo NAT.
- Il dispositivo remoto fa parte della rete locale di Administration Server, ma la relativa porta è chiusa da un firewall.

Per eseguire il tunneling della connessione tra un dispositivo client e Administration Server:

1. Nella struttura della console selezionare la cartella del gruppo che include il dispositivo client.
2. Nella scheda **Dispositivi** selezionare il dispositivo.
3. Nel menu di scelta rapida del dispositivo selezionare **Tutte le attività** → **Tunneling connessione**.
4. Creare un tunnel nella finestra **Tunneling connessione** visualizzata.

Connessione remota al desktop di un dispositivo client

L'amministratore può accedere in remoto al desktop di un dispositivo client attraverso Network Agent installato nel dispositivo client.

La connessione remota a un dispositivo tramite Network Agent è possibile anche se le porte TCP e UDP del dispositivo client sono chiuse. Dopo avere stabilito la connessione con il dispositivo, l'amministratore ottiene l'accesso completo alle informazioni memorizzate in tale dispositivo e può gestire le applicazioni installate.

Questa sezione descrive come stabilire una connessione con un dispositivo client Windows e un dispositivo client macOS tramite Network Agent.

Connessione ai dispositivi client Windows

Può essere stabilita la connessione remota con un dispositivo client Windows in uno dei seguenti modi:

- Utilizzando un componente standard di Microsoft Windows denominato Connessione Desktop remoto.

  La connessione a un desktop remoto viene stabilita attraverso l'utilità standard di Windows mstsc.exe in base alle impostazioni dell'utilità.

- Utilizzando la tecnologia Condivisione desktop Windows.

Connessione al dispositivo client Windows tramite Connessione Desktop remoto

La connessione alla sessione di desktop remoto corrente dell'utente viene stabilita senza che l'utente ne sia a conoscenza. Una volta che l'amministratore si è connesso alla sessione, l'utente del dispositivo viene disconnesso dalla sessione senza preavviso.

Per connettersi al desktop di un dispositivo client tramite il componente Connessione Desktop remoto:

1. Nella struttura di Administration Console selezionare il dispositivo a cui è necessario ottenere l'accesso.
2. Nel menu di scelta rapida del dispositivo selezionare **Tutte le attività → Connetti al dispositivo → Nuova sessione RDP**.

   Verrà avviata l'utilità standard di Windows mstsc.exe, che consente stabilire la connessione al desktop remoto.
3. Seguire le istruzioni visualizzate nelle finestre di dialogo dell'utilità.

Quando viene stabilita la connessione con il dispositivo, il desktop è disponibile nella finestra Connessione Desktop remoto di Microsoft Windows.

Connessione al dispositivo client Windows tramite Condivisione desktop Windows

Quando ci si connette a una sessione esistente di desktop remoto, l'utente della sessione nel dispositivo client riceve una richiesta per la connessione dall'amministratore. Nei rapporti creati da Kaspersky Security Center non sarà salvata alcuna informazione sull'attività remota nel dispositivo né sui relativi risultati.

L'amministratore può connettersi a una sessione esistente in un dispositivo client senza disconnettere l'utente in questa sessione. In questo caso, l'amministratore e l'utente della sessione nel dispositivo condividono l'accesso al desktop.

L'amministratore può configurare un controllo dell'attività dell'utente in un dispositivo client remoto. Durante il controllo, l'applicazione salva le informazioni sui file nel dispositivo client che sono stati aperti e/o modificati dall'amministratore.

Per connettersi al desktop di un dispositivo client tramite Condivisione desktop Windows, devono essere soddisfatte le seguenti condizioni:

- Microsoft Windows Vista o versione successiva è installato nella workstation dell'amministratore. Il tipo di sistema operativo del dispositivo che contiene Administration Server non impone alcuna limitazione alla connessione tramite Condivisione desktop Windows.

  Per verificare se la funzionalità Condivisione desktop Windows è inclusa nella versione di Windows in uso, assicurarsi che la chiave CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} sia presente nel Registro di sistema di Windows.

- Microsoft Windows Vista o versione successiva è installato nel dispositivo client.

- Kaspersky Security Center utilizza una licenza per Vulnerability e patch management.

Per connettersi al desktop di un dispositivo client tramite Condivisione desktop Windows:

1. Nella struttura di Administration Console selezionare il dispositivo a cui è necessario ottenere l'accesso.

2. Nel menu di scelta rapida del dispositivo selezionare **Tutte le attività** → **Connetti al dispositivo** → **Condivisione desktop Windows**.

3. Nella finestra **Seleziona sessione Desktop remoto** visualizzata selezionare la sessione nel dispositivo a cui è necessario connettersi.

   Se la connessione al dispositivo viene stabilita correttamente, il desktop del dispositivo sarà disponibile nella finestra **Visualizzatore sessione Desktop remoto Kaspersky**.

4. Per iniziare a interagire con il dispositivo, nel menu principale della finestra **Visualizzatore sessione Desktop remoto Kaspersky** selezionare **Azioni** → **Modalità interattiva**.

L'utilità **Visualizzatore sessione Desktop remoto Kaspersky** richiede una licenza commerciale.

Connessione ai dispositivi client macOS

L'amministratore può utilizzare il sistema VNC (Virtual Network Computing) per connettersi ai dispositivi macOS.

La connessione a un desktop remoto viene stabilita tramite un client VNC installato nel dispositivo Administration Server. Il client VNC passa il controllo della tastiera e del mouse dal dispositivo client all'amministratore.

Quando l'amministratore si connette al desktop remoto, l'utente non riceve notifiche o richieste di connessione dall'amministratore. L'amministratore si connette a una sessione esistente nel dispositivo client senza disconnettere l'utente da questa sessione.

Per connettersi al desktop di un dispositivo macOS client tramite il client VNC, devono essere soddisfatte le seguenti condizioni:

- Il client VNC è installato nel dispositivo Administration Server.
- L'accesso remoto e la gestione remota sono consentiti sul dispositivo client.
- L'utente ha consentito all'amministratore di accedere al dispositivo client nelle impostazioni **Condivisione** del sistema operativo macOS.

Per connettersi al desktop di un dispositivo client tramite il sistema VNC:

1. Nella struttura di Administration Console selezionare il dispositivo a cui è necessario ottenere l'accesso.
2. Nel menu di scelta rapida del dispositivo selezionare **Tutte le attività → Tunneling connessione**.
3. Nella finestra **Tunneling connessione** visualizzata, procedere come segue:
   a. Nella sezione **1. Porta di rete**, specificare il numero della porta di rete del dispositivo a cui è necessario connettersi.
      Per impostazione predefinita, viene utilizzata la porta 5900.
   b. Nella sezione **2. Tunneling**, fare clic sul pulsante **Crea tunnel**.
   c. Nella sezione **3. Impostazioni di rete**, fare clic sul pulsante **Copia**.
4. Aprire il client VNC e incollare gli attributi di rete copiati nel campo di testo. Premere **`Invio`**.
5. Nella finestra visualizzata, visualizzare i dettagli del certificato: Se si accetta di utilizzare il certificato, fare clic sul pulsante **Sì**.
6. Nella finestra **Autenticazione**, specificare le credenziali del dispositivo client, quindi fare clic su **OK**.

Connessione ai dispositivi tramite Condivisione desktop Windows

Per eseguire la connessione a un dispositivo tramite Condivisione desktop Windows:

1. Nella struttura della console, nella scheda **Dispositivi**, selezionare la cartella **Dispositivi gestiti**.
   Nell'area di lavoro di questa cartella viene visualizzato un elenco di dispositivi.
2. Nel menu di scelta rapida del dispositivo a cui si desidera eseguire la connessione selezionare **Connetti al dispositivo → Condivisione desktop Windows**.
   Verrà visualizzata la finestra **Seleziona sessione Desktop remoto**.
3. Nella finestra **Seleziona sessione Desktop remoto** selezionare una sessione desktop per la connessione al dispositivo.
4. Fare clic su **OK**.

Il dispositivo sarà connesso.

Configurazione del riavvio di un dispositivo client

Durante l'utilizzo, l'installazione o la rimozione di Kaspersky Security Center, potrebbe essere necessario riavviare il dispositivo. È possibile specificare le impostazioni di riavvio solo per i dispositivi che eseguono Windows.

Per configurare il riavvio di un dispositivo client:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui configurare il riavvio.
2. Nell'area di lavoro del gruppo selezionare la scheda **Criteri**.
3. Nell'area di lavoro selezionare un criterio di Kaspersky Security Center Network Agent nell'elenco dei criteri, quindi selezionare **Proprietà** nel menu di scelta rapida del criterio.
4. Nella finestra delle proprietà del criterio, selezionare la sezione **Gestione riavvio**.
5. Selezionare l'azione che deve essere eseguita se è richiesto il riavvio del dispositivo:
   - Selezionare **Non riavviare il sistema operativo** per bloccare il riavvio automatico.
   - Selezionare **Riavvia automaticamente il sistema operativo se necessario** per consentire il riavvio automatico.
   - Selezionare **Richiedi l'intervento dell'utente** per abilitare la richiesta di conferma del riavvio da parte dell'utente.

   È possibile specificare la frequenza delle richieste di riavvio e abilitare il riavvio forzato e la chiusura forzata delle applicazioni nelle sessioni bloccate nel dispositivo, selezionando le caselle di controllo corrispondenti e le impostazioni per gli orari.
6. Fare clic su **OK** per salvare le modifiche e chiudere la finestra delle proprietà del criterio.

A questo punto verrà configurato il riavvio del dispositivo.

Controllo delle azioni in un dispositivo client remoto

L'applicazione consente il controllo delle azioni dell'amministratore in un dispositivo client remoto che esegue Windows. Durante il controllo, l'applicazione salva nel dispositivo le informazioni sui file che sono stati aperti e/o modificati dall'amministratore. Il controllo delle azioni dell'amministratore è disponibile quando sono soddisfatte le seguenti condizioni:

- È in uso la licenza per Vulnerability e patch management.
- L'amministratore dispone del diritto per l'avvio dell'accesso condiviso al desktop del dispositivo remoto.

Per abilitare il controllo delle azioni in un dispositivo client remoto:

1. Nella struttura della console selezionare il gruppo di amministrazione per cui configurare il controllo delle azioni dell'amministratore.
2. Nell'area di lavoro del gruppo selezionare la scheda **Criteri**.

3. Selezionare un criterio di Kaspersky Security Center Network Agent, quindi selezionare **Proprietà** nel menu di scelta rapida del criterio.

4. Nella finestra delle proprietà del criterio selezionare la sezione **Condivisione desktop Windows**.

5. Selezionare la casella di controllo **Abilita controllo**.

6. Negli elenchi **Maschere dei file da monitorare durante la lettura** e **Maschere dei file da monitorare durante la modifica** aggiungere maschere file in cui l'applicazione deve monitorare le azioni durante il controllo.

   Per impostazione predefinita, l'applicazione monitora le azioni effettuate sui file con estensione .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt e .pdf.

7. Fare clic su **OK** per salvare le modifiche e chiudere la finestra delle proprietà del criterio.

Verrà configurato il controllo delle azioni eseguite dall'amministratore nel dispositivo remoto dell'utente con accesso desktop condiviso.

I record relativi alle azioni dell'amministratore nel dispositivo remoto vengono registrati:

- Nel registro eventi del dispositivo remoto.
- In un file con estensione syslog nella cartella Network Agent di un dispositivo remoto (ad esempio, C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- Nel database degli eventi di Kaspersky Security Center.

Verifica della connessione tra un dispositivo client e Administration Server

Kaspersky Security Center consente di controllare le connessioni tra un dispositivo client e Administration Server automaticamente o manualmente.

La verifica automatica della connessione viene eseguita sull'Administration Server. La verifica manuale della connessione viene eseguita sul dispositivo.

Verifica automatica della connessione tra un dispositivo client e Administration Server

Per avviare una verifica automatica della connessione tra un dispositivo client e Administration Server:

1. Nella struttura della console selezionare il gruppo di amministrazione che include il dispositivo.

2. Nell'area di lavoro del gruppo di amministrazione selezionare il dispositivo nella scheda **Dispositivi**.

3. Nel menu di scelta rapida del dispositivo selezionare **Verifica possibilità di accesso al dispositivo**.

Verrà visualizzata una finestra che contiene le informazioni sull'accessibilità del dispositivo.

Verifica manuale della connessione tra un dispositivo client e Administration Server. Utilità Klnagchk

È possibile verificare la connessione e ottenere informazioni dettagliate sulle impostazioni della connessione tra un dispositivo client e Administration Server utilizzando l'utilità klnagchk. L'utilità klnagchk si trova nella cartella di installazione di Network Agent.

Quando viene avviata dalla riga di comando, l'utilità klnagchk può eseguire le seguenti azioni (a seconda delle chiavi in uso):

- Visualizzare sullo schermo o registrare i valori delle impostazioni utilizzate per la connessione del Network Agent installato nel dispositivo ad Administration Server.
- Visualizzare sullo schermo o memorizzare in un file del registro eventi le statistiche di Network Agent (dal suo ultimo avvio) e i risultati dell'esecuzione dell'utilità.
- Tentativo di stabilire una connessione tra Network Agent e Administration Server.

  Se il tentativo di connessione non riesce, l'utilità invia un pacchetto ICMP per verificare lo stato del dispositivo in cui è installato Administration Server.

Per controllare la connessione tra il dispositivo client e Administration Server tramite l'utilità klnagchk:

Nel dispositivo in cui è installato Network Agent, avviare l'utilità klnagchk dalla riga di comando con un account di amministratore locale.

Sintassi della riga di comando per l'utilità:

```
klnagchk [-logfile <nome file>] [-sp] [-savecert <percorso del file di certificato>]
[-restart][-sendhb]
```

Descrizioni delle chiavi:

- `-logfile <nome file>`: memorizza in un file di registro i valori delle impostazioni della connessione tra Network Agent e Administration Server e i risultati dell'esecuzione dell'utilità.

  Per impostazione predefinita, le informazioni vengono salvate nel flusso di output standard (stdout). Se la chiave non è in uso, le impostazioni, i risultati e i messaggi di errore sono visualizzati sullo schermo.
- `--sp`: mostra la password per l'autenticazione dell'utente sul server proxy.

  La chiave è in uso se la connessione ad Administration Server è stabilita tramite un server proxy.
- `-savecert <nome file>`: salva il certificato utilizzato per l'accesso ad Administration Server in un file specificato.
- `-restart`: avvia Network Agent al termine dell'esecuzione dell'utilità.
- `-sendhb`: avvia la sincronizzazione di Network Agent con Administration Server.

Dopo l'avvio, l'utilità klnagchk accede ai file di configurazione di Network Agent e mostra i parametri di connessione. Questi parametri vengono specificati durante l'installazione di Network Agent e nelle impostazioni dei criteri di Network Agent:

- `Current device`: nome di rete di Windows del dispositivo client.
- `Network Agent version`: numero completo della versione di Network Agent (con patch) installata nel dispositivo
- `Administration Server address`: indirizzo di Administration Server.
- `Use SSL`: parametro che indica se viene utilizzata una connessione protetta durante la connessione ad Administration Server.

  Valori possibili:

  - 0: non viene utilizzata la connessione sicura.
  - 1: viene utilizzata la connessione sicura.
- `Compress traffic`: parametro che indica se il traffico tra il dispositivo client e Administration Server è compresso.
- `Numbers of the Administration Server SSL ports`: numeri di porte valide per la comunicazione con Administration Server quando si utilizza una connessione protetta.
- `Numbers of the Administration Server ports`: numeri di porte valide per la comunicazione con Administration Server quando si utilizza una connessione normale.
- `Use proxy server`: parametro che indica se viene utilizzato un server proxy.

  Valori possibili:

  - 0: non viene utilizzato il server proxy.
  - 1: viene utilizzato il server proxy.
- `Address`: indirizzo e porta del server proxy separati da due punti. Questo parametro viene visualizzato solo se viene utilizzato un server proxy.
- `User name`: nome utente per l'accesso al server proxy. Questo parametro viene visualizzato solo se viene utilizzato un server proxy.
- `Password`: password per l'accesso al server proxy. Questo parametro viene visualizzato solo se viene utilizzato un server proxy. Per mostrare la password del server proxy, è necessario utilizzare la chiave `sp` nel comando.
- `Administration Server certificate`: parametro che indica se il dispositivo client dispone di un certificato di Administration Server. Un certificato potrebbe non esistere, ad esempio, se Network Agent non si è mai connesso correttamente ad Administration Server.

  Valori possibili:

  - `not installed`: il dispositivo client non dispone di un certificato di Administration Server.
  - `available`: il dispositivo client dispone di un certificato di Administration Server.

- `Open UDP port`: parametro che indica se Network Agent utilizza la porta UDP per ricevere le richieste di sincronizzazione da Administration Server.

  Valori possibili:

  - 0: la porta UDP è chiusa per la ricezione delle richieste di sincronizzazione da Administration Server.
  - 1: la porta UDP è aperta per la ricezione delle richieste di sincronizzazione da Administration Server.

- `Numbers of UDP ports`: numero di porte UDP che possono essere utilizzate da Network Agent.
- `Location name`: posizione di rete del dispositivo.
- `State of network location`: parametro che indica se il dispositivo client può essere spostato da un profilo di connessione di Administration Server a un altro.

  Valori possibili:

  - `Enabled`: il profilo di connessione di Administration Server può essere cambiato per il dispositivo client.
  - `Disabled`: il profilo di connessione di Administration Server non può essere cambiato per il dispositivo client.

- `Profile to use`: profilo di connessione per Administration Server.
- `Condition`: indirizzo IP e subnet mask della rete a cui è connesso il dispositivo client.
- `Synchronization interval (min)`: intervallo standard tra le sincronizzazioni.
- `Connection timeout (in seconds)`: timeout della connessione.
- `Send / receive timeout (in seconds)`: timeout di connessione delle operazioni di lettura-scrittura.
- `Device ID`: identificativo del dispositivo nella rete. L' `Device ID` è univoco nei dispositivi client gestiti da un determinato Administration Server.
- `Locations of connection gateways`: parametri per la connessione del dispositivo client ad Administration Server tramite il gateway di connessione.
- `Location of distribution points`: parametri per la connessione del dispositivo client ad Administration Server tramite il punto di distribuzione.

- `Connection with server`: parametro che indica se il gateway di connessione dispone di una connessione continua ad Administration Server. Il parametro viene visualizzato solo se il dispositivo client funge da gateway di connessione.

  Valori possibili:

  - `active`: il gateway di connessione dispone di una connessione continua ad Administration Server.
  - `inactive`: il gateway di connessione non dispone di una connessione continua ad Administration Server.

- `Connection with server through connection gateway`: parametro che indica se la connessione ad Administration Server tramite un gateway di connessione è stata stabilita correttamente. Il parametro viene visualizzato solo se il dispositivo client funge da gateway di connessione.

  Valori possibili:

  - `active`: La connessione ad Administration Server tramite un gateway di connessione viene stabilita correttamente.
  - `inactive`: La connessione ad Administration Server tramite un gateway di connessione viene stabilita in modo errato.

Inoltre, l'output dell'utilità klnagchk può contenere una delle seguenti righe:

- `Administration Server is installed on this device`: l'utilità klnagchk viene eseguita nel dispositivo di Administration Server.
- `This device has been assigned a connection gateway but is not yet registered on Administration Server`: l'utilità klnagchk viene eseguita nel dispositivo in cui è installato Network Agent, in modalità gateway di connessione. Il gateway di connessione configurato è in attesa di una connessione da Administration Server, ma Administration Server non elenca il dispositivo tra i dispositivi gestiti. È necessario assicurarsi che Administration Server avvii una connessione al gateway di connessione.
- `This device is a connection gateway`: l'utilità klnagchk viene eseguita nel dispositivo che funge da gateway di connessione.
- `Acts as a distribution point`: l'utilità klnagchk viene eseguita nel dispositivo che funge da punto di distribuzione.

L'utilità klnagchk controlla lo stato del servizio Network Agent. Se il servizio non è in esecuzione, l'utilità si arresta. Se il servizio è in esecuzione, l'utilità mostra le seguenti statistiche di connessione:

- `Total number of synchronization requests`: numero di tentativi di connessione del dispositivo client ad Administration Server.
- `The number of successful synchronization request`: numero di tentativi riusciti di connessione del dispositivo client ad Administration Server.
- `Total number of synchronizations`: numero di tentativi di sincronizzazione delle impostazioni del dispositivo client con le impostazioni di Administration Server.
- `The number of successful synchronizations`: numero di tentativi riusciti di sincronizzazione delle impostazioni del dispositivo client con Administration Server.
- `Date/time of the last request for synchronization`: data e ora dell'ultima connessione.

È necessario utilizzare i parametri `Total number of synchronization requests` e `The number of successful synchronization request` durante l'analisi della connessione tra Administration Server e Network Agent. Le impostazioni del dispositivo client si sincronizzano con le impostazioni di Administration Server solo se le impostazioni di Administration Server sono state modificate (ad esempio, se sono state aggiunte nuove attività o se sono state modificate le impostazioni dei criteri). In caso contrario, i valori dei parametri `Total number of synchronizations` e `The number of successful synchronizations` rimangono invariati.

Per ulteriori informazioni su come risolvere i problemi relativi alla connessione di Network Agent ad Administration Server, fare riferimento a Domande frequenti su Kaspersky Security Center.

Informazioni sul controllo del tempo di connessione tra un dispositivo e Administration Server

Al momento dell'arresto di un dispositivo, Network Agent invia una notifica all'Administration Server di questo evento. In Administration Console il dispositivo è visualizzato come arrestato. Tuttavia, Network Agent non può notificare ad Administration Server tutti gli eventi di questo tipo. Administration Server, pertanto, analizza periodicamente l'attributo **Connesso ad Administration Server** (il valore di questo attributo è visualizzato in Administration Console, nella sezione **Generale** delle proprietà del dispositivo) per ogni dispositivo e lo confronta con l'intervallo di sincronizzazione nelle impostazioni correnti di Network Agent. Se un dispositivo non risponde per più di tre intervalli di sincronizzazione consecutivi, il dispositivo è contrassegnato come arrestato.

Identificazione dei dispositivi client in Administration Server

I dispositivi client sono identificati in base ai relativi nomi. Ogni dispositivo connesso ad Administration Server ha un nome univoco.

Il nome di un dispositivo è trasmesso ad Administration Server quando viene eseguito il polling della rete Windows ed è rilevato un nuovo dispositivo oppure durante la prima connessione ad Administration Server da parte del Network Agent installato in un dispositivo client. Per impostazione predefinita, il nome corrisponde al nome del dispositivo nella rete Windows (nome NetBIOS). Se un dispositivo con lo stesso nome è già registrato in Administration Server, al nome del dispositivo viene aggiunto un indice con un numero progressivo, ad esempio: **<Nome>-1**, **<Nome>-2**. Il dispositivo viene aggiunto al gruppo di amministrazione con questo nome.

Spostamento dei dispositivi in un gruppo di amministrazione

È possibile spostare i dispositivi da un gruppo di amministrazione a un altro solo se si dispone dell' autorizzazione **Modifica** nell'area **Gestione dei gruppi di amministrazione per i gruppi di amministrazione** di origine e di destinazione (o per l'Administration Server a cui appartengono questi gruppi).

Per includere uno o più dispositivi in un gruppo di amministrazione selezionato:

1. Nella struttura della console espandere la cartella **Dispositivi gestiti**.
2. Nella cartella **Dispositivi gestiti** selezionare la sottocartella che corrisponde al gruppo in cui saranno inclusi i dispositivi client.

   Se si desidera includere i dispositivi nel gruppo **Dispositivi gestiti**, è possibile saltare questo passaggio.
3. Nell'area di lavoro del gruppo di amministrazione selezionato, nella scheda **Dispositivi**, avviare il processo per includere i dispositivi nel gruppo in uno dei seguenti modi:

   - Aggiungendo i dispositivi al gruppo facendo clic sul pulsante **Sposta i dispositivi nel gruppo** nella finestra di informazioni dell'elenco dei dispositivi
   - Selezionando **Crea** → **Dispositivo** nel menu di scelta rapida dell'elenco dei dispositivi

   Verrà avviato lo Spostamento guidato dispositivi. Seguendo le istruzioni visualizzate, selezionare un metodo per spostare i dispositivi nel gruppo e creare un elenco di dispositivi da includere nel gruppo.

   Se l'elenco di dispositivi viene creato manualmente, è possibile utilizzare l'indirizzo IP (o un intervallo IP), un nome NetBIOS o un nome DNS come indirizzo di un dispositivo. È possibile spostare manualmente nell'elenco solo i dispositivi per cui sono già state aggiunte informazioni al database di Administration Server durante la connessione del dispositivo o dopo la device discovery.

   Per importare un elenco di dispositivi da un file, specificare un file TXT con l'elenco di indirizzi dei dispositivi da aggiungere. Ogni indirizzo deve essere specificato in una riga distinta.

Al termine della procedura guidata, i dispositivi selezionati vengono inclusi nel gruppo di amministrazione e visualizzati nell'elenco di dispositivi con i nomi generati da Administration Server.

È possibile spostare un dispositivo nel gruppo di amministrazione selezionato trascinandolo dalla cartella **Dispositivi non assegnati** nella cartella del gruppo di amministrazione.

Modifica di Administration Server per i dispositivi client

È possibile sostituire l'Administration Server che gestisce i dispositivi client con un altro server mediante l'attività Cambia Administration Server.

Per sostituire l'Administration Server che gestisce i dispositivi client con un altro server:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Nell'area di lavoro di questa cartella fare clic sul pulsante **Nuova attività**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nel passaggio **Selezionare il tipo di attività**, selezionare il nodo **Kaspersky Security Center Administration Server**, espandere la cartella **Avanzate**, quindi selezionare l'attività **Cambia Administration Server**.
4. Nella finestra visualizzata, fare clic sul pulsante **OK** per confermare di accettare i termini di modifica dell'Administration Server per i dispositivi client.

5. Nel passaggio **Impostazioni** della procedura guidata, selezionare l'Administration Server che si desidera utilizzare per gestire i dispositivi selezionati:

   - **Passa a un altro Administration Server primario**

     Per spostare i dispositivi client su un altro Administration Server primario, specificare le seguenti impostazioni di connessione dell'Administration Server:

     1. Nel campo **Administration Server** specificare l'indirizzo del nuovo Administration Server primario.
     2. Nel campo **Porta**, specificare il numero di porta per connettersi all'Administration Server.

        Il numero di porta predefinito è 14000.
     3. Nel campo **Porta SSL**, specificare il numero della porta SSL nell'Administration Server primario.

        Il numero di porta predefinito è 13000.
     4. Se necessario, selezionare la casella di controllo **Usa server proxy**.

        Se questa casella di controllo è deselezionata, viene utilizzata la connessione diretta per connettere il dispositivo ad Administration Server.

        Se questa casella di controllo è selezionata, specificare i parametri del server proxy:

        - **Indirizzo server proxy**
        - **Porta server proxy**

        Se il server proxy richiede l'autenticazione, nei campi **Nome utente** e **Password** specificare le credenziali dell'account con cui viene stabilita la connessione al server proxy. È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.
     5. Se necessario, caricare un nuovo certificato di Administration Server.

   - **Passa a un altro server virtuale in questo server primario**

     Selezionare questa opzione per spostare i dispositivi client sull'Administration Server virtuale sull'Administration Server primario corrente. A tale scopo, nel campo **Nome Administration Server virtuale**, specificare il nome dell'Administration Server virtuale necessario.

   Se necessario, specificare il tempo di attesa prima di riavviare Network Agent.

6. In questa fase della procedura guidata, selezionare i dispositivi a cui verrà assegnata l'attività:

   - **Seleziona i dispositivi della rete rilevati da Administration Server**. In questo caso l'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

   - **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**. È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

   - **Assegna un'attività a una selezione dispositivi**. In questo caso l'attività viene assegnata ai dispositivi inclusi in una selezione creata precedentemente. È possibile specificare la selezione predefinita o una selezione personalizzata creata.

   - **Assegna un'attività a un gruppo di amministrazione**. In questo caso, l'attività viene assegnata ai dispositivi inclusi nel gruppo di amministrazione creato precedentemente.

7. Nel passaggio **Selezione di un account per l'esecuzione dell'attività** della procedura guidata, specificare le impostazioni dell'account:

   - Account predefinito

     L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

     Per impostazione predefinita, questa opzione è selezionata.

   - Specifica account

     Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

     - Account

       Account tramite il quale viene eseguita l'attività.

     - Password

       Password dell'account con cui verrà eseguita l'attività.

8. Nel passaggio **Configurare la pianificazione delle attività** della procedura guidata è possibile creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvio pianificato:**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Giornaliera (ora legale non supportata)**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. Questa pianificazione non supporta l'ora legale. In altre parole, se l'orologio del sistema si sposta avanti o indietro di un'ora all'inizio o alla fine dell'ora legale, l'ora di inizio effettiva dell'attività non cambia.

    Non è consigliabile utilizzare questa pianificazione. È necessaria per la compatibilità con le versioni precedenti di Kaspersky Security Center.

    Per impostazione predefinita, l'attività viene avviata ogni giorno all'ora di sistema corrente.

  - **In base ai giorni della settimana**

    L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

  - **Mensile**

    L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

    Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

    Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

  - **Una sola volta**

    L'attività viene eseguita una volta, nella data e nell'ora specificate (per impostazione predefinita, il giorno in cui è stata creata l'attività).

  - **Manualmente**

    L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Immediatamente**

    L'attività viene eseguita immediatamente dopo che il dispositivo diventa visibile sulla rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

- **Esegui attività non effettuate**

Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

9. In questa fase della procedura guidata, specificare il nome dell'attività in fase di creazione.
10. Nel passaggio **Completare la creazione dell'attività** della procedura guidata fare clic sul pulsante **Fine** per chiudere la procedura guidata.

    Se si desidera che l'attività venga avviata al termine della Creazione guidata, selezionare la casella di controllo **Esegui l'attività al termine della procedura guidata**.

Dopo il completamento dell'attività, i dispositivi client per cui è stata creata passano sotto la gestione dell'Administration Server specificato nelle impostazioni dell'attività.

Se l'Administration Server supporta il criptaggio e la protezione dei dati e si sta creando un'attività Cambia Administration Server, viene visualizzato un avviso. L'avviso indica che, se nei dispositivi sono contenuti dati criptati, quando il nuovo server inizia a gestire i dispositivi, gli utenti saranno in grado di accedere solo ai dati criptati che hanno utilizzato in precedenza. In nessun altro caso sarà possibile accedere ai dati criptati. Per descrizioni dettagliate degli scenari in cui non è possibile accedere ai dati criptati, fare riferimento alla Guida di Kaspersky Endpoint Security for Windows.

Spostamento dei dispositivi connessi ad Administration Server tramite gateway di connessione a un altro Administration Server

È possibile spostare i dispositivi connessi ad Administration Server tramite i gateway di connessione in un altro Administration Server. Questa operazione potrebbe ad esempio essere necessaria se si installa un'altra versione di Administration Server e non si desidera reinstallare Network Agent nei dispositivi, poiché ciò potrebbe richiedere molto tempo.

I comandi descritti nelle istruzioni devono essere eseguiti nei dispositivi client con un account con diritti di amministratore.

Per spostare un dispositivo connesso tramite il gateway di connessione in un altro Administration Server:

1. Eseguire l'utilità klmover con `-address <indirizzo server>` per passare al nuovo Administration Server.
2. Eseguire il comando `klnagchk -nagwait -tl 4`.
3. Eseguire i seguenti comandi per impostare un nuovo gateway di connessione:
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_mode -sv false -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"`
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_loc -sv "<nome_o_ip_gateway>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Qui `gateway_ip_or_name` è l'indirizzo del gateway di connessione accessibile da Internet.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` è il numero della porta TCP in ascolto del gateway di connessione.
4. Eseguire il comando `klnagchk -restart -tl 4` per avviare il servizio Network Agent.

Il dispositivo viene spostato nel nuovo Administration Server e connesso tramite il nuovo gateway connesso.

Cluster e array di server

Kaspersky Security Center supporta la tecnologia cluster. Se Network Agent invia ad Administration Server informazioni che confermano che l'applicazione installata in un dispositivo client fa parte di un array di server, il dispositivo client diventa un nodo del cluster. Il cluster verrà aggiunto come un singolo oggetto nella cartella **Dispositivi gestiti** della struttura della console con l'icona dei server ( ).

Un cluster presenta alcune caratteristiche tipiche:

- Un cluster e i relativi nodi fanno sempre parte dello stesso gruppo di amministrazione.
- Se l'amministratore tenta di spostare un nodo del cluster, il nodo viene ripristinato nella posizione originale.
- Se l'amministratore tenta di spostare un cluster in un gruppo differente, tutti i relativi nodi verranno spostati.

Accensione, spegnimento e riavvio dei dispositivi client in remoto

Kaspersky Security Center consente di gestire in remoto i dispositivi client accendendoli, spegnendoli o riavviandoli.

Per gestire in remoto i dispositivi client:

1. Eseguire la connessione all'Administration Server che gestisce i dispositivi.
2. Creare un'attività di gestione dei dispositivi in uno dei seguenti modi:
   - Se è necessario accendere, spegnere o riavviare dispositivi inclusi nel gruppo di amministrazione selezionato, creare un'attività per il gruppo selezionato.
   - Se è necessario accendere, spegnere o riavviare dispositivi inclusi in diversi gruppi di amministrazione o non inclusi in alcun gruppo, creare un'attività per dispositivi specifici.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata. Nella finestra **Selezionare il tipo di attività** della Creazione guidata nuova attività selezionare il nodo **Kaspersky Security Center**, aprire la cartella **Avanzate**, quindi selezionare l'attività **Gestisci dispositivi**.
3. Eseguire l'attività creata.

Al termine dell'attività, il comando (accensione, spegnimento o riavvio) verrà eseguito sui dispositivi selezionati.

Informazioni sull'utilizzo della connessione continua tra un dispositivo gestito e Administration Server

Per impostazione predefinita, Kaspersky Security Center non prevede una connettività continua tra i dispositivi gestiti e l'Administration Server. I Network Agent nei dispositivi gestiti stabiliscono periodicamente connessioni ed eseguono la sincronizzazione con l'Administration Server. L'intervallo tra queste sessioni di sincronizzazione è definito in un criterio di Network Agent ed è di 15 minuti per impostazione predefinita. Se è necessaria una sincronizzazione anticipata (per forzare ad esempio l'applicazione di un criterio), Administration Server invia un pacchetto di rete firmato a Network Agent sulla porta UDP 15000. Administration Server può inviare questo pacchetto su una rete IPv4 o IPv6. Qualora non fosse possibile stabilire una connessione tramite UDP fra Administration Server e un dispositivo gestito, la sincronizzazione verrà eseguita alla successiva connessione di routine tra Network Agent e Administration Server all'interno dell'intervallo di sincronizzazione.

Tuttavia, alcune operazioni non possono essere eseguite senza una connessione anticipata tra Network Agent e Administration Server. Tra queste operazioni sono incluse l'esecuzione e l'arresto di attività locali, la ricezione di statistiche per un'applicazione gestita e la creazione di un tunnel. Per rendere possibili queste operazioni, è necessario abilitare l'opzione **Non eseguire la disconnessione da Administration Server** nel dispositivo gestito.

Informazioni sulla sincronizzazione forzata

Anche se Kaspersky Security Center sincronizza automaticamente lo stato, le impostazioni, le attività e i criteri per i dispositivi gestiti, in alcuni casi l'amministratore ha l'esigenza di sapere esattamente se la sincronizzazione è stata già eseguita per un determinato dispositivo.

Nel menu di scelta rapida dei dispositivi gestiti in Administration Console, la voce di menu **Tutte le attività** contiene il comando **Forza sincronizzazione**. Quando Kaspersky Security Center 15.1 esegue questo comando, Administration Server tenta di connettersi al dispositivo. Se questo tentativo va a buon fine viene eseguita la sincronizzazione forzata. In caso contrario, la sincronizzazione verrà forzata solo dopo la successiva connessione pianificata tra Network Agent e l'Administration Server.

Informazioni sulla pianificazione di connessione

Nella finestra delle proprietà di Network Agent, nella sottosezione **Pianificazione connessione** della sezione **Connettività**, è possibile specificare gli intervalli di tempo durante i quali Network Agent trasmetterà i dati ad Administration Server.

Connetti quando necessario. Se questa opzione è selezionata, la connessione viene stabilita quando Network Agent deve inviare i dati ad Administration Server.

Connetti negli intervalli di tempo specificati. Se questa opzione è selezionata, Network Agent si connette ad Administration Server all'ora specificata. È possibile aggiungere diversi periodi di tempo per la connessione.

Invio di messaggi agli utenti dei dispositivi

Per inviare un messaggio agli utenti dei dispositivi:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Creare un'attività di invio dei messaggi per gli utenti dei dispositivi in uno dei seguenti modi:
   - Se si desidera inviare un messaggio agli utenti di dispositivi che appartengono al gruppo di amministrazione selezionato, creare un'attività per il gruppo selezionato.
   - Se si desidera inviare un messaggio agli utenti dei dispositivi che appartengono ad altri gruppi di amministrazione o che non appartengono ad alcun gruppo, creare un'attività per dispositivi specifici.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Nella finestra Tipo di attività della Creazione guidata nuova attività selezionare il nodo **Kaspersky Security Center Administration Server**, aprire la cartella **Avanzate**, quindi selezionare l'attività **Invia messaggio all'utente**. L'attività Invia messaggio all'utente è disponibile solo per i dispositivi che eseguono Windows. È anche possibile inviare messaggi dal menu di scelta rapida dell'utente nella cartella **Account utente**.
4. Eseguire l'attività creata.

   Al termine dell'attività, il messaggio creato verrà inviato agli utenti dei dispositivi selezionati. L'attività Invia messaggio all'utente è disponibile solo per i dispositivi che eseguono Windows. È anche possibile inviare messaggi dal menu di scelta rapida dell'utente nella cartella **Account utente**.

Gestione di Kaspersky Security for Virtualization

Kaspersky Security Center supporta l'opzione di connessione di macchine virtuali ad Administration Server. Le macchine virtuali sono protette da Kaspersky Security for Virtualization. Per ulteriori dettagli, consultare la documentazione relativa all'applicazione.

Configurazione del passaggio degli stati del dispositivo

È possibile modificare le condizioni per assegnare lo stato *Critico* o *Avviso* a un dispositivo.

Per abilitare la modifica dello stato del dispositivo in Critico:

1. Aprire la finestra delle proprietà in uno dei seguenti modi:
   - Nella cartella **Criteri** nel menu di scelta rapida di un criterio di Administration Server selezionare **Proprietà**.
   - Selezionare **Proprietà** nel menu di scelta rapida di un gruppo di amministrazione.
2. Nella finestra **Proprietà** visualizzata, nel riquadro **Sezioni**, selezionare **Stato dispositivo**.
3. Nel riquadro a destra, nella sezione **Imposta su Critico se è specificato**, selezionare la casella di controllo accanto a una condizione nell'elenco.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio principale.

4. Fare doppio clic sul nome della condizione selezionata, quindi, nella finestra che si apre, impostare il valore richiesto per la condizione.

   Non è possibile impostare valori per le seguenti condizioni: Applicazione di protezione non installata, Applicazioni incompatibili installate, Rilevate vulnerabilità del software, Impostazioni dispositivo mobile non conformi al criterio, Problemi di sicurezza non elaborati rilevati, Stato dispositivo definito dall'applicazione, Il dispositivo è diventato non gestito, Applicazione di protezione non in esecuzione, La licenza è scaduta.

   Per la condizione **È necessario il riavvio**, è possibile specificare i motivi del riavvio. Si consiglia di selezionare le caselle di controllo accanto a tutti i motivi presenti nell'elenco.

5. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Critico*.

Per abilitare la modifica dello stato del dispositivo in Avviso:

1. Aprire la finestra delle proprietà in uno dei seguenti modi:
   - Nella cartella **Criteri** nel menu di scelta rapida del criterio di Administration Server selezionare **Proprietà**.
   - Selezionare **Proprietà** nel menu di scelta rapida del gruppo di amministrazione.
2. Nella finestra **Proprietà** visualizzata, nel riquadro **Sezioni**, selezionare **Stato dispositivo**.
3. Nel riquadro a destra, nella sezione **Imposta su Avviso se è specificato**, selezionare la casella di controllo accanto a una condizione nell'elenco.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio principale.

4. Fare doppio clic sul nome della condizione selezionata, quindi, nella finestra che si apre, impostare il valore richiesto per la condizione.

   Non è possibile impostare valori per le seguenti condizioni: Applicazione di protezione non installata, Applicazioni incompatibili installate, Rilevate vulnerabilità del software, Impostazioni dispositivo mobile non conformi al criterio, Problemi di sicurezza non elaborati rilevati, Stato dispositivo definito dall'applicazione, Il dispositivo è diventato non gestito, Applicazione di protezione non in esecuzione, La licenza è scaduta.

   Per la condizione **È necessario il riavvio**, è possibile specificare i motivi del riavvio. Si consiglia di selezionare le caselle di controllo accanto a tutti i motivi presenti nell'elenco.

5. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Avviso*.

Tagging dei dispositivi e visualizzazione dei tag assegnati

Kaspersky Security Center consente di eseguire il tagging dei dispositivi. Un *tag* è l'ID di un dispositivo che può essere utilizzato per raggruppare, descrivere o cercare i dispositivi. I tag assegnati ai dispositivi possono essere utilizzati per la creazione di selezioni, per il rilevamento dei dispositivi e per la distribuzione dei dispositivi tra i gruppi di amministrazione.

È possibile assegnare tag ai dispositivi in modalità manuale o automatica. Tagging manuale di un dispositivo nelle proprietà del dispositivo: è possibile utilizzare il tagging manuale quando è necessario assegnare un tag a un singolo dispositivo. Il tagging automatico viene eseguito da Administration Server in base alle regole di tagging specificate.

Nelle proprietà di un Administration Server è possibile configurare il tagging automatico per i dispositivi gestiti dall'Administration Server in questione. Ai dispositivi viene assegnato automaticamente un tag quando vengono soddisfatte le regole specificate. A ogni tag corrisponde una regola individuale. Le regole vengono applicate alle proprietà di rete del dispositivo, al sistema operativo, alle applicazioni installate nel dispositivo e ad altre proprietà del dispositivo. È ad esempio possibile impostare una regola che assegnerà il tag *Win* a tutti i dispositivi che eseguono Windows. Sarà quindi possibile utilizzare il tag durante la creazione di una selezione dispositivi. Questo consentirà di ordinare tutti i dispositivi che eseguono Windows e di assegnare loro un'attività.

È inoltre possibile utilizzare i tag come condizioni di attivazione del profilo criterio in un dispositivo gestito per applicare profili criterio specifici solo nei dispositivi con determinati tag. Se ad esempio un dispositivo a cui è stato assegnato il tag *Corriere* viene visualizzato nel gruppo di amministrazione *Utenti* e se è stata abilitata l'attivazione del profilo criterio corrispondente in base al tag *Corriere*, il criterio creato per il gruppo *Utenti* non verrà applicato al dispositivo e verrà invece applicato il profilo criterio. Il profilo criterio consente al dispositivo di avviare alcune applicazioni la cui esecuzione è stata bloccata dal criterio.

È possibile creare diverse regole di tagging. A un singolo dispositivo possono essere assegnati diversi tag se sono state create più regole di tagging e se vengono contemporaneamente soddisfatte le rispettive condizioni di tali regole. È possibile visualizzare l'elenco di tutti i tag assegnati nelle proprietà del dispositivo. Ogni regola di tagging può essere abilitata o disabilitata. Se una regola è abilitata, viene applicata ai dispositivi gestiti da Administration Server. Se attualmente non si utilizza una regola ma questa potrebbe essere necessaria in futuro, non bisogna rimuoverla. Basta deselezionare la casella di controllo **Abilita regola**. In questo caso la regola viene disabilitata e non verrà eseguita finché non viene selezionata nuovamente la casella di controllo **Abilita regola**. Può essere necessario disabilitare una regola senza rimuoverla se si desidera escluderla temporaneamente dall'elenco delle regole di tagging e quindi includerla di nuovo.

Tagging automatico dei dispositivi

È possibile creare e modificare le regole di tagging automatico nella finestra delle proprietà di Administration Server.

Per eseguire il tagging automatico dei dispositivi:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server per cui è necessario specificare le regole di tagging.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server selezionare la sezione **Regole di tagging**.
4. Nella sezione **Regole di tagging** fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Nuova regola**.
5. Nella finestra **Nuova regola** configurare le proprietà generali della regola:

   - Specificare il nome della regola.

     Il nome della regola non può superare i 255 caratteri e non può includere caratteri speciali (ad esempio `"* <>?\:|`).
   - Abilitare o disabilitare la regola utilizzando la casella di controllo **Abilita regola**.

     Per impostazione predefinita, la casella di controllo **Abilita regola** è selezionata.
   - Nel campo **Tag** immettere il nome del tag.

     Il nome del tag non può superare i 255 caratteri e non può includere caratteri speciali (ad esempio `"*<>? \:|`).
6. Nella sezione **Condizioni** fare clic sul pulsante **Aggiungi** per aggiungere una nuova condizione o sul pulsante **Proprietà** per modificare una condizione esistente.

   Verrà visualizzata la finestra Creazione guidata nuova condizione regola di tagging automatico.
7. Nella finestra **Condizione per l'assegnazione dei tag** selezionare le caselle di controllo per le condizioni relative al tagging. È possibile selezionare più condizioni.
8. In base alle condizioni di tagging selezionate, la procedura guidata visualizza le finestre per la configurazione delle condizioni corrispondenti. Configurare l'attivazione della regola in base alle seguenti condizioni:

   - **Utilizzo del dispositivo o associazione a una specifica rete** - Proprietà di rete del dispositivo, ad esempio nome del dispositivo nella rete Windows e inclusione del dispositivo in un dominio o in una subnet IP.

     > Se per il database utilizzato per Kaspersky Security Center sono impostate regole di confronto con distinzione tra maiuscole e minuscole, mantenere le maiuscole e le minuscole quando si specifica un nome DNS del dispositivo. In caso contrario, la regola di tagging automatico non funzionerà.
   - **Utilizzo di Active Directory** - Presenza del dispositivo in un'unità organizzativa di Active Directory e appartenenza del dispositivo a un gruppo di Active Directory.
   - **Applicazioni specifiche** - Presenza di Network Agent nel dispositivo, tipo di sistema operativo, versione e architettura.
   - **Macchine virtuali** - Inclusione del dispositivo in un determinato tipo di macchine virtuali.
   - **Installazione di un'applicazione dal registro applicazioni** - Presenza di applicazioni di vari produttori nel dispositivo.

9. Dopo la configurazione della condizione, immettere un nome, quindi chiudere la procedura guidata.

   Se necessario, è possibile impostare più condizioni per una singola regola. In questo caso, il tag verrà essere assegnato a un dispositivo se soddisfa almeno una condizione. Le condizioni che sono state aggiunte saranno visualizzate nella finestra delle proprietà della regola.

10. Fare clic su **OK** nella finestra **Nuova regola**, quindi fare clic su **OK** nella finestra delle proprietà di Administration Server.

Le regole create vengono applicate ai dispositivi gestiti dall'Administration Server selezionato. Se le impostazioni di un dispositivo soddisfano le condizioni della regola, al dispositivo viene assegnato il tag.

Visualizzazione e configurazione dei tag assegnati a un dispositivo

È possibile visualizzare l'elenco di tutti i tag che sono stati assegnati a un dispositivo, nonché passare alla configurazione delle regole di tagging automatico nella finestra delle proprietà del dispositivo.

Per visualizzare e configurare i tag che sono stati assegnati a un dispositivo:

1. Nella struttura della console aprire la cartella **Dispositivi gestiti**.

2. Nell'area di lavoro della cartella **Dispositivi gestiti** selezionare il dispositivo per cui si desidera visualizzare i tag assegnati.

3. Dal menu di scelta rapida del dispositivo mobile selezionare **Proprietà**.

4. Nella finestra delle proprietà del dispositivo selezionare la sezione **Tag**.

   Verrà visualizzato un elenco dei tag assegnati al dispositivo selezionato, nonché il modo in cui è stato assegnato ciascun tag: manualmente o tramite una regola.

5. Se necessario, eseguire una delle seguenti operazioni:

   - Per passare alla configurazione delle regole di tagging, fare clic sul collegamento **Configura regole di tagging automatico** (solo per Windows).
   - Per rinominare un tag, selezionarne uno e fare clic sul pulsante **Rinomina**.
   - Per rimuovere un tag, selezionarne uno e fare clic sul pulsante **Rimuovi**.
   - Per aggiungere manualmente un tag, immetterne uno nel campo nella parte inferiore della sezione **Tag**, quindi fare clic sul pulsante **Aggiungi**.

6. Fare clic sul pulsante **Applica** se sono state apportate modifiche alla sezione **Tag** per rendere effettive le modifiche.

7. Fare clic su **OK**.

Se è stato rimosso o rinominato un tag nelle proprietà del dispositivo, questa modifica non influirà sulle regole di tagging impostate nelle proprietà di Administration Server. La modifica verrà applicata solo al dispositivo in cui è stata apportata.

Diagnostica remota dei dispositivi client. Utilità di diagnostica remota di Kaspersky Security Center

L'utilità di diagnostica remota di Kaspersky Security Center (di seguito denominata utilità di diagnostica remota) è progettata per l'esecuzione remota delle seguenti operazioni sui dispositivi client:

- Abilitazione e disabilitazione della traccia, modifica del livello di traccia e download del file di traccia.
- Download di informazioni sul sistema e impostazioni dell'applicazione.
- Download dei registri eventi.
- Generazione di un file di dump per un'applicazione.
- Avvio della diagnostica e download dei rapporti.
- Avvio e arresto delle applicazioni.

È possibile utilizzare i registri eventi e i rapporti di diagnostica scaricati da un dispositivo client per eseguire autonomamente la risoluzione dei problemi. Inoltre, uno specialista del Servizio di assistenza tecnica di Kaspersky potrebbe richiedere di scaricare file di traccia, file di dump, registri eventi e rapporti di diagnostica da un dispositivo client per ulteriori analisi da parte di Kaspersky.

L'utilità di diagnostica remota viene installata automaticamente nel dispositivo insieme ad Administration Console.

Connessione dell'utilità di diagnostica remota a un dispositivo client

Per connettere l'utilità di diagnostica remota a un dispositivo client:

1. Selezionare qualsiasi gruppo di amministrazione nella struttura della console.
2. Nella scheda **Dispositivi** dell'area di lavoro selezionare **Strumenti personalizzati** → **Diagnostica remota** nel menu di scelta rapida di qualsiasi dispositivo.

   Verrà aperta la finestra principale dell'utilità di diagnostica remota.
3. Nel primo campo della finestra principale dell'utilità di diagnostica remota specificare gli strumenti da utilizzare per connettersi al dispositivo:
   - **Accedi tramite la rete di Microsoft Windows**.
   - **Accedi tramite Administration Server**.

4. Se si seleziona **Accedi tramite la rete di Microsoft Windows** nel primo campo della finestra principale dell'utilità, eseguire le seguenti azioni:

   - Nel campo **Dispositivo** specificare l'indirizzo del dispositivo a cui è necessario connettersi

     È possibile utilizzare un indirizzo IP, un nome NetBIOS o un nome DNS come indirizzo del dispositivo.

     Il valore predefinito è l'indirizzo del dispositivo dal cui menu di scelta rapida è stata avviata l'utilità.

   - Specificare un account per la connessione al dispositivo:

     - **Esegui la connessione come utente corrente** (opzione selezionata per impostazione predefinita). Connettersi utilizzando l'account utente corrente.

     - **Utilizza nome utente e password specificati per la connessione**. Connettersi utilizzando un account utente fornito. Specificare il **nome utente** e la **password** per l'account desiderato.

   La connessione a un dispositivo è possibile solo tramite l'account dell'amministratore locale del dispositivo.

5. Se si seleziona **Accedi tramite Administration Server** nel primo campo della finestra principale dell'utilità, eseguire le seguenti azioni:

   - Nel campo **Administration Server** specificare l'indirizzo dell'Administration Server da cui si desidera connettersi al dispositivo.

     È possibile utilizzare un indirizzo IP, un nome NetBIOS o un nome DNS come indirizzo del server.

     Il valore predefinito è l'indirizzo dell'Administration Server da cui è stata eseguita l'utilità.

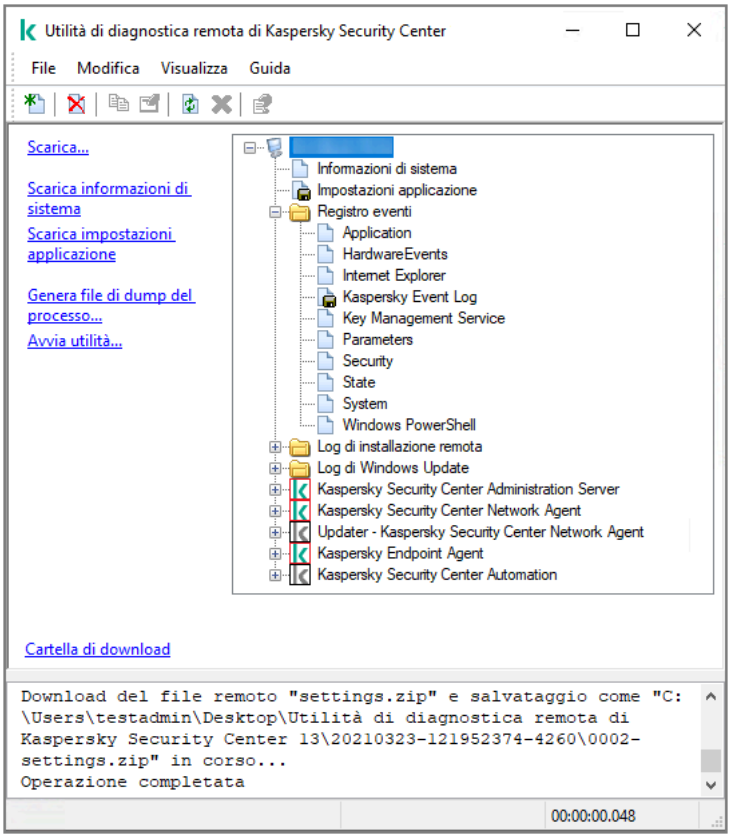
   - Se necessario, selezionare le caselle di controllo **Usa SSL**, **Comprimi traffico** e **Il dispositivo appartiene all'Administration Server secondario**.

     Se la casella di controllo **Il dispositivo appartiene all'Administration Server secondario** è selezionata, è possibile specificare nel campo **Il dispositivo appartiene all'Administration Server secondario** il nome dell'Administration Server secondario che gestisce il dispositivo facendo clic sul pulsante **Sfoglia**.

6. Per connettersi al dispositivo, fare clic sul pulsante **Accedi**.

   È necessario concedere l'autorizzazione utilizzando la verifica in due passaggi se la verifica in due passaggi è abilitata per l'account.

Verrà visualizzata la finestra per la diagnostica remota del dispositivo (vedere la figura seguente). Nella parte sinistra della finestra sono disponibili i collegamenti alle operazioni di diagnostica dei dispositivi. Nella parte destra della finestra è riportata la struttura degli oggetti del dispositivo che l'utilità può utilizzare. Nella parte inferiore della finestra è visualizzato lo stato di avanzamento delle operazioni dell'utilità.



Utilità di diagnostica remota. Finestra di diagnostica remota del dispositivo

L'utilità di diagnostica remota salva i file scaricati dai dispositivi sul desktop del dispositivo da cui è stata avviata.

Generazione di un file di dump per un'applicazione

Un file di dump dell'applicazione consente di visualizzare i parametri dell'applicazione in esecuzione in un dispositivo client in un determinato momento. Questo file contiene anche informazioni sui moduli che sono stati caricati per un'applicazione.

L'ottenimento di dump da dispositivi basati su Linux non è supportato.

Per ottenere i dump tramite la diagnostica remota, viene utilizzata l'utilità kldumper. Questa utilità è progettata per ottenere i dump dei processi delle applicazioni Kaspersky su richiesta degli specialisti dell'Assistenza tecnica. Informazioni dettagliate sui requisiti per l'utilizzo dell'utilità kldumper sono fornite nella Knowledge Base di Kaspersky Security Center.

Per creare un file di dump per un'applicazione:

1. Nell'area di lavoro della cartella **Dispositivi gestiti**, nella scheda **Dispositivi**, aprire il menu di scelta rapida del dispositivo necessario, quindi selezionare **Strumenti personalizzati → Diagnostica remota**.

   Verrà visualizzata la finestra **Utilità di diagnostica remota di Kaspersky Security Center**.

2. Connettere l'utilità di diagnostica remota a un dispositivo client.

   Verrà visualizzata la finestra per la diagnostica remota del dispositivo.

3. Nella parte sinistra della finestra, fare clic sul collegamento **Genera file di dump del processo**

4. Nella finestra **Generazione del file di dump della memoria del processo in corso** visualizzata, specificare il file eseguibile dell'applicazione per la quale si desidera generare un file dump.

5. Fare clic sul pulsante **OK**.

Viene scaricato un archivio con il file di dump per l'applicazione specificata.

Se l'applicazione specificata non è in esecuzione nel dispositivo client, la cartella "result" contenuta nell'archivio scaricato sarà vuota.

Se l'applicazione specificata è in esecuzione, ma il download non riesce con un errore o la cartella "result" contenuta nell'archivio scaricato è vuota, fare riferimento alla Knowledge Base di Kaspersky Security Center.

Abilitazione e disabilitazione della traccia, download del file di traccia

Per abilitare la traccia in un dispositivo remoto:

1. Eseguire l'utilità di diagnostica remota ed eseguire la connessione al dispositivo desiderato.

2. Nella struttura di oggetti del dispositivo selezionare l'applicazione per cui si desidera abilitare la traccia.

   La traccia può essere abilitata e disabilitata per le applicazioni con funzionalità Auto-Difesa solo se il dispositivo è connesso utilizzando gli strumenti di Administration Server.

   Se si desidera abilitare la traccia per Network Agent, è anche possibile eseguire tale operazione durante la creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità. In questo caso, Network Agent scrive le informazioni di traccia anche se l'analisi è disabilitata per Network Agent nell'utilità di diagnostica remota.

3. Per abilitare la traccia:

   a. Nella parte sinistra della finestra dell'utilità di diagnostica remota fare clic su **Abilita traccia**.

   b. Nella finestra **Selezionare il livello di traccia** visualizzata è consigliabile mantenere i valori predefiniti delle impostazioni. Se necessario, uno specialista del Servizio di assistenza tecnica fornirà il supporto richiesto per il processo di configurazione. Sono disponibili le seguenti impostazioni:

   - **Livello di traccia**

     Il livello di traccia definisce la quantità di dettagli contenuti nel file di traccia.

   - **Traccia basata sulla rotazione** (disponibile solo per Kaspersky Endpoint Security)

     L'applicazione sovrascrive le informazioni di tracciamento per evitare un aumento eccessivo delle dimensioni del file di traccia. Specificare il numero massimo di file da utilizzare per archiviare le informazioni di tracciamento e la dimensione massima di ciascun file. Se viene eseguita la scrittura del numero massimo di file di traccia della dimensione massima, il file di traccia meno recente viene eliminato in modo da consentire la creazione di un nuovo file di traccia.

   c. Fare clic su **OK**.

4. Per Kaspersky Endpoint Security, uno specialista del Servizio di assistenza tecnica può richiedere di abilitare il tracciamento Xperf per ottenere informazioni sulle prestazioni del sistema.

   Per abilitare la traccia Xperf:

   a. Nella parte sinistra della finestra dell'utilità di diagnostica remota fare clic su **Abilita traccia Xperf**.

   b. Nella finestra **Selezionare il livello di traccia** visualizzata, a seconda di quanto richiesto dallo specialista del Servizio di assistenza tecnica, selezionare uno dei seguenti livelli di traccia:

   - **Livello superficiale**

     Un file di traccia di questo tipo contiene la quantità minima di informazioni sul sistema.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Livello approfondito**

     Un file di traccia di questo tipo contiene informazioni più dettagliate rispetto ai file di traccia di tipo *Superficiale* e può essere richiesto dagli specialisti del Servizio di assistenza tecnica quando un file di traccia di tipo *Superficiale* non è sufficiente per la valutazione delle prestazioni. Un file di traccia *Approfondito* contiene informazioni tecniche sul sistema, incluse informazioni su hardware, sistema operativo, elenco di processi e applicazioni avviati e arrestati, eventi utilizzati per la valutazione delle prestazioni ed eventi raccolti da Strumento Valutazione sistema Windows.

   c. Selezionare uno dei seguenti tipi di traccia:

   - **Tipologia di base**

Le informazioni di tracciamento vengono ricevute durante l'esecuzione dell'applicazione Kaspersky Endpoint Security.

Per impostazione predefinita, questa opzione è selezionata.

- **Tipologia al riavvio**

  Le informazioni di tracciamento vengono ricevute all'avvio del sistema operativo nel dispositivo gestito. Questo tipo di tracciamento è utile quando il problema che influisce sulle prestazioni del sistema si verifica dopo l'accensione del dispositivo e prima dell'avvio di Kaspersky Endpoint Security.

d. Potrebbe anche essere necessario abilitare l'opzione **Traccia basata sulla rotazione** per impedire un aumento eccessivo delle dimensioni del file di traccia. Specificare quindi la dimensione massima del file di traccia. Quando il file raggiunge la dimensione massima, le informazioni di tracciamento meno recenti vengono sovrascritte da quelle nuove.

e. Fare clic su **OK**.

In alcuni casi, è necessario riavviare un'applicazione di protezione e la relativa attività per abilitare il tracciamento.

L'utilità di diagnostica remota consente di abilitare la traccia per l'applicazione selezionata.

Per scaricare un file di traccia di un'applicazione:

1. Eseguire l'utilità di diagnostica remota e connettersi al dispositivo desiderato, come descritto in "Connessione dell'utilità di diagnostica remota a un dispositivo client".
2. Nel nodo dell'applicazione selezionare il file desiderato nella cartella **File di traccia**.
3. Nella parte sinistra della finestra dell'utilità di diagnostica remota fare clic su **Scarica l'intero file**.

   Per i file di grandi dimensioni possono essere scaricate le parti della traccia più recenti.

   È possibile eliminare il file di traccia selezionato. Il file può essere eliminato dopo avere disabilitato la traccia.

Il file selezionato verrà scaricato nel percorso specificato nella parte inferiore della finestra.

Per disabilitare la traccia in un dispositivo remoto:

1. Eseguire l'utilità di diagnostica remota e connettersi al dispositivo desiderato, come descritto in "Connessione dell'utilità di diagnostica remota a un dispositivo client".
2. Nella struttura di oggetti del dispositivo selezionare l'applicazione per cui si desidera disabilitare la traccia.

   La traccia può essere abilitata e disabilitata per le applicazioni con funzionalità Auto-Difesa solo se il dispositivo è connesso utilizzando gli strumenti di Administration Server.

3. Nella parte sinistra della finestra dell'utilità di diagnostica remota fare clic su **Disabilita traccia**.

L'utilità di diagnostica remota consente di disabilitare la traccia per l'applicazione selezionata.

Download delle impostazioni delle applicazioni

Per scaricare le impostazioni dell'applicazione da un dispositivo remoto:

1. Eseguire l'utilità di diagnostica remota e connettersi al dispositivo desiderato, come descritto in "Connessione dell'utilità di diagnostica remota a un dispositivo client".

2. Nella struttura di oggetti della finestra dell'utilità di diagnostica remota selezionare il nodo superiore con il nome del dispositivo.

3. Nella parte sinistra della finestra dell'utilità di diagnostica remota selezionare l'azione desiderata delle seguenti opzioni:

   - **Scarica informazioni di sistema**

   - **Scarica impostazioni applicazione**

   - **Genera file di dump del processo**

     Nella finestra visualizzata facendo clic sul collegamento specificare il file eseguibile dell'applicazione per cui generare un file dump.

   - **Avvia utilità**

     Nella finestra visualizzata facendo clic sul collegamento specificare il file eseguibile dell'utilità da avviare e le relative impostazioni di esecuzione.

L'utilità selezionata viene scaricata e avviata nel dispositivo.

Download dei registri eventi

Per scaricare un registro eventi da un dispositivo remoto:

1. Eseguire l'utilità di diagnostica remota e connettersi al dispositivo desiderato, come descritto in "Connessione dell'utilità di diagnostica remota a un dispositivo client".

2. Nella cartella **Registri eventi di sistema** della struttura di oggetti del dispositivo selezionare il registro desiderato.

3. Scaricare il registro selezionato facendo clic sul collegamento **Scarica registro eventi <nome registro eventi>** nella parte sinistra della finestra dell'utilità di diagnostica remota.

Il registro eventi selezionato verrà scaricato nel percorso specificato nel riquadro inferiore.

Download di più elementi di informazioni diagnostiche

L'utilità di diagnostica remota di Kaspersky Security Center consente di scaricare più elementi di informazioni diagnostiche, inclusi registri eventi, informazioni sul sistema, file di traccia e file di dump.

Per scaricare le informazioni diagnostiche da un dispositivo remoto:

1. Eseguire l'utilità di diagnostica remota e connettersi al dispositivo desiderato, come descritto in "Connessione dell'utilità di diagnostica remota a un dispositivo client".
2. Nella parte sinistra della finestra dell'utilità di diagnostica remota fare clic su **Scarica**.
3. Selezionare le caselle di controllo accanto agli elementi che si desidera scaricare.
4. Fare clic su **Avvia**.

Ogni elemento selezionato verrà scaricato nel percorso specificato nel riquadro inferiore.

Avvio della diagnostica e download dei risultati

Per avviare la diagnostica per un'applicazione in un dispositivo remoto e scaricarne i risultati:

1. Eseguire l'utilità di diagnostica remota e connettersi al dispositivo desiderato, come descritto in "Connessione dell'utilità di diagnostica remota a un dispositivo client".
2. Nella struttura di oggetti del dispositivo selezionare l'applicazione desiderata.
3. Avviare la diagnostica facendo clic sul collegamento **Esegui diagnostica** nella parte sinistra della finestra dell'utilità di diagnostica remota.

   Verrà visualizzato un rapporto di diagnostica nel nodo dell'applicazione selezionata nella struttura di oggetti.
4. Selezionare il nuovo rapporto di diagnostica generato nella struttura di oggetti, quindi scaricarlo facendo clic sul collegamento **Cartella di download**.

Il rapporto selezionato verrà scaricato nel percorso specificato nel riquadro inferiore.

Avvio, arresto e riavvio delle applicazioni

È possibile avviare, arrestare e riavviare le applicazioni solo se il dispositivo è stato connesso utilizzando gli strumenti di Administration Server.

Per avviare, arrestare o riavviare un'applicazione:

1. Eseguire l'utilità di diagnostica remota e connettersi al dispositivo desiderato, come descritto in "Connessione dell'utilità di diagnostica remota a un dispositivo client".
2. Nella struttura di oggetti del dispositivo selezionare l'applicazione desiderata.
3. Selezionare un'azione nella parte sinistra della finestra dell'utilità di diagnostica remota:
   - **Arresta applicazione**
   - **Riavvia applicazione**
   - **Avvia applicazione**

A seconda dell'azione selezionata, l'applicazione viene avviata, arrestata o riavviata.

Dispositivi di protezione UEFI

Un *dispositivo di protezione UEFI* è un dispositivo con una soluzione Kaspersky per UEFI integrata al livello del BIOS. La protezione integrata garantisce la sicurezza del dispositivo fin dall'avvio del sistema, mentre la protezione nei dispositivi senza software integrato inizia solo dopo l'avvio dell'applicazione di protezione. Kaspersky Security Center supporta la gestione di tali dispositivi.

Per modificare le impostazioni di connessione dei dispositivi di protezione UEFI:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server selezionare **Impostazioni di connessione del server** → **Porte aggiuntive**.
4. Nella sezione **Porte aggiuntive** modificare le impostazioni desiderate:
   - **Porta aperta per i dispositivi di protezione UEFI e i dispositivi KasperskyOS**

     I dispositivi di protezione UEFI possono connettersi all'Administration Server.

   - **Porta per i dispositivi di protezione UEFI e i dispositivi KasperskyOS**

     È possibile modificare il numero di porta se l'opzione **Porta aperta per i dispositivi di protezione UEFI e i dispositivi KasperskyOS** è abilitata. Il numero di porta predefinito è 13294.
5. Fare clic su **OK**.

Impostazioni di un dispositivo gestito

Per visualizzare le impostazioni di un dispositivo gestito:

1. Nella struttura della console selezionare la cartella **Dispositivi gestiti**.
2. Selezionare un dispositivo nell'area di lavoro della cartella.
3. Nel menu di scelta rapida del dispositivo selezionare **Proprietà**.

Viene aperta la finestra delle proprietà del dispositivo selezionato, con la sezione **Generale** selezionata.

Generale

La sezione **Generale** visualizza informazioni generali sul dispositivo client. Le informazioni sono fornite in base ai dati ricevuti durante l'ultima sincronizzazione del dispositivo client con Administration Server:

- **Nome**

  In questo campo è possibile visualizzare e modificare il nome di un dispositivo client nel gruppo di amministrazione.

- **Descrizione**

  In questo campo è possibile immettere un'ulteriore descrizione di un dispositivo client.

- **Dominio Windows**

  Gruppo di lavoro o dominio Windows che contiene il dispositivo.

- **Nome NetBIOS**

  Nome di rete di Windows del dispositivo client.

- **Nome DNS**

  Nome del dominio DNS del dispositivo client.

- **Indirizzo IP**

  Indirizzo IP del dispositivo.

- **Gruppo**

  Gruppo di amministrazione che include il dispositivo client.

- **Ultimo aggiornamento**

  Data dell'ultimo aggiornamento delle applicazioni o dei database anti-virus.

- **Ultima visibilità**

  Data e ora in cui il dispositivo è risultato visibile nella rete per l'ultima volta.

- **Connesso ad Administration Server**

  Data e ora dell'ultima connessione del Network Agent installato nel dispositivo client ad Administration Server.

- **Non eseguire la disconnessione da Administration Server**

  Se questa opzione è abilitata, viene mantenuta una connessione continua tra il dispositivo gestito e Administration Server. È consigliabile utilizzare questa opzione se non si utilizzano server push, che offrono questo tipo di connettività.

  Se questa opzione è disabilitata e i server push non sono in uso, il dispositivo gestito si connette ad Administration Server solo per sincronizzare i dati o trasmettere le informazioni.

  Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

  Questa opzione è disabilitata per impostazione predefinita nei dispositivi gestiti. Questa opzione è abilitata per impostazione predefinita nel dispositivo in cui è installato Administration Server e rimane abilitata anche se si tenta di disabilitarla.

Protezione

Nella sezione **Protezione** vengono visualizzate informazioni sullo stato corrente della protezione anti-virus nel dispositivo client:

- **Stato dispositivo**

  Stato del dispositivo client assegnato in base ai criteri definiti dall'amministratore per lo stato della protezione anti-virus nel dispositivo e l'attività del dispositivo nella rete.

- **Tutti i problemi**

  Questa tabella contiene un elenco completo dei problemi rilevati dalle applicazioni gestite installate nel dispositivo client. Ogni problema è accompagnato da uno stato, che l'applicazione suggerisce di assegnare al dispositivo per il problema.

- **Protezione in tempo reale**

  Questo campo indica lo stato corrente della protezione in tempo reale nel dispositivo client.

  Quando cambia lo stato del dispositivo, il nuovo stato viene visualizzato nella finestra delle proprietà del dispositivo solo dopo la sincronizzazione del dispositivo client con l'Administration Server.

- **Ultima scansione su richiesta**

  Data e ora dell'ultima scansione malware eseguita nel dispositivo client.

- **Numero totale di minacce rilevate**

  Numero totale di minacce rilevate nel dispositivo client dall'installazione dell'applicazione di protezione (prima scansione) o dall'ultimo azzeramento del contatore delle minacce.

- **Minacce attive**

  Numero di file non elaborati nel dispositivo client.

  Questo campo ignora il numero di file non elaborati nei dispositivi mobili.

- **Stato criptaggio disco**

  Stato corrente del criptaggio dei file nelle unità locali del dispositivo. Per una descrizione degli stati consultare la Guida di Kaspersky Endpoint Security for Windows.

Applicazioni

Nella sezione **Applicazioni** sono elencate tutte le applicazioni Kaspersky installate nel dispositivo client. Questa sezione contiene il pulsante di avvio () e il pulsante di arresto () che consentono di avviare e arrestare l'applicazione Kaspersky selezionata (escluso Network Agent). Questi pulsanti sono abilitati se la porta 15000 UDP è disponibile nei dispositivi gestiti per la ricezione delle notifiche push da Administration Server. Se il dispositivo gestito non è disponibile per le notifiche push, ma la modalità di connessione continua ad Administration Server è abilitata (l'opzione **Non eseguire la disconnessione da Administration Server** nella sezione **Generale** è abilitata), anche i pulsanti Avvia e Arresta sono disponibili. La sezione **Applicazioni** contiene anche le seguenti informazioni:

- **Eventi**

  Fare clic sul pulsante per visualizzare l'elenco degli eventi verificatisi nel dispositivo client durante l'esecuzione dell'applicazione e per visualizzare i risultati delle attività per questa applicazione.

- **Statistiche**

  Fare clic su questo pulsante per visualizzare le informazioni statistiche correnti relative all'applicazione.

- **Proprietà**

  Fare clic sul pulsante per ricevere informazioni sull'applicazione e per configurare l'applicazione.

Attività

Nella scheda **Attività**, è possibile gestire le attività dei dispositivi client: visualizzare l'elenco delle attività esistenti, creare nuove attività, rimuovere, avviare e arrestare le attività, modificare le relative impostazioni e visualizzare i risultati dell'esecuzione. L'elenco delle attività è basato sui dati ricevuti durante l'ultima sessione di sincronizzazione del client con Administration Server. Administration Server richiede i dettagli dello stato delle attività al dispositivo client.

I pulsanti Avvia (), Arresta () e Rimuovi () sono abilitati se la porta 15000 UDP è disponibile nei dispositivi gestiti per la ricezione delle notifiche push da Administration Server. Se il dispositivo gestito non è disponibile per le notifiche push, ma la modalità di connessione continua ad Administration Server è abilitata (l'opzione **Non eseguire la disconnessione da Administration Server** nella sezione **Generale** è abilitata), anche i pulsanti Avvia, Arresta e Rimuovi sono disponibili.

Se la connessione non viene stabilita, lo stato dell'attività non viene visualizzato e i pulsanti vengono disabilitati.

Eventi

Nella scheda **Eventi** sono visualizzati gli eventi registrati in Administration Server per il dispositivo client selezionato.

Tag

Nella sezione **Tag** è possibile gestire l'elenco di parole chiave utilizzate per cercare i dispositivi client: visualizzare l'elenco dei tag esistenti, assegnare tag dall'elenco, configurare le regole per il tagging automatico, aggiungere nuovi tag e rinominare tag esistenti, nonché rimuovere tag.

Informazioni di sistema

La sezione **Informazioni generali di sistema** fornisce le informazioni sull'applicazione installata nel dispositivo client.

Registro delle applicazioni

Nella sezione **Registro delle applicazioni** è possibile visualizzare il registro delle applicazioni installate nel dispositivo client e i relativi aggiornamenti, nonché configurare la visualizzazione del registro delle applicazioni.

Le informazioni sulle applicazioni installate vengono fornite se Network Agent installato nel dispositivo client invia le informazioni richieste ad Administration Server. È possibile configurare l'invio di informazioni ad Administration Server nella finestra delle proprietà di Network Agent o del relativo criterio, nella sezione **Archivi**.

- **Visualizza solo applicazioni di protezione incompatibili**

  Se questa opzione è abilitata, l'elenco delle applicazioni contiene solo le applicazioni di protezione incompatibili con le applicazioni Kaspersky.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Mostra aggiornamenti**

  Se questa opzione è abilitata, l'elenco delle applicazioni contiene non solo le applicazioni ma anche i pacchetti di aggiornamento installati.

  Per visualizzare l'elenco degli aggiornamenti sono necessari 100 KB di traffico. Se si chiude l'elenco e lo si riapre, sarà necessario utilizzare altri 100 KB di traffico.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Esporta in un file**

  Fare clic su questo pulsante per esportare l'elenco delle applicazioni installate nel dispositivo in un file CSV o TXT.

- **Cronologia**

  Fare clic su questo pulsante per visualizzare gli eventi che riguardano l'installazione delle applicazioni nel dispositivo. Vengono visualizzate le seguenti informazioni:

  - Data e ora in cui l'applicazione è stata installata nel dispositivo
  - Nome applicazione
  - Versione applicazione

- **Proprietà**

  Fare clic su questo pulsante per visualizzare le proprietà dell'applicazione selezionata nell'elenco delle applicazioni installate nel dispositivo. Vengono visualizzate le seguenti informazioni:

  - Nome applicazione
  - Versione applicazione
  - Fornitore dell'applicazione

File eseguibili

La sezione **File eseguibili** visualizza i file eseguibili rilevati nel dispositivo client.

Registro hardware

Nella sezione **Registro hardware** è possibile visualizzare le informazioni relative all'hardware installato nel dispositivo client. È possibile visualizzare queste informazioni per i dispositivi Windows e i dispositivi Linux.

Assicurarsi che l'utilità lshw sia installata nei dispositivi Linux da cui si desidera recuperare i dettagli dell'hardware. I dettagli dell'hardware recuperati dalle macchine virtuali potrebbero essere incompleti a seconda dell'hypervisor utilizzato.

Se Network Agent è installato in un dispositivo che esegue Windows, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo:

- RAM
- Dispositivi di archiviazione di massa
- Scheda madre
- CPU

- Schede di rete
- Monitor
- Scheda video
- Scheda audio

Se Network Agent è installato in un dispositivo che esegue Linux o macOS, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo, se tali informazioni sono fornite dal sistema operativo:

- Volume totale RAM
- Volume totale dei dispositivi di archiviazione di massa
- Scheda madre
- CPU
- Schede di rete

Sessioni

La sezione **Sessioni** visualizza le informazioni sul proprietario del dispositivo client solo per i dispositivi Windows e contiene le informazioni sugli account degli utenti che hanno utilizzato il dispositivo client selezionato.

Le informazioni sugli utenti del dominio vengono generate sulla base dei dati di Active Directory. I dettagli degli utenti locali sono forniti da Windows Security Account Manager installato nel dispositivo client.

- **Proprietario dispositivo**

  Il campo **Proprietario dispositivo** visualizza il nome dell'utente che l'amministratore può contattare quando si rende necessario eseguire determinate operazioni con il dispositivo client.

  Utilizzare i pulsanti **Assegna** e **Proprietà** per selezionare il proprietario del dispositivo e visualizzare le informazioni sull'utente che è stato designato come proprietario del dispositivo.

  Utilizzare il pulsante con la croce rossa per eliminare il proprietario attuale del dispositivo.

L'elenco visualizza gli account degli utenti che lavorano sul dispositivo client.

- **Nome**

  Nome del dispositivo nella rete Windows.

- **Nome partecipante**

  Nome (di dominio o locale) dell'utente che ha effettuato l'accesso al sistema nel dispositivo.

- **Account**

  Account dell'utente che ha effettuato l'accesso al dispositivo.

- **E-mail**

  Indirizzo e-mail dell'utente.

- **Telefono**

  Numero di telefono dell'utente.

Problemi di sicurezza

Nella scheda **Problemi di sicurezza**, è possibile visualizzare, modificare e creare problemi di sicurezza per il dispositivo client. I problemi di sicurezza possono essere creati automaticamente, tramite le applicazioni gestite Kaspersky installate nel dispositivo client, o manualmente, dall'amministratore. Se ad esempio alcuni utenti trasferiscono regolarmente malware dalle proprie unità rimovibili nei dispositivi, l'amministratore può creare un problema di sicurezza. L'amministratore può fornire una breve descrizione del caso e le azioni consigliate (ad esempio, azioni disciplinari da intraprendere nei confronti di un utente) nel testo del problema di sicurezza e può aggiungere un collegamento per l'utente o gli utenti.

Un problema di sicurezza per cui sono state eseguite tutte le azioni richieste viene definito *elaborato*. La presenza di problemi di sicurezza non elaborati può essere selezionata come condizione per il passaggio dello stato del dispositivo a *Critico* o *Avviso*.

Questa sezione contiene un elenco dei problemi di sicurezza creati per il dispositivo. I problemi di sicurezza sono classificati in base al tipo e al livello di criticità. Il tipo di un problema di sicurezza è definito dall'applicazione Kaspersky che crea il problema di sicurezza. È possibile evidenziare i problemi di sicurezza elaborati nell'elenco selezionando la casella di controllo nella colonna **Trattati**.

Vulnerabilità del software

La sezione **Vulnerabilità del software** fornisce informazioni sulle vulnerabilità delle applicazioni di terze parti installate nei dispositivi client. È possibile utilizzare il campo di ricerca sopra l'elenco per cercare le vulnerabilità in base al nome.

- **Esporta in un file**

  Fare clic sul pulsante **Esporta in un file** per salvare l'elenco delle vulnerabilità nel file. Per impostazione predefinita, l'applicazione esporta l'elenco delle vulnerabilità in un file CSV.

- **Mostra solo le vulnerabilità che possono essere risolte**

  Se questa opzione è abilitata, nella sezione verranno visualizzate le vulnerabilità che è possibile correggere tramite una patch.

  Se questa opzione è disabilitata, nella sezione verranno visualizzate sia le vulnerabilità che è possibile correggere tramite una patch che quelle per cui non è disponibile alcuna patch.

  Per impostazione predefinita, questa opzione è abilitata.

- **Proprietà**

  Selezionare una vulnerabilità del software nell'elenco e fare clic sul pulsante **Proprietà** per visualizzare le proprietà della vulnerabilità del software selezionata in una finestra separata. Nella finestra è possibile eseguire le seguenti operazioni:

  - Ignorare la vulnerabilità del software in questo dispositivo gestito (in Administration Console o in Kaspersky Security Center Web Console).
  - Visualizzare l'elenco delle correzioni consigliate per la vulnerabilità.
  - Specificare manualmente gli aggiornamenti software per correggere la vulnerabilità (in Administration Console o in Kaspersky Security Center Web Console).
  - Visualizzare le istanze della vulnerabilità.
  - Visualizzare l'elenco delle attività esistenti per correggere la vulnerabilità e creare nuove attività per correggere la vulnerabilità.

Aggiornamenti disponibili

Questa sezione visualizza un elenco degli aggiornamenti software rilevati nel dispositivo, ma non ancora installati. Le informazioni sugli aggiornamenti facoltativi di Microsoft Windows non vengono inviate ad Administration Server.

- **Mostra aggiornamenti installati**

  Se questa opzione è abilitata, nell'elenco saranno visualizzati sia gli aggiornamenti non installati che quelli già installati nel dispositivo client.

  Per impostazione predefinita, questa opzione è disabilitata.

Criteri attivi

Questa sezione consente di visualizzare un elenco di criteri delle applicazioni Kaspersky attualmente assegnate a questo dispositivo.

- Esporta in un file

  È possibile fare clic sul pulsante **Esporta in un file** per salvare l'elenco dei criteri attivi in un file. Per impostazione predefinita, l'applicazione esporta l'elenco dei criteri in un file CSV.

Profili criterio attivi

- Profili criterio attivi

  L'elenco consente di visualizzare informazioni sui profili criterio esistenti, che sono attivi nei dispositivi client. È possibile utilizzare la barra di ricerca sopra l'elenco per trovare profili criterio attivi nell'elenco immettendo un nome criterio o il nome di un profilo criterio.

- Esporta in un file

  È possibile fare clic sul pulsante **Esporta in un file** per salvare l'elenco dei profili criterio attivi in un file. Per impostazione predefinita, l'applicazione esporta l'elenco dei profili criterio in un file CSV.

Punti di distribuzione

In questa sezione viene fornito un elenco dei punti di distribuzione con cui interagisce il dispositivo.

- Esporta in un file

  Fare clic sul pulsante **Esporta in un file** per salvare in un file un elenco di punti di distribuzione con cui interagisce il dispositivo. Per impostazione predefinita, l'applicazione esporta l'elenco di dispositivi in un file CSV.

- Proprietà

  Fare clic sul pulsante **Proprietà** per visualizzare e configurare il punto di distribuzione con cui interagisce il dispositivo.

Impostazioni generali dei criteri

Generale

Nella sezione **Generale** è possibile modificare lo stato del criterio e specificare l'ereditarietà delle impostazioni criterio:

- Nella sezione **Stato criterio** è possibile selezionare una modalità criterio:
  - **Criterio attivo**

    Se questa opzione è selezionata, il criterio diventa attivo.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Criterio fuori sede**

    Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.

  - **Criterio inattivo**

    Se questa opzione è selezionata, il criterio diventa inattivo, ma viene comunque salvato nella cartella **Criteri**. Se necessario, il criterio può essere attivato.

- Nel gruppo di impostazioni **Ereditarietà impostazioni** è possibile configurare l'ereditarietà del criterio:
  - **Eredita impostazioni dal criterio padre**

    Se questa opzione è abilitata, i valori delle impostazioni del criterio vengono ereditati dal criterio di gruppo di livello superiore e pertanto vengono bloccati.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Forza ereditarietà impostazioni nei criteri figlio**

    Se questa opzione è abilitata, una volta applicate le modifiche ai criteri, verranno eseguite le seguenti azioni:

    - I valori delle impostazioni dei criteri saranno propagati ai criteri dei sottogruppi di amministrazione, ovvero ai criteri secondari.
    - Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio secondario, l'opzione **Eredita impostazioni dal criterio principale** sarà abilitata automaticamente.

    Se questa opzione è abilitata, le impostazioni dei criteri secondari vengono bloccate.

    Per impostazione predefinita, questa opzione è disabilitata.

Configurazione eventi

La sezione **Configurazione eventi** consente di configurare la registrazione degli eventi e le notifiche degli eventi. Gli eventi vengono distribuiti nelle seguenti schede in base al livello di importanza:

- **Critico**

  La scheda **Critico** non è visualizzata nelle proprietà del criterio di Network Agent.

- **Errore funzionale**
- **Avviso**
- **Informazioni**

In ogni scheda, l'elenco mostra i tipi di eventi e il periodo di archiviazione predefinito per gli eventi in Administration Server (in giorni). Facendo clic sul pulsante **Proprietà** è possibile specificare le impostazioni di registrazione degli eventi e le notifiche sugli eventi selezionati nell'elenco. Per impostazione predefinita, le impostazioni di notifica comuni specificate per l'intero Administration Server vengono utilizzate per tutti i tipi di eventi. Tuttavia, è possibile modificare impostazioni specifiche per i tipi di eventi desiderati.

Ad esempio, nella scheda **Avviso**, è possibile configurare il tipo di evento **Si è verificato un problema di sicurezza**. Tali eventi possono ad esempio verificarsi quando lo spazio libero sul disco di un punto di distribuzione è inferiore a 2 GB (sono necessari almeno 4 GB per installare le applicazioni e scaricare gli aggiornamenti in remoto). Per configurare l'evento **Si è verificato un problema di sicurezza**, selezionarlo e fare clic sul pulsante **Proprietà**. Successivamente è possibile specificare la posizione in cui archiviare gli eventi che si sono verificati e la modalità di notifica.

Se Network Agent ha rilevato un problema di sicurezza, è possibile gestire tale problema utilizzando le impostazioni di un dispositivo gestito.

Per selezionare più tipi di eventi, utilizzare il tasto **MAIUSC** o **CTRL**. Per selezionare tutti i tipi, utilizzare il pulsante **Seleziona tutto**.

Impostazioni del criterio di Network Agent

Per configurare il criterio di Network Agent:

1. Nella struttura della console selezionare la cartella **Criteri**.
2. Nell'area di lavoro della cartella selezionare il criterio di Network Agent.
3. Nel menu di scelta rapida del criterio selezionare **Proprietà**.

Verrà visualizzata la finestra delle proprietà del criterio di Network Agent.

Consultare la tabella di confronto che illustra nel dettaglio come si applicano le impostazioni riportate di seguito, a seconda del tipo di sistema operativo utilizzato.

Generale

Nella sezione **Generale** è possibile modificare lo stato del criterio e specificare l'ereditarietà delle impostazioni criterio:

- Nella sezione **Stato criterio** è possibile selezionare una modalità criterio:
  - **Criterio attivo**

    Se questa opzione è selezionata, il criterio diventa attivo.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Criterio fuori sede**

    Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.

  - **Criterio inattivo**

    Se questa opzione è selezionata, il criterio diventa inattivo, ma viene comunque salvato nella cartella **Criteri**. Se necessario, il criterio può essere attivato.

- Nel gruppo di impostazioni **Ereditarietà impostazioni** è possibile configurare l'ereditarietà del criterio:
  - **Eredita impostazioni dal criterio padre**

    Se questa opzione è abilitata, i valori delle impostazioni del criterio vengono ereditati dal criterio di gruppo di livello superiore e pertanto vengono bloccati.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Forza ereditarietà impostazioni nei criteri figlio**

    Se questa opzione è abilitata, una volta applicate le modifiche ai criteri, verranno eseguite le seguenti azioni:

    - I valori delle impostazioni dei criteri saranno propagati ai criteri dei sottogruppi di amministrazione, ovvero ai criteri secondari.
    - Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio secondario, l'opzione **Eredita impostazioni dal criterio principale** sarà abilitata automaticamente.

    Se questa opzione è abilitata, le impostazioni dei criteri secondari vengono bloccate.

    Per impostazione predefinita, questa opzione è disabilitata.

Configurazione eventi

La sezione **Configurazione eventi** consente di configurare la registrazione degli eventi e le notifiche degli eventi. Gli eventi vengono distribuiti nelle seguenti schede in base al livello di importanza:

- **Critico**

  La scheda **Critico** non è visualizzata nelle proprietà del criterio di Network Agent.

- **Errore funzionale**
- **Avviso**
- **Informazioni**

In ogni scheda, l'elenco mostra i tipi di eventi e il periodo di archiviazione predefinito per gli eventi in Administration Server (in giorni). Facendo clic sul pulsante **Proprietà** è possibile specificare le impostazioni di registrazione degli eventi e le notifiche sugli eventi selezionati nell'elenco. Per impostazione predefinita, le impostazioni di notifica comuni specificate per l'intero Administration Server vengono utilizzate per tutti i tipi di eventi. Tuttavia, è possibile modificare impostazioni specifiche per i tipi di eventi desiderati.

Ad esempio, nella scheda **Avviso**, è possibile configurare il tipo di evento **Si è verificato un problema di sicurezza**. Tali eventi possono ad esempio verificarsi quando lo spazio libero sul disco di un punto di distribuzione è inferiore a 2 GB (sono necessari almeno 4 GB per installare le applicazioni e scaricare gli aggiornamenti in remoto). Per configurare l'evento **Si è verificato un problema di sicurezza**, selezionarlo e fare clic sul pulsante **Proprietà**. Successivamente è possibile specificare la posizione in cui archiviare gli eventi che si sono verificati e la modalità di notifica.

Se Network Agent ha rilevato un problema di sicurezza, è possibile gestire tale problema utilizzando le impostazioni di un dispositivo gestito.

Per selezionare più tipi di eventi, utilizzare il tasto **MAIUSC** o **CTRL**. Per selezionare tutti i tipi, utilizzare il pulsante **Seleziona tutto**.

Impostazioni

Nella sezione **Impostazioni** è possibile configurare il criterio di Network Agent:

- **Distribuisci i file solo tramite punti di distribuzione**

  Se questa opzione è abilitata, i Network Agent nei dispositivi gestiti recuperano gli aggiornamenti solo dai punti di distribuzione.

  Se questa opzione è disabilitata, i Network Agent nei dispositivi gestiti recuperano gli aggiornamenti dai punti di distribuzione o da Administration Server.

  > Le applicazioni di protezione nei dispositivi gestiti recuperano gli aggiornamenti dalla sorgente impostata nell'attività di aggiornamento per ciascuna applicazione di protezione. Se si abilita l'opzione **Distribuisci i file solo tramite punti di distribuzione**, assicurarsi che Kaspersky Security Center sia impostato come sorgente degli aggiornamenti nelle attività di aggiornamento.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima della coda di eventi (MB)**

  In questo campo è possibile specificare la quantità massima di spazio su disco che una coda di eventi può occupare.

  Il valore predefinito è 2 megabyte (MB).

- **L'applicazione può recuperare i dati estesi del criterio nel dispositivo**

  Network Agent installato in un dispositivo gestito trasferisce le informazioni sul criterio dell'applicazione di protezione applicato all'applicazione di protezione (ad esempio Kaspersky Endpoint Security for Windows). È possibile visualizzare le informazioni trasferite nell'interfaccia dell'applicazione di protezione.

  Network Agent trasferisce le seguenti informazioni:

  - Ora della distribuzione del criterio al dispositivo gestito.
  - Nome del criterio attivo al momento della distribuzione del criterio al dispositivo gestito.
  - Nome del criterio fuori sede al momento della distribuzione del criterio al dispositivo gestito (non disponibile per Network Agent for Linux).
  - Nome e percorso completo del gruppo di amministrazione che conteneva il dispositivo gestito al momento della distribuzione del criterio al dispositivo gestito.
  - Elenco dei profili di criteri attivi con i relativi nomi e priorità al momento della distribuzione del criterio al dispositivo gestito.

  È possibile utilizzare le informazioni per assicurarsi che venga applicato il criterio corretto al dispositivo e per la risoluzione dei problemi. Per impostazione predefinita, questa opzione è disabilitata.

- **Proteggi il servizio Network Agent dalle operazioni non autorizzate di rimozione o terminazione e impedisci la modifica delle impostazioni**

  Quando questa opzione è abilitata, dopo l'installazione di Network Agent in un dispositivo gestito, il componente non può essere rimosso o riconfigurato senza i privilegi richiesti. Il servizio Network Agent non può essere arrestato. Questa opzione non ha effetto sui controller di dominio.

  Abilitare questa opzione per proteggere Network Agent sulle workstation gestite con diritti di amministratore locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa password di disinstallazione**

  Se questa opzione è abilitata, facendo clic sul pulsante **Modifica** è possibile specificare la password per l'utilità klmover e la disinstallazione remota di Network Agent.

  Per impostazione predefinita, questa opzione è disabilitata.

Archivi

Nella sezione **Archivi** è possibile selezionare i tipi di oggetti i cui dettagli verranno inviati da Network Agent ad Administration Server:

- **Informazioni dettagliate sugli aggiornamenti Windows Update**

  Se questa opzione è abilitata, le informazioni sugli aggiornamenti di Microsoft Windows Update da installare nei dispositivi client vengono inviate ad Administration Server.

  A volte, anche se l'opzione è disabilitata, gli aggiornamenti vengono visualizzati nelle proprietà del dispositivo, nella sezione **Aggiornamenti disponibili**. Questo potrebbe ad esempio accadere se i dispositivi dell'organizzazione presentassero vulnerabilità correggibili tramite questi aggiornamenti.

  Per impostazione predefinita, questa opzione è abilitata. È disponibile solo per Windows.

  Le informazioni sugli aggiornamenti facoltativi di Microsoft Windows non vengono inviate ad Administration Server.

- **Dettagli sulle vulnerabilità del software e sugli aggiornamenti corrispondenti**

  Se questa opzione è abilitata, le informazioni sulle vulnerabilità del software di terze parti (incluso il software Microsoft) rilevate nei dispositivi gestiti e sugli aggiornamenti software per correggere le vulnerabilità di terze parti (escluso il software Microsoft) vengono inviate ad Administration Server.

  Selezionando questa opzione (**Dettagli sulle vulnerabilità del software e sugli aggiornamenti corrispondenti**) aumentano il carico di rete, il carico sul disco di Administration Server e il consumo di risorse di Network Agent.

  Per impostazione predefinita, questa opzione è abilitata. È disponibile solo per Windows.

  Per gestire gli aggiornamenti software del software Microsoft, utilizzare l'opzione **Informazioni dettagliate sugli aggiornamenti Windows Update.**

- **Dettagli registro hardware**

  Network Agent installato in un dispositivo invia informazioni sull'hardware del dispositivo ad Administration Server. È possibile visualizzare i dettagli hardware nelle proprietà del dispositivo.

  Assicurarsi che l'utilità lshw sia installata nei dispositivi Linux da cui si desidera recuperare i dettagli dell'hardware. I dettagli dell'hardware recuperati dalle macchine virtuali potrebbero essere incompleti a seconda dell'hypervisor utilizzato.

- **Informazioni dettagliate sulle applicazioni installate**

  Se questa opzione è abilitata, le informazioni sulle applicazioni installate nei dispositivi client vengono inviate ad Administration Server.

  Per impostazione predefinita, questa opzione è abilitata.

- **Includi informazioni sulle patch**

  Le informazioni sulle patch delle applicazioni installate nei dispositivi client vengono inviate ad Administration Server. L'abilitazione di questa opzione può aumentare il carico su Administration Server e DBMS, nonché incrementare il volume del database.

  Per impostazione predefinita, questa opzione è abilitata. È disponibile solo per Windows.

Se la modifica di alcune impostazioni in questa sezione non è consentita dal criterio di Network Agent, non è possibile modificare tali impostazioni.

Vulnerabilità e aggiornamenti software

Nella sezione **Vulnerabilità e aggiornamenti software** è possibile configurare la ricerca e la distribuzione degli aggiornamenti di Windows, nonché abilitare la scansione dei file eseguibili per rilevare la presenza di vulnerabilità:

- **Usa Administration Server come server WSUS**

  Se questa opzione è abilitata, gli aggiornamenti di Windows vengono scaricati in Administration Server. Administration Server fornisce gli aggiornamenti scaricati a Windows Update nei dispositivi client in modalità centralizzata tramite Network Agent.

  Se questa opzione è disabilitata, Administration Server non viene utilizzato per scaricare gli aggiornamenti di Windows. In questo caso, i dispositivi client ricevono autonomamente gli aggiornamenti di Windows.

  Per impostazione predefinita, questa opzione è disabilitata.

- In **Consentire agli utenti di gestire l'installazione degli aggiornamenti Windows Update** è possibile limitare gli aggiornamenti di Windows che gli utenti possono installare manualmente nei propri dispositivi tramite Windows Update.

  Nei dispositivi che eseguono Windows 10, se Windows Update ha già rilevato aggiornamenti per il dispositivo, la nuova opzione selezionata in **Consentire agli utenti di gestire l'installazione degli aggiornamenti Windows Update** verrà applicata solo dopo l'installazione degli aggiornamenti rilevati.

  Selezionare un elemento nell'elenco a discesa:

  - **Consentire agli utenti di installare tutti gli aggiornamenti Windows Update applicabili**

    Gli utenti possono installare nei propri dispositivi tutti gli aggiornamenti di Microsoft Windows Update applicabili.

    Selezionare questa opzione se non si desidera interferire nell'installazione degli aggiornamenti.

    Quando l'utente installa manualmente gli aggiornamenti di Microsoft Windows Update, gli aggiornamenti possono essere scaricati dai server Microsoft anziché da Administration Server. Questo è possibile se Administration Server non ha ancora scaricato gli aggiornamenti. Il download degli aggiornamenti dai server Microsoft comporta un traffico aggiuntivo.

  - **Consentire agli utenti di installare solo gli aggiornamenti Windows Update approvati**

    Gli utenti possono installare nei propri dispositivi tutti gli aggiornamenti di Microsoft Windows Update applicabili e approvati dall'amministratore.

    Ad esempio, potrebbe essere utile controllare prima l'installazione degli aggiornamenti in un ambiente di test e verificare che non interferiscano con l'utilizzo dei dispositivi e solo successivamente consentire l'installazione degli aggiornamenti approvati nei dispositivi client.

    Quando l'utente installa manualmente gli aggiornamenti di Microsoft Windows Update, gli aggiornamenti possono essere scaricati dai server Microsoft anziché da Administration Server. Questo è possibile se Administration Server non ha ancora scaricato gli aggiornamenti. Il download degli aggiornamenti dai server Microsoft comporta un traffico aggiuntivo.

- **Non consentire agli utenti di installare gli aggiornamenti Windows Update**

  Gli utenti non possono installare manualmente gli aggiornamenti di Microsoft Windows Update nei propri dispositivi. Tutti gli aggiornamenti applicabili vengono installati in base alla configurazione specificata dall'amministratore.

  Selezionare questa opzione se si desidera gestire l'installazione degli aggiornamenti in modo centralizzato.

  È ad esempio possibile ottimizzare la pianificazione degli aggiornamenti in modo da evitare di sovraccaricare la rete. È possibile pianificare le installazioni degli aggiornamenti in orario non lavorativo, in modo che non interferiscano con la produttività degli utenti.

- Nel gruppo di impostazioni **Modalità di ricerca di Windows Update** è possibile selezionare la modalità di ricerca degli aggiornamenti:

  - **Attiva**

    Se questa opzione è selezionata, Administration Server con il supporto di Network Agent avvia una richiesta da un Windows Update Agent nel dispositivo client alla sorgente degli aggiornamenti: server Windows Update o WSUS. Successivamente, Network Agent trasmette le informazioni ricevute da Windows Update Agent ad Administration Server.

    L'opzione è valida solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** dell'attività *Trova vulnerabilità e aggiornamenti richiesti* è selezionata.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Passiva**

    Se questa opzione è selezionata, Network Agent trasmette periodicamente ad Administration Server le informazioni sugli aggiornamenti recuperati durante l'ultima sincronizzazione di Windows Update Agent con la sorgente degli aggiornamenti. Se non viene eseguita la sincronizzazione di Windows Update Agent con una sorgente degli aggiornamenti, le informazioni sugli aggiornamenti in Administration Server diventano obsolete.

    Selezionare questa opzione se si desidera ottenere gli aggiornamenti dalla cache della memoria della sorgente degli aggiornamenti.

  - **Disabilitata**

    Se questa opzione è selezionata, Administration Server non richiede informazioni sugli aggiornamenti.

    Selezionare questa opzione se, ad esempio, si desidera prima testare gli aggiornamenti nel dispositivo locale.

- **Esegui la scansione dei file eseguibili per rilevarne le vulnerabilità al momento dell'esecuzione**

  Se questa opzione è abilitata, i file eseguibili vengono esaminati alla ricerca di vulnerabilità al momento dell'esecuzione.

  Per impostazione predefinita, questa opzione è abilitata.

Gestione riavvio

Nella sezione **Gestione riavvio** è possibile specificare l'azione che deve essere eseguita se il sistema operativo di un dispositivo gestito deve essere riavviato per utilizzare, installare o disinstallare correttamente un'applicazione:

- **Non riavviare il sistema operativo**

  Il sistema operativo non sarà riavviato.

- **Riavvia automaticamente il sistema operativo se necessario**

  Se necessario, il sistema operativo sarà riavviato automaticamente.

- **Richiedi l'intervento dell'utente**

  All'utente viene chiesto di confermare il riavvio del sistema operativo.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, all'utente verrà richiesto di confermare il riavvio del sistema operativo con la frequenza specificata nel campo accanto alla casella di controllo. La frequenza predefinita per la richiesta di conferma è di 5 minuti.

    Se questa opzione è disabilitata, all'utente non verrà richiesto ripetutamente di confermare il riavvio.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Forza riavvio dopo (min.)**

    Se questa opzione è abilitata, dopo la richiesta di conferma all'utente, verrà forzato il riavvio del sistema operativo alla scadenza dell'intervallo di tempo specificato nel campo accanto alla casella di controllo.

    Se questa opzione è disabilitata, non verrà forzato il riavvio.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Tempo di attesa prima della chiusura forzata delle applicazioni nelle sessioni bloccate (min.)**

    Viene forzata la chiusura delle applicazioni quando il dispositivo dell'utente viene bloccato (automaticamente dopo un intervallo di inattività specificato o manualmente).

    Se questa opzione è abilitata, viene forzata la chiusura delle applicazioni nel dispositivo bloccato alla scadenza dell'intervallo di tempo specificato nel campo di immissione.

    Se questa opzione è disabilitata, le applicazioni nel dispositivo bloccato non vengono chiuse.

    Per impostazione predefinita, questa opzione è disabilitata.

Condivisione desktop Windows

Nella sezione **Condivisione desktop Windows** è possibile abilitare e configurare il controllo delle azioni eseguite dall'amministratore in un dispositivo remoto quando viene condiviso l'accesso al desktop:

- **Abilita controllo**

  Se questa opzione è abilitata, il controllo delle azioni dell'amministratore nel dispositivo remoto è abilitato. I record relativi alle azioni dell'amministratore nel dispositivo remoto vengono registrati:

  - Nel registro eventi del dispositivo remoto
  - In un file con estensione syslog nella cartella di installazione di Network Agent nel dispositivo remoto
  - Nel database degli eventi di Kaspersky Security Center

  Il controllo delle azioni dell'amministratore è disponibile quando sono soddisfatte le seguenti condizioni:

  - È in uso la licenza per Vulnerability e patch management
  - L'amministratore dispone del diritto per l'avvio dell'accesso condiviso al desktop del dispositivo remoto

  Se questa opzione è disabilitata, il controllo delle azioni dell'amministratore nel dispositivo remoto è disabilitato.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Maschere dei file da monitorare durante la lettura**

  L'elenco contiene le maschere dei file. Quando il controllo è abilitato, l'applicazione monitora i file di lettura dell'amministratore corrispondenti alle maschere e salva le informazioni sui file letti. L'elenco è disponibile se la casella di controllo **Abilita controllo** è selezionata. È possibile modificare le maschere dei file e aggiungerne di nuove all'elenco. Ogni nuova maschera di file deve essere specificata nell'elenco su una nuova riga.

  Per impostazione predefinita, sono specificate le seguenti maschere dei file: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Maschere dei file da monitorare durante la modifica**

  L'elenco contiene maschere dei file nel dispositivo remoto. Quando il controllo è abilitato, l'applicazione monitora le modifiche apportate dall'amministratore ai file corrispondenti alle maschere e salva le informazioni su tali modifiche. L'elenco è disponibile se la casella di controllo **Abilita controllo** è selezionata. È possibile modificare le maschere dei file e aggiungerne di nuove all'elenco. Ogni nuova maschera di file deve essere specificata nell'elenco su una nuova riga.

  Per impostazione predefinita, sono specificate le seguenti maschere dei file: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Gestire patch e aggiornamenti

Nella sezione **Gestire patch e aggiornamenti** è possibile configurare il download e la distribuzione degli aggiornamenti, nonché l'installazione delle patch nei dispositivi gestiti:

- **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito**

  Se questa opzione è abilitata, le patch di Kaspersky con lo stato di approvazione *Indefinito* vengono installate automaticamente nei dispositivi gestiti subito dopo il download dai server di aggiornamento.

  Se questa opzione è disabilitata, le patch di Kaspersky che sono state scaricate e contrassegnate con lo stato *Indefinito* saranno installate solo dopo che si modifica il relativo stato in *Approvato*.

  Per impostazione predefinita, questa opzione è abilitata.

- **Scarica aggiornamenti e database anti-virus da Administration Server anticipatamente (scelta consigliata)**

  Se questa opzione è abilitata, viene utilizzato il modello offline di download degli aggiornamenti. Quando Administration Server riceve gli aggiornamenti, segnala a Network Agent (nei dispositivi in cui è installato) gli aggiornamenti che saranno necessari per le applicazioni gestite. Quando Network Agent riceve le informazioni su questi aggiornamenti, scarica anticipatamente i file appropriati da Administration Server. Alla prima connessione con Network Agent, Administration Server avvia un download degli aggiornamenti. Una volta che Network Agent ha scaricato tutti gli aggiornamenti in un dispositivo client, tali aggiornamenti diventano disponibili per le applicazioni nel dispositivo.

  Quando un'applicazione gestita in un dispositivo client tenta di accedere a Network Agent per gli aggiornamenti, questo Network Agent verifica se dispone di tutti gli aggiornamenti richiesti. Se gli aggiornamenti sono stati ricevuti da Administration Server non più di 25 ore prima del momento in cui vengono richiesti dall'applicazione gestita, il Network Agent non si connette ad Administration Server, ma fornisce all'applicazione gestita gli aggiornamenti dalla cache locale. La connessione con Administration Server potrebbe non essere stabilita quando Network Agent fornisce gli aggiornamenti alle applicazioni nei dispositivi client, ma la connessione non è necessaria per l'aggiornamento.

  Se questa opzione è disabilitata, non viene utilizzato il modello offline di download degli aggiornamenti. Gli aggiornamenti vengono distribuiti in base alla pianificazione dell'attività di download degli aggiornamenti.

  Per impostazione predefinita, questa opzione è abilitata.

Connettività

La sezione **Connettività** include tre sottosezioni nidificate:

- **Rete**
- **Profili connessione** (solo per Windows e macOS)
- **Pianificazione connessione**

Nella sottosezione **Rete** è possibile configurare la connessione ad Administration Server, abilitare l'utilizzo di una porta UDP e specificare il relativo numero. Sono disponibili le seguenti opzioni:

- Nel gruppo di impostazioni **Connessione ad Administration Server** è possibile configurare la connessione ad Administration Server e specificare l'intervallo di tempo per la sincronizzazione tra i dispositivi client e Administration Server:

  - Comprimi traffico di rete

    Se questa opzione è abilitata, la velocità di trasferimento dei dati da parte di Network Agent viene aumentata attraverso una riduzione della quantità di informazioni da trasferire e una conseguente riduzione del carico di Administration Server.

    Il carico di lavoro sulla CPU del computer client potrebbe aumentare.

    Per impostazione predefinita, questa casella di controllo è abilitata.

  - Apri porte di Network Agent in Microsoft Windows Firewall

    Se questa opzione è abilitata, le porte, necessarie per l'utilizzo di Network Agent vengono aggiunte all'elenco di esclusioni di Microsoft Windows Firewall.

    Per impostazione predefinita, questa opzione è abilitata.

  - Usa SSL

    Se questa opzione è abilitata, la connessione ad Administration Server viene stabilita attraverso una porta sicura tramite SSL.

    Per impostazione predefinita, questa opzione è abilitata.

  - Usa il gateway di connessione nel punto di distribuzione (se disponibile) con le impostazioni di connessione predefinite

    Se questa opzione è abilitata, viene utilizzato il gateway di connessione nel punto di distribuzione con le impostazioni specificate nelle proprietà del gruppo di amministrazione.

    Per impostazione predefinita, questa opzione è abilitata.

- Usa porta UDP

  Se è necessario che Network Agent si connetta ad Administration server attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in **Porta UDP**. Per impostazione predefinita, questa opzione è abilitata. La porta UDP predefinita per la connessione ad Administration Server è 15000.

- **Numero di porta UDP**

  In questo campo è possibile immettere il numero della porta UDP. Il numero di porta predefinito è 15000.

  Viene utilizzato il sistema decimale per i record.

  Se il dispositivo client esegue Windows XP Service Pack 2, il firewall integrato blocca la porta UDP 15000. Si consiglia di aprire questa porta manualmente.

- **Usa punto di distribuzione per forzare la connessione ad Administration Server**

  Selezionare questa opzione se è stata selezionata l'opzione **Usa questo punto di distribuzione come server push** nella finestra delle impostazioni del punto di distribuzione. In caso contrario, il punto di distribuzione non fungerà da server push.

Nella sottosezione **Profili connessione** è possibile specificare le impostazioni del percorso di rete, configurare i profili di connessione per Administration Server e abilitare la modalità fuori sede quando Administration Server non è disponibile.

- **Impostazioni percorso di rete**

  Le impostazioni del percorso di rete definiscono le caratteristiche della rete alla quale è connesso il dispositivo client e specificano le regole per il passaggio di Network Agent da un profilo di connessione Administration Server all'altro quando tali caratteristiche di rete subiscono variazioni.

- **Profili connessione di Administration Server**

  In questa sezione è possibile visualizzare e aggiungere profili per la connessione di Network Agent ad Administration Server. In questa sezione è inoltre possibile creare regole per il passaggio di Network Agent a diversi Administration Server quando si verificano i seguenti eventi:

  - Quando il dispositivo client si connette a un'altra rete locale
  - Quando il dispositivo perde la connessione con la rete locale dell'organizzazione
  - Quando cambia l'indirizzo del gateway di connessione o l'indirizzo del server DNS viene modificato

  I profili di connessione sono supportati solo per i dispositivi che eseguono Windows e macOS.

- **Abilita la modalità fuori sede quando Administration Server non è disponibile**

  Se questa opzione è abilitata, in caso di utilizzo di questo profilo per la connessione, le applicazioni installate nel dispositivo client utilizzeranno i profili criterio per i dispositivi in modalità fuori sede, nonché i criteri fuori sede. Se non è definito alcun criterio fuori sede per l'applicazione, verrà utilizzato il criterio attivo.

  Se questa opzione è disabilitata, le applicazioni utilizzeranno i criteri attivi.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Pianificazione connessione** è possibile specificare gli intervalli di tempo durante i quali Network Agent invia i dati ad Administration Server:

- Connetti quando necessario

  Se questa opzione è selezionata, la connessione viene stabilita quando Network Agent deve inviare i dati ad Administration Server.

  Per impostazione predefinita, questa opzione è selezionata.

- Connetti negli intervalli di tempo specificati

  Se questa opzione è selezionata, Network Agent si connette ad Administration Server all'ora specificata. È possibile aggiungere diversi periodi di tempo per la connessione.

Punti di distribuzione

La sezione **Punti di distribuzione** include quattro sottosezioni nidificate:

- **Polling della rete**
- **Impostazioni della connessione Internet**
- **Proxy KSN**
- **Aggiornamenti**

Nella sottosezione **Polling della rete** è possibile configurare il polling automatico della rete. È possibile abilitare tre tipi di polling, ovvero il polling della rete, il polling dell'intervallo IP e il polling di Active Directory:

- **Consenti il polling della rete**

  Se l'opzione è abilitata, Administration Server esegue automaticamente il polling della rete in base alla pianificazione configurata facendo clic sui collegamenti **Imposta pianificazione di polling rapido** e **Imposta pianificazione di polling completo**.

  Se questa opzione è disabilitata, Administration Server esegue il polling della rete con l'intervallo specificato nel campo **Frequenza di polling della rete (min.)**.

  L'intervallo di device discovery per le versioni di Network Agent precedenti alla 10.2 può essere configurato nei campi **Frequenza dei polling dai domini Windows (min.)** (per il polling di rete Windows rapido) e **Frequenza di polling della rete (min.)** (per il polling di rete Windows completo).

  Per impostazione predefinita, questa opzione è disabilitata.

- **Abilita polling intervalli IP**

  Se l'opzione è abilitata, il punto di distribuzione esegue automaticamente il polling degli intervalli IP in base alla pianificazione configurata facendo clic sul pulsante **Imposta pianificazione di polling**.

  Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling degli intervalli IP.

  La frequenza di polling dell'intervallo IP per le versioni di Network Agent precedenti alla 10.2 può essere configurata nel campo **Intervallo di polling (min.)**. Il campo è disponibile se l'opzione è abilitata.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa polling Zeroconf (solo nelle piattaforme Linux; gli intervalli IP specificati manualmente verranno ignorati)**

  Se questa opzione è abilitata, il punto di distribuzione esegue automaticamente il polling della rete con i dispositivi IPv6 utilizzando le reti zero-configuration (definite anche *Zeroconf*). In questo caso, il polling dell'intervallo IP abilitati viene ignorato, poiché il punto di distribuzione esegue il polling dell'intera rete.

  Per iniziare a utilizzare Zeroconf è necessario soddisfare le seguenti condizioni:

  - Il punto di distribuzione deve eseguire Linux.
  - È necessario installare l'utilità avahi-browse nel punto di distribuzione.

  Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling delle reti con i dispositivi IPv6.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Abilita polling di Active Directory**

  Se l'opzione è abilitata, il punto di distribuzione esegue automaticamente il polling di Active Directory in base alla pianificazione configurata facendo clic sul collegamento **Imposta pianificazione di polling**.

  Se questa opzione è disabilitata, Administration Server non esegue il polling di Active Directory.

  La frequenza di polling di Active Directory per le versioni di Network Agent precedenti alla 10.2 può essere configurata nel campo **Intervallo di polling (min.)**. Il campo è disponibile se questa opzione è abilitata.

  Per impostazione predefinita, questa opzione è disabilitata.

Se i punti di distribuzione utilizzano un server proxy durante la connessione a Internet, nella sottosezione **Impostazioni connessione Internet** è possibile specificare le seguenti impostazioni:

- **Usa server proxy**

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile configurare la connessione al server proxy.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Indirizzo server proxy**

  Indirizzo del server proxy.

- **Numero di porta**

  Il numero di porta utilizzato per la connessione.

- **Ignora il server proxy per gli indirizzi locali**

  Se questa opzione è abilitata, non viene utilizzato alcun server proxy per la connessione ai dispositivi nella rete locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Autenticazione server proxy**

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Nome utente**

  Account utente con cui viene stabilita la connessione al server proxy.

- **Password**

  Password dell'account con cui verrà eseguita l'attività.

Nella sottosezione **Proxy KSN** è possibile configurare l'applicazione per l'utilizzo del punto di distribuzione per l'inoltro delle richieste KSN dai dispositivi gestiti:

- **Abilita proxy KSN da parte del punto di distribuzione**

  Il servizio proxy KSN viene eseguito nel dispositivo utilizzato come punto di distribuzione. Utilizzare questa funzionalità per ridistribuire e ottimizzare il traffico nella rete.

  Il punto di distribuzione invia le statistiche KSN, elencate nell'informativa di Kaspersky Security Network, a Kaspersky. Per impostazione predefinita, l'informativa KSN è disponibile in %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Per impostazione predefinita, questa opzione è disabilitata. L'attivazione di questa opzione ha effetto solo se le opzioni **Usa Administration Server come server proxy** e **Accetto di utilizzare Kaspersky Security Network** sono abilitate nella finestra delle proprietà di Administration Server.

  È possibile assegnare il nodo di un cluster attivo-passivo a un punto di distribuzione e abilitare il proxy KSN in tale nodo.

- **Inoltra richieste KSN ad Administration Server**

  Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti ad Administration Server.

  Per impostazione predefinita, questa opzione è abilitata.

- **Accedi a KSN Cloud/KPSN direttamente tramite Internet**

  Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti a KSN Cloud o KPSN. Anche le richieste KSN generate nello stesso punto di distribuzione vengono inviate direttamente a KSN Cloud o KPSN.

  I punti di distribuzione in cui è installato Network Agent versione 11 (o precedente) non possono accedere direttamente a KPSN. Se si desidera riconfigurare i punti di distribuzione per inviare richieste KSN a KPSN, abilitare l'opzione **Inoltra richieste KSN ad Administration Server** per ciascun punto di distribuzione.

  I punti di distribuzione in cui è installato Network Agent versione 12 (o successive) possono accedere direttamente a KPSN.

- **Porta TCP**

  Numero della porta TCP utilizzata dai dispositivi gestiti per la connessione al server proxy KSN. Il numero di porta predefinito è 13111.

- **Usa porta UDP**

  Se è necessario che Network Agent si connetta ad Administration server attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in **Porta UDP**. Per impostazione predefinita, questa opzione è abilitata. La porta UDP predefinita per la connessione ad Administration Server è 15000.

Nella sottosezione **Aggiornamenti** è possibile specificare se Network Agent deve scaricare i file diff abilitando o disabilitando l'opzione **Scarica file diff**. Questa opzione è abilitata per impostazione predefinita.

Cronologia revisioni

Nella scheda **Cronologia revisioni** è possibile visualizzare la cronologia delle revisioni dei criteri di Network Agent. È possibile confrontare le revisioni, visualizzare le revisioni ed eseguire operazioni avanzate, ad esempio salvare le revisioni in un file, eseguire il rollback a una revisione e aggiungere e modificare le descrizioni delle revisioni.

Gestione degli account utente

Questa sezione fornisce informazioni sugli account e i ruoli utente supportati dall'applicazione. Vengono inoltre fornite istruzioni per la creazione di account e ruoli per gli utenti di Kaspersky Security Center.

Kaspersky Security Center consente di gestire account utente e gruppi di account. L'applicazione supporta tre tipi di account:

- Account dei dipendenti dell'organizzazione. Administration Server recupera i dati degli account degli utenti di dominio durante il polling del controller del dominio dell'organizzazione.
- Account degli utenti locali. Account locali nei dispositivi gestiti, nonché account locali nel dispositivo in cui è installato Administration Server.
- Account di utenti interni di Kaspersky Security Center. È possibile creare account di utenti interni. Questi account vengono utilizzati solo all'interno di Kaspersky Security Center.

Utilizzo degli account utente

Kaspersky Security Center consente di gestire account utente e gruppi di account. L'applicazione supporta due tipi di account:

- Account dei dipendenti dell'organizzazione. Administration Server recupera i dati degli account degli utenti durante il polling della rete dell'organizzazione.
- Account degli utenti interni. Questi account vengono applicati quando si utilizzano Administration Server virtuali. Gli account degli utenti interni vengono creati e utilizzati solo in Kaspersky Security Center.

È possibile visualizzare l'elenco degli account utente in uno dei seguenti modi:

- Nella struttura della console, passare a **Avanzate** → **Account utente**.
- Nella struttura della console, passare a **Dispositivi gestiti** → scheda **Dispositivi** → collegamento al <nome del dispositivo> → sezione **Sessioni**.

  La sezione **Sessioni** mostra gli account utente con sessioni attive nei dispositivi in cui viene eseguito Windows.

L'elenco degli account utente viene visualizzato correttamente se sono soddisfatti i seguenti requisiti:

- Utilizzare Network Agent con la stessa versione di Administration Server o successiva.
- Il polling di Active Directory è abilitato per visualizzare gli account degli utenti del dominio.
- Nei dispositivi gestiti in cui viene eseguito Windows, il servizio **Server (LanmanServer)** è in esecuzione.

È possibile eseguire le seguenti operazioni con gli account utente e i gruppi di account:

- Configurare i diritti di accesso degli utenti alle funzionalità dell'applicazione tramite i ruoli.
- Inviare messaggi agli utenti tramite e-mail e SMS.
- Visualizzare l'elenco dei dispositivi mobili dell'utente.
- Rilasciare e installare certificati nei dispositivi mobili di un utente.
- Visualizzare l'elenco dei certificati rilasciati all'utente.
- Disabilitare la verifica in due passaggi per un account utente.

Aggiunta di un account di un utente interno

Per aggiungere un nuovo account utente interno di Kaspersky Security Center:

1. Nella struttura della console aprire la cartella **Account utente**.
   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.
2. Nell'area di lavoro fare clic sul pulsante **Aggiungi utente**.

3. Nella finestra **Nuovo utente** visualizzata specificare le impostazioni del nuovo account utente:

- Un nome utente ()

  > Prestare attenzione durante l'immissione del nome utente. Non sarà possibile modificarlo dopo il salvataggio delle modifiche.

- **Descrizione**
- **Nome completo**
- **E-mail principale**
- **Telefono principale**
- **Password** per la connessione dell'utente a Kaspersky Security Center

  La password deve rispettare le seguenti regole:

  - La password deve avere una lunghezza compresa tra 8 e 256 caratteri.
  - La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
    - Lettere maiuscole (A-Z)
    - Lettere minuscole (a-z)
    - Numeri (0-9)
    - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - La password non deve contenere spazi, caratteri Unicode o la combinazione di "." e "@", quando "." si trova prima di "@".

  Per visualizzare la password immessa, tenere premuto il pulsante **Mostra**.

  > Il numero di tentativi per l'immissione della password è limitato. Per impostazione predefinita, il numero massimo di tentativi di immissione della password consentiti è 10. È possibile modificare il numero di tentativi di immissione della password consentiti, come descritto in "Modifica del numero di tentativi di immissione della password consentiti".

  > Se l'utente raggiunge il numero di tentativi specificato per l'immissione della password, il relativo account viene bloccato per un'ora. Nell'elenco degli account utente l'icona dell'utente () di un account bloccato è visualizzata in grigio (non disponibile). È possibile sbloccare l'account utente solo modificando la password.

- Se necessario, selezionare la casella di controllo **Disabilita account** per impedire all'utente di connettersi all'applicazione. È ad esempio possibile disabilitare un account se si desidera crearlo anticipatamente ma attivarlo in un secondo momento.
- Selezionare la casella di controllo **Richiedi la password quando vengono modificate le impostazioni dell'account** se si desidera abilitare un'opzione aggiuntiva per proteggere un account utente dalle modifiche

non autorizzate. Se questa opzione è abilitata, la modifica delle impostazioni dell'account utente richiede l'autorizzazione dell'utente con il diritto Modifica elenchi di controllo degli accessi agli oggetti dell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

4. Fare clic su **OK**.

Il nuovo account utente creato verrà visualizzato nell'area di lavoro della cartella **Account utente**.

Modifica di un account di un utente interno

Per modificare un account di un utente interno in Kaspersky Security Center:

1. Nella struttura della console aprire la cartella **Account utente**.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.

2. Nell'area di lavoro fare doppio clic sull'account dell'utente interno che si desidera modificare.

3. Nella finestra **Proprietà: <nome utente>** visualizzata modificare le impostazioni dell'account utente:

- **Descrizione**
- **Nome completo**
- **E-mail principale**
- **Telefono principale**
- **Password** per la connessione dell'utente a Kaspersky Security Center

  La password deve rispettare le seguenti regole:

  - La password deve avere una lunghezza compresa tra 8 e 256 caratteri.
  - La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
    - Lettere maiuscole (A-Z)
    - Lettere minuscole (a-z)
    - Numeri (0-9)
    - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - La password non deve contenere spazi, caratteri Unicode o la combinazione di "." e "@", quando "." si trova prima di "@".

  Per visualizzare la password immessa, tenere premuto il pulsante **Mostra**.

  Il numero di tentativi per l'immissione della password è limitato. Per impostazione predefinita, il numero massimo di tentativi di immissione della password consentiti è 10. È possibile modificare il numero di tentativi di immissione della password consentiti, come descritto in "Modifica del numero di tentativi di immissione della password consentiti".

  Se l'utente raggiunge il numero di tentativi specificato per l'immissione della password, il relativo account viene bloccato per un'ora. Nell'elenco degli account utente l'icona dell'utente () di un account bloccato è visualizzata in grigio (non disponibile). È possibile sbloccare l'account utente solo modificando la password.

- Se necessario, selezionare la casella di controllo **Disabilita account** per impedire all'utente di connettersi all'applicazione. È ad esempio possibile disabilitare un account dopo che un dipendente lascia l'azienda.
- Selezionare l'opzione **Richiedi la password quando vengono modificate le impostazioni dell'account** se si desidera abilitare un'opzione aggiuntiva per proteggere un account utente dalle modifiche non autorizzate. Se questa opzione è abilitata, la modifica delle impostazioni dell'account utente richiede l'autorizzazione dell'utente con il diritto Modifica elenchi di controllo degli accessi agli oggetti dell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

4. Fare clic su **OK**.

L'account utente modificato verrà visualizzato nell'area di lavoro della cartella **Account utente**.

Modifica del numero di tentativi di immissione della password consentiti

L'utente di Kaspersky Security Center può immettere una password non valida un numero limitato di volte. Una volta raggiunto il limite, l'account utente viene bloccato per un'ora.

Per impostazione predefinita, il numero massimo di tentativi di immissione della password consentiti è 10. È possibile modificare il numero di tentativi di immissione della password consentiti, come descritto in questa sezione.

Per modificare il numero di tentativi di immissione della password consentiti:

1. Aprire il Registro di sistema del dispositivo in cui è installato Administration Server (ad esempio, in locale, utilizzando il comando regedit dal menu **Start** → **Esegui**).
2. Passare alla seguente chiave:
   - Per i sistemi a 32 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - Per i sistemi a 64 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. Se il valore SrvSplPpcLogonAttempts non è presente, crearlo. Il tipo di valore è DWORD.

   Per impostazione predefinita, dopo l'installazione di Kaspersky Security Center questo valore non viene creato.
4. Specificare il numero di tentativi richiesti nel valore SrvSplPpcLogonAttempts.
5. Fare clic su **OK** per salvare le modifiche.
6. Riavviare il servizio Administration Server.

Il numero massimo di tentativi di immissione della password consentiti è stato modificato.

Configurazione del controllo dell'univocità del nome di un utente interno

È possibile configurare il controllo dell'univocità del nome di un utente interno di Kaspersky Security Center quando il nome viene aggiunto all'applicazione. Il controllo dell'univocità del nome di un utente interno può essere eseguito solo in un Administration Server virtuale o nell'Administration Server primario per cui deve essere creato l'account utente oppure in tutti gli Administration Server virtuali e nell'Administration Server primario. Per impostazione predefinita, il controllo dell'univocità del nome di un utente interno viene eseguito in tutti gli Administration Server virtuali e nell'Administration Server primario.

Per abilitare il controllo dell'univocità del nome di un utente interno in un Administration Server virtuale o nell'Administration Server primario:

1. Aprire il Registro di sistema del dispositivo in cui è installato Administration Server (ad esempio, in locale, utilizzando il comando regedit dal menu **Start** → **Esegui**).
2. Passare al seguente hive:
   - Per i sistemi a 32 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Per i sistemi a 64 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Per la chiave LP_InterUserUniqVsScope (DWORD), impostare il valore 00000001.

   Il valore predefinito specificato per questa chiave è 0.
4. Riavviare il servizio Administration Server.

Il controllo dell'univocità del nome verrà eseguito solo nell'Administration Server virtuale in cui è stato creato l'utente interno o nell'Administration Server primario, se l'utente interno è stato creato nell'Administration Server primario.

Per abilitare il controllo dell'univocità del nome di un utente interno in tutti gli Administration Server virtuali e nell'Administration Server primario:

1. Aprire il Registro di sistema del dispositivo in cui è installato Administration Server (ad esempio, in locale, utilizzando il comando regedit dal menu **Start** → **Esegui**).
2. Passare al seguente hive:
   - Per i sistemi a 64 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
   - Per i sistemi a 32 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
3. Per la chiave LP_InterUserUniqVsScope (DWORD), impostare il valore 00000000.

   Il valore predefinito specificato per questa chiave è 0.
4. Riavviare il servizio Administration Server.

Il controllo dell'univocità del nome verrà eseguito in tutti gli Administration Server virtuali e nell'Administration Server primario.

Aggiunta di un gruppo di protezione

È possibile aggiungere gruppi di protezione (gruppi di utenti) e configurare in modo flessibile i gruppi e l'accesso dei gruppi di protezione alle diverse funzionalità dell'applicazione. Ai gruppi di protezione possono essere assegnati nomi corrispondenti ai rispettivi scopi. Ad esempio, il nome può corrispondere alla collocazione degli utenti nell'ufficio o al nome dell'unità organizzativa dell'azienda a cui appartengono gli utenti.

Un utente può appartenere a diversi gruppi di protezione. Un account utente gestito da un Administration Server virtuale può appartenere solo a gruppi di protezione di tale server virtuale e avere diritti di accesso solo all'interno di questo server virtuale.

Per aggiungere un gruppo di protezione:

1. Nella struttura della console selezionare la cartella **Account utente**.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.

2. Fare clic sul pulsante **Aggiungi gruppo di protezione**.

   Verrà visualizzata la finestra **Aggiungi gruppo di protezione**.

3. Nella finestra **Aggiungi gruppo di protezione**, nella sezione **Generale**, specificare il nome del gruppo.

   Il nome del gruppo non può superare i 255 caratteri e contenere simboli speciali come *, <, >, ?, \, :, |. Il nome del gruppo deve essere univoco.

   È possibile immettere la descrizione del gruppo nel campo di immissione **Descrizione**. La compilazione del campo **Descrizione** è facoltativa.

4. Fare clic su **OK**.

Il gruppo di protezione aggiunto viene visualizzato nella cartella **Account utente** nella struttura della console. È possibile aggiungere utenti al nuovo gruppo creato.

Aggiunta di un utente a un gruppo

Per aggiungere un utente a un gruppo:

1. Nella struttura della console selezionare la cartella **Account utente**.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.

2. Nell'elenco degli account utente e dei gruppi selezionare il gruppo a cui si desidera aggiungere l'utente.

3. Nella finestra delle proprietà del gruppo selezionare la sezione **Utenti del gruppo** e fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata una finestra con un elenco di utenti.

4. Nell'elenco selezionare l'utente da includere nel gruppo.

5. Fare clic su **OK**.

L'utente viene aggiunto al gruppo ed è visualizzato nell'elenco degli utenti del gruppo.

Configurazione dei diritti di accesso alle funzionalità dell'applicazione. Controllo dell'accesso basato sui ruoli

Kaspersky Security Center offre l'accesso in base al ruolo alle funzionalità di Kaspersky Security Center e delle applicazioni Kaspersky gestite.

È possibile configurare i diritti di accesso alle funzionalità dell'applicazione per gli utenti di Kaspersky Security Center in uno dei seguenti modi:

- Attraverso la configurazione dei diritti per ciascun utente o gruppo di utenti singolarmente.
- Attraverso la creazione di ruoli utente standard con un set di diritti predefinito e l'assegnazione di tali ruoli agli utenti sulla base dell'ambito delle relative mansioni lavorative.

Il ruolo utente (definito anche ruolo) è un insieme predefinito di diritti di accesso alle funzionalità di Kaspersky Security Center o delle applicazioni Kaspersky gestite. Un ruolo può essere assegnato a un utente o a un gruppo di utenti.

L'applicazione dei ruoli utente ha lo scopo di semplificare e abbreviare le procedure di routine per la configurazione dei diritti di accesso degli utenti alle funzionalità dell'applicazione. I diritti di accesso all'interno di un ruolo vengono configurati in base alle attività standard e all'ambito delle mansioni lavorative degli utenti.

Ai ruoli utente possono essere assegnati nomi corrispondenti ai rispettivi scopi. È possibile creare un numero illimitato di ruoli nell'applicazione.

È possibile utilizzare i ruoli utente predefiniti con un set di diritti già configurato oppure creare nuovi ruoli e configurare autonomamente i diritti richiesti.

Diritti di accesso alle funzionalità dell'applicazione

La tabella seguente mostra le funzionalità di Kaspersky Security Center con i diritti di accesso per gestire le attività, i rapporti e le impostazioni associati e per eseguire le azioni utente associate.

Per eseguire le azioni utente elencate nella tabella, un utente deve disporre del diritto specificato accanto all'azione.

I diritti **Lettura**, **Scrittura** e **Esecuzione** sono applicabili a qualsiasi attività, rapporto o impostazione. Oltre a questi diritti, un utente deve disporre del diritto **Esegui operazioni per le selezioni dispositivi** per gestire attività, rapporti o impostazioni relativi alle selezioni dispositivi.

Tutte le attività, i rapporti, le impostazioni e i pacchetti di installazione mancanti nella tabella appartengono all'area funzionale **Caratteristiche generali: Funzionalità di base**.

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: Gestione dei gruppi di amministrazione	**Scrittura**	• Aggiungere un dispositivo a un gruppo di amministrazione: **Scrittura** • Eliminare un dispositivo da un gruppo di amministrazione: **Scrittura** • Aggiungere un gruppo di amministrazione a un altro gruppo di amministrazione: **Scrittura** • Eliminare un gruppo di amministrazione da un altro gruppo di amministrazione: **Scrittura**	None	None	None
Caratteristiche generali: Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi	**Lettura**	Ottenere l'accesso in Lettura a tutti gli oggetti: **Lettura**	None	None	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: Funzionalità di base	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Regole di spostamento dei dispositivi (creazione, modifica o eliminazione) per il server virtuale: **Scrittura**, **Esegui operazioni per le selezioni dispositivi** • Ottenere un certificato personalizzato per il protocollo Mobile (LWNGT): **Lettura** • Impostare un certificato personalizzato per il protocollo Mobile (LWNGT): **Scrittura** • Ottenere l'elenco di reti definito da NLA: **Lettura** • Aggiungere, modificare o eliminare l'elenco di reti definito da NLA: **Scrittura** • Visualizzare gli elenchi di controllo di accesso dei gruppi: **Lettura** • Visualizzare il registro eventi Kaspersky: **Lettura** • Visualizzare la chiave di ripristino per ripristinare l'accesso a un disco rigido con Crittografia unità BitLocker: **Esecuzione**	• "Scarica aggiornamenti nell'archivio di Administration Server" • "Invia rapporti" • "Distribuisci pacchetto di installazione" • "Installa l'applicazione negli Administration Server secondari in remoto"	• "Rapporto sullo stato della protezione" • "Rapporto sulle minacce" • "Rapporto sui dispositivi più infetti" • "Rapporto sullo stato dei database anti-virus" • "Rapporto sugli errori" • "Rapporto sugli attacchi di rete" • "Rapporto di riepilogo sulle applicazioni di protezione per il sistema di posta installate" • "Rapporto di riepilogo sulle applicazioni di difesa perimetrale installate" • "Rapporto di riepilogo sui tipi di applicazioni installate" • "Rapporto sugli utenti dei dispositivi infetti" • "Rapporto sugli incidenti" • "Rapporto sugli eventi" • "Rapporto sull'attività dei punti di distribuzione" • "Rapporto sugli Administration Server secondari" • "Rapporto sugli eventi di Controllo Dispositivi" • "Rapporto sulle vulnerabilità" • "Rapporto sulle applicazioni proibite" • "Rapporto su Controllo Web" • "Rapporto sullo stato di criptaggio dei dispositivi gestiti" • "Rapporto sullo stato di criptaggio dei dispositivi di	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
				archiviazione di massa" • "Rapporto sugli errori di criptaggio dei file" • "Rapporto sul blocco dell'accesso ai file criptati" • "Rapporto sui diritti di accesso ai dispositivi criptati" • "Rapporto sulle autorizzazioni utente effettive" • "Rapporto sui diritti"	
Caratteristiche generali: Oggetti eliminati	• **Lettura** • **Scrittura**	• Visualizzare gli oggetti eliminati nel Cestino: **Lettura** • Eliminare gli oggetti dal Cestino: **Scrittura**	None	None	None
Caratteristiche generali: Elaborazione degli eventi	• **Elimina eventi** • **Modifica impostazioni di notifica eventi** • **Modifica impostazioni registro eventi** • **Scrittura**	• Modificare le impostazioni di registrazione degli eventi: **Modifica impostazioni registro eventi** • Modificare le impostazioni di notifica degli eventi: **Modifica impostazioni di notifica eventi** • Eliminare gli eventi: **Elimina eventi**	None	None	Impostazioni: • Impostazioni Epidemia di virus: numero di rilevamenti di virus necessari per creare un evento Epidemia di virus • Impostazioni Epidemia di virus: periodo di tempo per la valutazione dei rilevamenti di virus • Numero massimo di eventi archiviati nel database • Periodo di tempo per l'archiviazione degli eventi dai dispositivi eliminati

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: Operazioni in Administration Server	• **Lettura** • **Scrittura** • **Esecuzione** • **Modifica elenchi di controllo degli accessi agli oggetti** • **Esegui operazioni per le selezioni dispositivi**	• Specificare le porte dell'Administration Server per la connessione di Network Agent: **Scrittura** • Specificare le porte del proxy di attivazione avviato sull'Administration Server: **Scrittura** • Specificare le porte del proxy di attivazione per i dispositivi mobili avviato sull'Administration Server: **Scrittura** • Specificare le porte del server Web per la distribuzione di pacchetti indipendenti: **Scrittura** • Specificare le porte del server Web per la distribuzione dei profili MDM: **Scrittura** • Specificare le porte SSL di Administration Server per la connessione tramite Kaspersky Security Center Web Console: **Scrittura** • Specificare le porte dell'Administration Server per la connessione mobile: **Scrittura** • Specificare il numero massimo di eventi archiviati nel database dell'Administration Server: **Scrittura** • Specificare il numero massimo di eventi che possono essere inviati dall'Administration Server: **Scrittura** • Specificare il periodo di tempo durante il quale gli eventi possono essere inviati dall'Administration Server: **Scrittura**	• "Backup dei dati di Administration Server" • "Manutenzione database"	None	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: Distribuzione applicazione Kaspersky	• **Gestisci patch di Kaspersky** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	Accettare o rifiutare l'installazione della patch: **Gestisci patch di Kaspersky**	None	• "Rapporto sull'utilizzo delle chiavi di licenza da parte dell'Administration Server virtuale" • "Rapporto sulle versioni del software Kaspersky" • "Rapporto sulle applicazioni incompatibili" • "Rapporto sulle versioni degli aggiornamenti dei moduli software Kaspersky" • "Rapporto sulla distribuzione della protezione"	Pacchetto di installazione: "Kaspersky"
Caratteristiche generali: Gestione delle chiavi di licenza	• **Esporta file chiave** • **Scrittura**	• Esportare il file chiave: **Esporta file chiave** • Modificare le impostazioni della chiave di licenza di Administration Server: **Scrittura**	None	None	None
Caratteristiche generali: Gestione dei rapporti forzata	• **Lettura** • **Scrittura**	• Creare rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Scrittura** • Eseguire rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Lettura**	None	None	None
Caratteristiche generali: Gerarchia di Administration Server	**Configura gerarchia di Administration Server**	Registrare, aggiornare o eliminare gli Administration Server secondari: **Configura gerarchia di Administration Server**	None	None	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: Autorizzazioni utente	**Modifica elenchi di controllo degli accessi agli oggetti**	• Modificare le proprietà Protezione di qualsiasi oggetto: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire i ruoli utente: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire gli utenti interni: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire i gruppi di protezione: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire gli alias: **Modifica elenchi di controllo degli accessi agli oggetti**	None	None	None
Caratteristiche generali: Administration Server virtuali	• **Gestisci Administration Server virtuali** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Ottenere l'elenco degli Administration Server virtuali: **Lettura** • Ottenere informazioni sull'Administration Server virtuale: **Lettura** • Creare, aggiornare o eliminare un Administration Server virtuale: **Gestisci Administration Server virtuali** • Spostare un Administration Server virtuale in un altro gruppo: **Gestisci Administration Server virtuali** • Impostare le autorizzazioni dei server virtuali: **Gestisci Administration Server virtuali**	None	"Rapporto sui risultati dell'installazione degli aggiornamenti software di terze parti"	None
Caratteristiche generali: Gestione delle chiavi di criptaggio	• **Lettura** • **Scrittura**	• Esportare le chiavi di criptaggio: **Lettura** • Importare le chiavi di criptaggio: **Scrittura**	None	None	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Mobile Device Management: Generale	• **Connetti nuovi dispositivi** • **Invia solo comandi informativi ai dispositivi mobili** • **Invia comandi ai dispositivi mobili** • **Gestisci certificati** • **Lettura** • **Scrittura**	• Ottenere dati di ripristino del servizio di gestione delle chiavi: **Lettura** • Eliminare i certificati utente: **Gestisci certificati** • Ottenere la parte pubblica del certificato utente: **Lettura** • Controllare se l'infrastruttura a chiave pubblica (PKI) è abilitata: **Lettura** • Controllare l'account dell'infrastruttura a chiave pubblica (PKI): **Lettura** • Ottenere i modelli dell'infrastruttura a chiave pubblica (PKI): **Lettura** • Ottenere i modelli dell'infrastruttura a chiave pubblica (PKI) tramite il certificato EKU (Extended Key Usage): **Lettura** • Controllare se il certificato dell'infrastruttura a chiave pubblica (PKI) è stato revocato: **Lettura** • Aggiornare le impostazioni di emissione del certificato utente: **Gestisci certificati** • Ottenere le impostazioni di emissione del certificato utente: **Lettura** • Ottenere i pacchetti per nome applicazione e versione: **Lettura** • Impostare o annullare il certificato utente: **Gestisci certificati** • Rinnovare il certificato utente: **Gestisci certificati** • Impostare il tag del certificato utente: **Gestisci certificati** • Eseguire la generazione del pacchetto di installazione MDM; annullare la generazione del	None	None	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
		pacchetto di installazione MDM: **Connetti nuovi dispositivi**			
Gestione sistema: Connettività	• **Avvia sessioni RDP** • **Connetti a sessioni RDP esistenti** • **Avvia tunneling** • **Salva i file dei dispositivi nella workstation dell'amministratore** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Creare una sessione di condivisione desktop: **Avvia sessioni RDP** • Creare una sessione RDP: **Connetti a sessioni RDP esistenti** • Creare un tunnel: **Avvia tunneling** • Salvare l'elenco della rete di contenuti: **Salva i file dei dispositivi nella workstation dell'amministratore**	None	"Rapporto sugli utenti dei dispositivi"	None
Gestione sistema: Inventario hardware	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Ottenere o esportare un oggetto dell'inventario hardware: **Lettura** • Aggiungere, impostare o eliminare un oggetto dell'inventario hardware: **Scrittura**	None	• "Rapporto sul registro hardware" • "Rapporto sulle modifiche della configurazione" • "Rapporto sull'hardware"	None
Gestione sistema: Controllo accesso alla rete (NAC)	• **Lettura** • **Scrittura**	• Visualizzare le impostazioni CISCO: **Lettura** • Modificare le impostazioni CISCO: **Scrittura**	None	None	None
Gestione sistema: Distribuzione del sistema operativo	• **Distribuisci server PXE** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Distribuire server PXE: **Distribuisci server PXE** • Visualizzare un elenco di server PXE: **Lettura** • Avviare o interrompere il processo di installazione nei client PXE: **Esecuzione** • Gestire i driver per WinPE e le immagini del sistema operativo: **Scrittura**	"Crea pacchetto installazione in base a immagine sistema operativo dispositivo di riferimento"	None	Pacchetto di installazione: "OS Image"

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Gestione sistema: Vulnerability e patch management	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Visualizzare le proprietà delle patch di terzi: **Lettura** • Modificare le proprietà delle patch di terzi: **Scrittura**	• "Esegui sincronizzazione di Windows Update" • "Installa aggiornamenti di Windows Update" • "Correggi vulnerabilità" • "Installa aggiornamenti richiesti e correggi vulnerabilità"	"Rapporto sugli aggiornamenti software"	None
Gestione sistema: Installazione remota	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Visualizzazione delle proprietà del pacchetto di installazione basato su Vulnerability e patch management di terzi: **Lettura** • Modifica delle proprietà del pacchetto di installazione basato su Vulnerability e patch management di terzi: **Scrittura**	None	None	Pacchetti di installazione: • "Applicazione personalizzata" • "Pacchetto VAPM"
Gestione sistema: Inventario software	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	None	None	• "Rapporto sulle applicazioni installate" • "Rapporto sulla cronologia del registro applicazioni" • "Rapporto sullo stato dei gruppi di applicazioni concesse in licenza" • "Rapporto sulle chiavi di licenza del software di terze parti"	None

Ruoli utente predefiniti

I ruoli utente assegnati agli utenti di Kaspersky Security Center forniscono set di diritti di accesso alle funzionalità dell'applicazione.

Agli utenti creati in un server virtuale non può essere assegnato un ruolo in Administration Server.

È possibile utilizzare i ruoli utente predefiniti con un set di diritti già configurato oppure creare nuovi ruoli. Quando si crea un nuovo ruolo, è necessario impostare l'ambito del ruolo e assegnare autonomamente i diritti di accesso alle funzionalità di Kaspersky Security Center. Alcuni dei ruoli utente predefiniti disponibili in Kaspersky Security Center possono essere associati a posizioni lavorative specifiche, ad esempio **Auditor**, **Security Officer** e **Supervisore** (questi ruoli sono presenti in Kaspersky Security Center a partire dalla versione 11). I diritti di accesso di questi ruoli sono preconfigurati in base alle attività standard e all'ambito delle mansioni lavorative delle posizioni associate. La tabella seguente illustra il modo in cui è possibile associare i ruoli a posizioni specifiche.

Esempi di ruoli per posizioni specifiche

Ruolo	Commento
Auditor	Consente tutte le operazioni di visualizzazione e l'esecuzione di qualsiasi attività creata su selezioni di dispositivi connessi all'Administration Server tramite Network Agent con diritti di amministratore locale (radice per Linux). Si consiglia di assegnare questo ruolo a un gruppo con attenzione limitato di utenti che ne hanno bisogno per svolgere le proprie funzioni ufficiali.
Supervisore	Consente tutte le operazioni di visualizzazione; non consente le altre operazioni. È possibile assegnare questo ruolo a un security officer e ad altri manager responsabili della sicurezza IT dell'organizzazione.
Security Officer	Consente tutte le operazioni di visualizzazione e la gestione dei rapporti; concede autorizzazioni limitate per l'area **Gestione sistema**: **Connettività**. È possibile assegnare questo ruolo a un addetto responsabile della sicurezza IT dell'organizzazione.

La tabella seguente illustra i diritti di accesso assegnati a ciascun ruolo utente predefinito.

Diritti di accesso dei ruoli utente predefiniti

Ruolo	Descrizione

Amministratore Administration Server	Consente tutte le operazioni nelle seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Elaborazione degli eventi**
	  • **Gerarchia di Administration Server**
	  • **Administration Server virtuali**
	• **Gestione sistema**:
	  • **Connettività**
	  • **Inventario hardware**
	  • **Inventario software**
	Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.

Operatore Administration Server	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Administration Server virtuali**
	• **Gestione sistema**:
	  • **Connettività**
	  • **Inventario hardware**
	  • **Inventario software**

Ruolo	Descrizione
Auditor	Consente tutte le operazioni nelle aree funzionali, in **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Oggetti eliminati** • **Gestione dei rapporti forzata** È possibile assegnare questo ruolo a una persona che esegue il controllo dell'organizzazione.

Amministratore installazione	Consente tutte le operazioni nelle seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Distribuzione del software Kaspersky**
	  • **Gestione delle chiavi di licenza**
	• **Gestione sistema**:
	  • **Distribuzione del sistema operativo**
	  • **Vulnerability e patch management**
	  • **Installazione remota**
	  • **Inventario software**
	Concede i diritti **Lettura** ed **Esecuzione** nell'area funzionale **Caratteristiche generali: Administration Server virtuali**.

Operatore installazione	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Distribuzione del software Kaspersky** (concede anche il diritto **Gestisci patch di Kaspersky** in quest'area)
	  • **Administration Server virtuali**
	• **Gestione sistema**:
	  • **Distribuzione del sistema operativo**
	  • **Vulnerability e patch management**
	  • **Installazione remota**
	  • **Inventario software**

Amministratore Kaspersky Endpoint Security	Consente tutte le operazioni nelle seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • Area Kaspersky Endpoint Security, incluse tutte le funzionalità Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.
Operatore Kaspersky Endpoint Security	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • Area Kaspersky Endpoint Security, incluse tutte le funzionalità
Amministratore principale	Consente tutte le operazioni nelle aree funzionali, *ad eccezione* delle seguenti aree, **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Gestione dei rapporti forzata** Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.

Ruolo	Descrizione

Operatore principale	Concede i diritti **Lettura** ed **Esecuzione** (ove applicabile) in tutte le seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Oggetti eliminati**
	  • **Operazioni in Administration Server**
	  • **Distribuzione applicazione Kaspersky**
	  • **Administration Server virtuali**
	• **Mobile Device Management: Generale**
	• **Gestione sistema**, incluse tutte le funzionalità
	• Area Kaspersky Endpoint Security, incluse tutte le funzionalità

Amministratore Mobile Device Management	Consente tutte le operazioni nelle seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • **Mobile Device Management: Generale**
Operatore Mobile Device Management	Concede i diritti **Lettura** ed **Esecuzione** nell'area funzionale **Caratteristiche generali**: **Funzionalità di base**. Concede i diritti **Lettura** e **Invia solo comandi informativi ai dispositivi mobili** nell'area funzionale **Mobile Device Management**: **Generale**.
Security Officer	Consente tutte le operazioni nelle seguenti aree funzionali, in **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Gestione dei rapporti forzata** Concede i diritti **Lettura**, **Scrittura**, **Esecuzione**, **Salva i file dei dispositivi nella workstation dell'amministratore** ed **Esegui operazioni per le selezioni di dispositivi** nell'area funzionale **Gestione sistema: Connettività**. È possibile assegnare questo ruolo a un addetto responsabile della sicurezza IT dell'organizzazione.
Utente del Portale Self Service	Consente tutte le operazioni nell'area funzionale **Mobile Device Management: Portale Self Service**. Questa funzionalità non è supportata in Kaspersky Security Center 11 e versioni successive.
Supervisore	Concede il diritto **Lettura** nelle aree funzionali **Caratteristiche generali**: **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** e **Caratteristiche generali**: **Gestione dei rapporti forzata**. È possibile assegnare questo ruolo a un security officer e ad altri manager responsabili della sicurezza IT dell'organizzazione.
Amministratore di Vulnerability e patch management	Consente tutte le operazioni nelle aree funzionali **Caratteristiche generali**: **Funzionalità di base** e **Gestione sistema** (incluse tutte le funzionalità).
Operatore di Vulnerability e patch management	Concede i diritti **Lettura** ed **Esecuzione** (ove applicabile) nelle aree funzionali **Caratteristiche generali**: **Funzionalità di base** e **Gestione sistema** (incluse tutte le funzionalità).

Aggiunta di un ruolo utente

Per aggiungere un ruolo utente:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.

3. Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni**, selezionare **Ruoli utente** e fare clic sul pulsante **Aggiungi**.

   La sezione **Ruoli utente** è disponibile se l'opzione **Visualizza le sezioni delle impostazioni di protezione** è abilitata.

4. Nella finestra delle proprietà **Nuovo ruolo** configurare il ruolo:

   - In **Sezioni** selezionare **Generale** e specificare il nome del ruolo.

     Il nome di un ruolo non può superare i 100 caratteri.

   - Selezionare la sezione **Diritti** e configurare il set di diritti selezionando le caselle di controllo **Consenti** e **Nega** accanto alle funzionalità dell'applicazione.

   Se si utilizza l'Administration Server primario, è possibile abilitare l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari**.

5. Fare clic su **OK**.

Il ruolo viene aggiunto.

I ruoli utente creati per Administration Server vengono visualizzati nella finestra delle proprietà di Administration Server nella sezione **Ruoli utente**. È possibile modificare ed eliminare ruoli utente, nonché assegnare ruoli a gruppi di utenti o utenti selezionati.

Assegnazione di un ruolo a un utente o un gruppo di protezione

Per assegnare un ruolo a un utente o a un gruppo di utenti:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server selezionare la sezione **Protezione**.

   La sezione **Sicurezza** è disponibile se la casella di controllo **Visualizza le sezioni delle impostazioni di protezione** è selezionata nella finestra delle impostazioni dell'interfaccia.

4. Nel campo **Nomi di gruppi o utenti** selezionare un utente o un gruppo di utenti a cui si desidera assegnare un ruolo.

   Se l'utente o il gruppo non è contenuto nel campo, è possibile aggiungerlo facendo clic sul pulsante **Aggiungi**.

   Quando si aggiunge un utente facendo clic sul pulsante **Aggiungi**, è possibile selezionare il tipo di autenticazione utente (Microsoft Windows o Kaspersky Security Center). L'autenticazione Kaspersky Security Center viene utilizzata per selezionare gli account degli utenti interni impiegati per l'utilizzo degli Administration Server virtuali.

5. Selezionare la scheda **Ruoli** e fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Ruoli utente**. In questa finestra sono visualizzati i ruoli utente che sono stati creati.

6. Nella finestra **Ruoli utente** selezionare un ruolo per il gruppo di sicurezza.

7. Fare clic su **OK**.

Il ruolo con un set di diritti per l'utilizzo di Administration Server viene assegnato all'utente o al gruppo di sicurezza. I ruoli assegnati sono visualizzati nella scheda **Ruoli** nella sezione **Protezione** della finestra delle proprietà di Administration Server.

Assegnazione delle autorizzazioni a utenti e gruppi

È possibile concedere a utenti e gruppi autorizzazioni per l'utilizzo delle diverse funzionalità dell'Administration Server e delle applicazioni Kaspersky per cui sono disponibili plug-in di gestione, ad esempio Kaspersky Endpoint Security for Windows.

Per assegnare le autorizzazioni a un utente o un gruppo di utenti:

1. Nella struttura della console eseguire una delle seguenti operazioni:

   - Espandere il nodo **Administration Server**, quindi selezionare la sottocartella con il nome dell'Administration Server desiderato.

   - Selezionare il gruppo di amministrazione.

2. Dal menu di scelta rapida di Administration Server o del gruppo di amministrazione selezionare **Proprietà**.

3. Nella finestra delle proprietà di Administration Server (o nella finestra delle proprietà del gruppo di amministrazione) visualizzata, nel riquadro sinistro **Sezioni**, selezionare **Protezione**.

   La sezione **Sicurezza** è disponibile se la casella di controllo **Visualizza le sezioni delle impostazioni di protezione** è selezionata nella finestra delle impostazioni dell'interfaccia.

4. Nella sezione **Sicurezza**, nell'elenco **Nomi di gruppi o utenti**, selezionare un utente o un gruppo.

5. Nell'elenco delle autorizzazioni nella parte inferiore dell'area di lavoro, nella scheda **Diritti** configurare il set di diritti per l'utente o il gruppo:

   a. Fare clic sul segno più (+) per espandere i nodi nell'elenco e ottenere l'accesso alle autorizzazioni.

   b. Selezionare le caselle di controllo **Consenti** e **Nega** accanto alle autorizzazioni desiderate.

      Esempio 1: espandere il nodo **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** o **Oggetti eliminati**, quindi selezionare **Lettura**.

      Esempio 2: espandere il nodo **Funzionalità di base**, quindi selezionare **Scrittura**.

6. Al termine della configurazione del set di diritti, fare clic su **Applica**.

Verrà configurato il set di diritti per l'utente o il gruppo di utenti.

Le autorizzazioni dell'Administration Server (o del gruppo di amministrazione) sono suddivise nelle seguenti aree:

- Caratteristiche generali:
  - Gestione dei gruppi di amministrazione
  - Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi
  - Funzionalità di base
  - Oggetti eliminati
  - Elaborazione degli eventi
  - Operazioni in Administration Server (solo nella finestra delle proprietà di Administration Server)
  - Distribuisci applicazioni Kaspersky
  - Gestione delle chiavi di licenza
  - Gestione dei rapporti forzata
  - Gerarchia di server
  - Diritti utente
  - Administration Server virtuali
- Mobile Device Management:
  - Generale
- Gestione sistema:
  - Connettività
  - Inventario hardware
  - Controllo accesso alla rete (NAC)
  - Distribuisci sistema operativo
  - Gestisci vulnerabilità e patch
  - Installazione remota
  - Inventario software

Se non si seleziona **Consenti** o **Nega** per un'autorizzazione, l'autorizzazione viene considerata *non definita*: è negata finché non viene negata o consentita in modo esplicito per l'utente.

I diritti di un utente sono la somma di quanto segue:

- I diritti propri dell'utente
- I diritti di tutti i ruoli assegnati all'utente
- I diritti di tutto il gruppo di protezione a cui appartiene l'utente
- I diritti di tutti i ruoli assegnati ai gruppi di protezione a cui appartiene l'utente

Se almeno uno di questi set di diritti ha l'autorizzazione **Nega**, l'autorizzazione viene negata all'utente, anche se altri set la consentono o la lasciano non definita.

Propagazione dei ruoli utente agli Administration Server secondari

Per impostazione predefinita, gli elenchi dei ruoli utente degli Administration Server primari e secondari sono indipendenti. È possibile configurare l'applicazione in modo da propagare automaticamente i ruoli utente creati nell'Administration Server primario a tutti gli Administration Server secondari. I ruoli utente possono inoltre essere propagati da un Administration Server secondario ai relativi Administration Server secondari.

Per propagare i ruoli utente dall'Administration Server primario agli Administration Server secondari:

1. Aprire la finestra principale dell'applicazione.
2. Eseguire una delle seguenti operazioni:
   - Nella struttura della console fare clic con il pulsante destro del mouse sul nome di Administration Server, quindi selezionare **Proprietà**.
   - Se è presente un criterio di Administration Server attivo, nell'area di lavoro della cartella **Criteri** fare clic con il pulsante destro del mouse su questo criterio, quindi selezionare **Proprietà** dal menu di scelta rapida.
3. Nella finestra delle proprietà di Administration Server o nella finestra delle impostazioni del criterio, nel riquadro **Sezioni**, selezionare **Ruoli utente**.

   La sezione **Ruoli utente** è disponibile se l'opzione **Visualizza le sezioni delle impostazioni di protezione** è abilitata.

4. Abilitare l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari**.
5. Fare clic su **OK**.

L'applicazione copierà i ruoli utente dell'Administration Server primario negli Administration Server secondari.

Quando l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari** è abilitata e vengono propagati i ruoli utente, questi non possono essere modificati o eliminati negli Administration Server secondari. Quando si crea un nuovo ruolo o si modifica un ruolo esistente nell'Administration Server primario, le modifiche vengono copiate automaticamente negli Administration Server secondari. Quando si elimina un ruolo utente nell'Administration Server primario, questo ruolo rimane negli Administration Server secondari, ma può essere modificato o eliminato.

I ruoli propagati all'Administration Server secondario dal server primario sono visualizzati con l'icona del lucchetto ( ). Non è possibile modificare tali ruoli nell'Administration Server secondario.

Se si crea un ruolo nell'Administration Server primario ed è presente un ruolo con lo stesso nome nell'Administration Server secondario, il nuovo ruolo viene copiato nell'Administration Server secondario con l'aggiunta di un indice al nome, ad esempio ~~1, ~~2 (l'indice può essere casuale).

Se si disabilita l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari**, tutti i ruoli utente restano negli Administration Server secondari, ma diventano indipendenti da quelli nell'Administration Server primario. Dopo essere diventati indipendenti, i ruoli utente negli Administration Server secondari possono essere modificati o eliminati.

Assegnazione dell'utente come proprietario dispositivo

È possibile assegnare l'utente come proprietario dispositivo per allocare un dispositivo a tale utente. Se è necessario eseguire determinate azioni sul dispositivo (ad esempio eseguire l'upgrade dell'hardware), l'amministratore può inviare una notifica al proprietario del dispositivo per ricevere la relativa autorizzazione.

Per assegnare un utente come proprietario di un dispositivo:

1. Nella struttura della console selezionare la cartella **Dispositivi gestiti**.
2. Nell'area di lavoro della cartella, nella scheda **Dispositivi**, selezionare il dispositivo per cui si desidera assegnare un proprietario.
3. Nel menu di scelta rapida del dispositivo selezionare **Proprietà**.
4. Nella finestra delle proprietà del dispositivo selezionare **Informazioni di sistema** → **Sessioni**.
5. Fare clic sul pulsante **Assegna** accanto al campo **Proprietario dispositivo**.
6. Nella finestra **Selezione utente** selezionare l'utente da assegnare come proprietario dispositivo e fare clic su **OK**.
7. Fare clic su **OK**.

Il proprietario dispositivo viene assegnato. Per impostazione predefinita, il campo **Proprietario dispositivo** è compilato con un valore di Active Directory e viene aggiornato durante ogni polling di Active Directory. È possibile visualizzare l'elenco dei proprietari del dispositivo nel **Rapporto sui proprietari del dispositivo**. È possibile creare un rapporto utilizzando la Creazione guidata nuovo rapporto.

Invio di messaggi agli utenti

Per inviare un messaggio a un utente tramite e-mail:

1. Nella struttura della console, nella cartella **Account utente**, selezionare un utente.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.
2. Nel menu di scelta rapida dell'utente selezionare **Notifica tramite e-mail**.
3. Inserire le informazioni nei campi rilevanti nella finestra **Invia messaggio all'utente** e fare clic sul pulsante **OK**.

Il messaggio verrà inviato all'indirizzo e-mail specificato nelle proprietà dell'utente.

Per inviare un messaggio SMS a un utente:

1. Nella struttura della console, nella cartella **Account utente**, selezionare un utente.
2. Dal menu di scelta rapida dell'utente selezionare **Invia un SMS**.
3. Inserire le informazioni nei campi rilevanti nella finestra **Testo SMS** e fare clic sul pulsante **OK**.

Il messaggio verrà inviato al dispositivo mobile con il numero specificato nelle proprietà dell'utente.

Visualizzazione dell'elenco dei dispositivi mobili dell'utente

Per visualizzare un elenco dei dispositivi mobili di un utente:

1. Nella struttura della console, nella cartella **Account utente**, selezionare un utente.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.
2. Nel menu di scelta rapida dell'account utente selezionare **Proprietà**.
3. Nella finestra delle proprietà dell'account utente selezionare la sezione **Dispositivi mobili**.

Nella sezione **Dispositivi mobili** è possibile visualizzare l'elenco dei dispositivi mobili dell'utente e le informazioni su ciascuno di essi. È possibile fare clic sul pulsante **Esporta in un file** per salvare l'elenco di dispositivi mobili in un file.

Installazione di un certificato per un utente

È possibile installare tre tipi di certificati per un utente:

- Certificato condiviso, richiesto per identificare il dispositivo mobile dell'utente.
- Certificato di posta, richiesto per configurare la posta aziendale nel dispositivo mobile dell'utente.
- Certificato VPN, richiesto per configurare la rete privata virtuale (VPN) nel dispositivo mobile dell'utente.

Per rilasciare un certificato a un utente e installarlo:

1. Nella struttura della console aprire la cartella **Account utente** e selezionare un account utente.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.
2. Nel menu di scelta rapida dell'account utente selezionare **Installa certificato**.

Verrà avviata l'Installazione guidata certificato. Seguire le istruzioni della procedura guidata.

Al termine dell'Installazione guidata certificato, il certificato verrà creato e installato per l'utente. È possibile visualizzare l'elenco dei certificati utente installati ed esportarlo in un file.

Visualizzazione dell'elenco dei certificati rilasciati a un utente

Per visualizzare un elenco di tutti i certificati rilasciati a un utente:

1. Nella struttura della console, nella cartella **Account utente**, selezionare un utente.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.

2. Nel menu di scelta rapida dell'account utente selezionare **Proprietà**.

3. Nella finestra delle proprietà dell'account utente selezionare la sezione **Certificati**.

Nella sezione **Certificati** è possibile visualizzare l'elenco dei certificati dell'utente e le informazioni su ciascuno di essi. È possibile fare clic sul pulsante **Esporta in un file** per salvare l'elenco di certificati in un file.

Informazioni sull'amministratore del Administration Server virtuale

Un amministratore della rete aziendale gestita tramite un Administration Server virtuale avvia Kaspersky Security Center Web Console con l'account utente specificato in questa finestra per visualizzare i dettagli della protezione anti-virus.

Se necessario, è possibile creare diversi account amministratore in un server virtuale.

Agli utenti creati in un server virtuale non può essere assegnato un ruolo in Administration Server.

L'amministratore di un Administration Server virtuale è un utente interno di Kaspersky Security Center. Nessun dato relativo agli utenti interni viene trasferito al sistema operativo. Kaspersky Security Center esegue l'autenticazione degli utenti interni.

Installazione remota di sistemi operativi e applicazioni

Kaspersky Security Center consente di creare immagini dei sistemi operativi e distribuirle nei dispositivi client in rete, nonché di eseguire l'installazione remota delle applicazioni Kaspersky o di altri produttori.

Per creare immagini dei sistemi operativi, installare gli strumenti di distribuzione di Windows ADK e gli strumenti del componente aggiuntivo Windows PE per Windows ADK in Administration Server. È possibile creare un'immagine di qualsiasi versione del sistema operativo Windows che soddisfi i requisiti di Kaspersky Security Center.

Kaspersky Security Center non supporta le versioni a 64 bit di Windows ADK e Windows PE.

Acquisizione di immagini dei sistemi operativi

Kaspersky Security Center consente di acquisire le immagini dei sistemi operativi dai dispositivi e di trasferirle all'Administration Server. Le immagini dei sistemi operativi vengono archiviate in Administration Server in una cartella dedicata. L'immagine del sistema operativo di un dispositivo di riferimento viene acquisita e quindi creata attraverso un'attività di creazione del pacchetto di installazione.

La funzionalità di acquisizione delle immagini dei sistemi operativi presenta le seguenti caratteristiche:

- Non è possibile acquisire un'immagine del sistema operativo in un dispositivo in cui è installato Administration Server.
- Durante l'acquisizione di un'immagine del sistema operativo, l'utilità sysprep.exe reimposta le impostazioni del dispositivo di riferimento. Se si desidera ripristinare le impostazioni del dispositivo di riferimento, selezionare la casella di controllo **Crea copia di backup dello stato del dispositivo** state nella Creazione guidata immagine del sistema operativo.
- Il processo di acquisizione dell'immagine consente di riavviare il dispositivo di riferimento.

Distribuzione delle immagini dei sistemi operativi nei nuovi dispositivi

È possibile utilizzare le immagini ricevute per la distribuzione nei dispositivi della rete in cui non è stato ancora installato alcun sistema operativo. In questo caso, viene utilizzata una tecnologia denominata Preboot eXecution Environment (PXE). Selezionare un dispositivo della rete da utilizzare come server PXE server. Il dispositivo deve soddisfare i seguenti requisiti:

- Network Agent deve essere installato nel dispositivo.
- Nel dispositivo non può essere attivo alcun server DHCP, poiché un server PXE utilizza le stesse porte di un server DHCP.
- Il segmento della rete che comprende il dispositivo non deve contenere altri server PXE.

Devono essere soddisfatte le seguenti condizioni per distribuire un sistema operativo:

- Nel dispositivo deve essere installata una scheda di rete.
- Il dispositivo deve essere connesso alla rete.
- L'opzione per l'avvio dalla rete deve essere selezionata nel BIOS all'avvio del dispositivo.

La distribuzione di un sistema operativo viene eseguita nel modo seguente:

1. Il dispositivo client stabilisce una connessione con il server PXE durante il processo di avvio.
2. Il dispositivo client viene avviato in Ambiente preinstallazione di Windows (WinPE).

   L'aggiunta del dispositivo a WinPE può richiedere la configurazione del set di driver per WinPE.

3. Il dispositivo client viene registrato in Administration Server.

4. L'amministratore assegna al dispositivo client un pacchetto di installazione con un'immagine del sistema operativo.

   L'amministratore può aggiungere i driver richiesti al pacchetto di installazione con l'immagine del sistema operativo. L'amministratore può anche specificare un file di configurazione con le impostazioni del sistema operativo (file di risposta) da applicare durante l'installazione.

5. Il sistema operativo viene distribuito nel dispositivo client.

L'amministratore può specificare manualmente gli indirizzi MAC dei dispositivi client che non sono ancora connessi e assegnare loro il pacchetto di installazione con l'immagine del sistema operativo. Quando i dispositivi client selezionati si connettono al server PXE, il sistema operativo viene automaticamente installato in tali dispositivi.

Distribuzione delle immagini dei sistemi operativi nei dispositivi in cui è già installato un altro sistema operativo

La distribuzione delle immagini dei sistemi operativi nei dispositivi client in cui è già installato un altro sistema operativo viene eseguita tramite l'attività di installazione remota per dispositivi specifici.

Si noti che viene eseguita un'installazione pulita del sistema operativo. Tutti i dati verranno eliminati.

Installazione di applicazioni Kaspersky e di altri produttori

L'amministratore può creare pacchetti di installazione di qualsiasi applicazione, incluse quelle specificate dall'utente, e installare le applicazioni nei dispositivi client tramite l'attività di installazione remota.

Creazione di immagini dei sistemi operativi

Le immagini dei sistemi operativi vengono create tramite l'attività di rimozione dell'immagine del sistema operativo del dispositivo di riferimento.

Per creare l'attività di creazione dell'immagine del sistema operativo:

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Pacchetti di installazione**.
2. Fare clic sul pulsante **Crea pacchetto di installazione** per eseguire la Creazione guidata nuovo pacchetto.
3. Nella finestra **Selezionare il tipo di pacchetto di installazione** della procedura guidata fare clic sul pulsante **Creare un pacchetto di installazione con l'immagine del sistema operativo**.
4. Seguire le istruzioni della procedura guidata.

   Al termine della procedura guidata, viene creata un'attività di Administration Server denominata **Crea pacchetto di installazione in base all'immagine del sistema operativo del dispositivo di riferimento**. È possibile visualizzare l'attività nella cartella **Attività**.

Al termine dell'attività **Crea pacchetto di installazione in base all'immagine del sistema operativo del dispositivo di riferimento**, verrà creato un pacchetto di installazione che è possibile utilizzare per distribuire il sistema operativo nei dispositivi client tramite un server PXE o mediante l'attività di installazione remota. È possibile visualizzare il pacchetto di installazione nella cartella **Pacchetti di installazione**.

Installazione di immagini dei sistemi operativi

Kaspersky Security Center consente di distribuire immagini WIM di sistemi operativi Windows® desktop e server nei dispositivi della rete di un'organizzazione.

È possibile utilizzare i seguenti metodi per recuperare un'immagine di un sistema operativo da distribuire tramite gli strumenti di Kaspersky Security Center:

- Eseguire l'importazione dal file install.wim incluso nel pacchetto di distribuzione di Windows
- Acquisire un'immagine da un dispositivo di riferimento

Sono supportati due scenari per la distribuzione delle immagini dei sistemi operativi:

- Distribuzione in un dispositivo "pulito", ovvero senza alcun sistema operativo installato
- Distribuzione in un dispositivo Windows

Utilizzare Ambiente preinstallazione di Windows (Windows PE) per l'acquisizione e la distribuzione di immagini del sistema operativo. Tutti i driver richiesti per il corretto funzionamento di tutti i dispositivi di destinazione devono essere aggiunti a WinPE. In genere, è necessario aggiungere la scheda di rete e i driver del controller di archiviazione.

Per implementare gli scenari di distribuzione e acquisizione delle immagini, devono essere soddisfatti i seguenti requisiti:

- Windows Automated Installation Kit (WAIK) versione 2.0 o successiva o Windows ADK con il componente aggiuntivo Windows PE per Windows ADK deve essere installato in Administration Server. Se lo scenario consente l'installazione o l'acquisizione di immagini in Windows XP, deve essere installato WAIK.
- Un server DHCP deve essere disponibile nella rete che contiene il dispositivo di destinazione.
- La cartella condivisa dell'Administration Server deve essere accessibile in lettura dalla rete che contiene il dispositivo di destinazione. Se la cartella condivisa si trova in Administration Server, è richiesto l'accesso per l'account KlPxeUser (questo account viene creato automaticamente durante l'esecuzione del programma di installazione di Administration Server). Se la cartella condivisa è all'esterno dell'Administration Server, è necessario concedere l'accesso al gruppo Everyone.

Al momento della selezione dell'immagine del sistema operativo da installare, l'amministratore deve specificare esplicitamente l'architettura della CPU del dispositivo di destinazione: x86 o x86-64.

Configurazione dell'indirizzo del server proxy KSN

Per impostazione predefinita, il nome della connessione o l'indirizzo IP di Administration Server coincide con l'indirizzo del server proxy KSN. Se si modifica il nome della connessione o l'indirizzo IP per Administration Server, è necessario specificare l'indirizzo del server proxy KSN corretto per prevenire la perdita di connessione tra i dispositivi host e KSN.

Per configurare l'indirizzo del server proxy KSN:

1. Nella struttura della console accedere a **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.
2. Nel menu di scelta rapida **Pacchetti di installazione** selezionare **Proprietà**.
3. Nella finestra visualizzata specificare il nuovo indirizzo del server proxy KSN nella scheda **Generale**.
4. Fare clic sul pulsante **Applica**.

D'ora in poi l'indirizzo specificato verrà utilizzato come indirizzo del server proxy KSN. È consigliabile abilitare l'opzione **Usa proxy KSN** per ottimizzare il traffico nella rete.

Aggiunta di driver per Ambiente preinstallazione di Windows (WinPE)

Per aggiungere driver per Ambiente preinstallazione di Windows (WinPE)

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Distribuisci immagini dei dispositivi**.
2. Nell'area di lavoro della cartella **Distribuisci immagini dei dispositivi** fare clic sul pulsante **Azioni aggiuntive** e selezionare **Configura set di driver per Ambiente preinstallazione di Windows (WinPE)** nell'elenco a discesa.

   Verrà visualizzata la finestra **Driver Ambiente preinstallazione di Windows**.
3. Nella finestra **Driver Ambiente preinstallazione di Windows** fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Selezionare un driver**.
4. Nella finestra **Selezionare un driver** selezionare un driver dall'elenco.

   Se il driver necessario manca nell'elenco, fare clic sul pulsante **Aggiungi** e specificare il nome del driver e la cartella del pacchetto di distribuzione del driver nella finestra **Aggiungere un driver** visualizzata.

   È possibile selezionare una cartella facendo clic sul pulsante **Sfoglia**.

   Nella finestra **Aggiungere un driver** fare clic su **OK**.
5. Nella finestra **Selezionare un driver** fare clic su **OK**.

   Il driver verrà aggiunto all'archivio di Administration Server. Dopo essere stato aggiunto all'archivio, il driver viene visualizzato nella finestra **Selezionare un driver**.
6. Nella finestra **Driver Ambiente preinstallazione di Windows** fare clic su **OK**.

Il driver verrà aggiunto ad Ambiente preinstallazione di Windows (WinPE).

Aggiunta di driver a un pacchetto di installazione con un'immagine del sistema operativo

Per aggiungere driver a un pacchetto di installazione con un'immagine del sistema operativo:

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Pacchetti di installazione**.
2. Nel menu di scelta rapida di un pacchetto di installazione con un'immagine del sistema operativo selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del pacchetto di installazione.
3. Nella finestra delle proprietà del pacchetto di installazione selezionare la sezione **Driver aggiuntivi**.
4. Fare clic sul pulsante **Aggiungi** nella sezione **Driver aggiuntivi**.

   Verrà visualizzata la finestra **Selezionare un driver**.
5. Nella finestra **Selezionare un driver** selezionare i driver che si desidera aggiungere al pacchetto di installazione con l'immagine del sistema operativo.

   È possibile aggiungere nuovi driver all'archivio dell'Administration Server facendo clic sul pulsante **Aggiungi** nella finestra **Selezionare un driver**.
6. Fare clic su **OK**.

I driver aggiunti sono visualizzati nella sezione **Driver aggiuntivi** della finestra delle proprietà del pacchetto di installazione con l'immagine del sistema operativo.

Configurazione dell'utilità sysprep.exe

L'utilità sysprep.exe consente di preparare il dispositivo per la creazione di un'immagine del sistema operativo.

Per configurare l'utilità sysprep.exe:

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Pacchetti di installazione**.
2. Nel menu di scelta rapida di un pacchetto di installazione con un'immagine del sistema operativo selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del pacchetto di installazione.
3. Nella finestra delle proprietà del pacchetto di installazione selezionare la sezione **Impostazioni di sysprep.exe**.

4. Nella sezione **Impostazioni di sysprep.exe** specificare un file di configurazione da utilizzare durante la distribuzione del sistema operativo nel dispositivo client:

   - **Usa file di configurazione predefinito**. Selezionare questa opzione per utilizzare il file di risposte generato per impostazione predefinita durante l'acquisizione dell'immagine del sistema operativo.
   - **Specifica valori personalizzati delle impostazioni principali**. Selezionare questa opzione per specificare i valori per le impostazioni tramite l'interfaccia utente.
   - **Specifica file di configurazione**. Selezionare questa opzione per utilizzare un file di risposte personalizzato.

5. Per applicare le modifiche apportate, fare clic sul pulsante **Applica**.

Distribuzione di sistemi operativi nei nuovi dispositivi della rete

Per distribuire un sistema operativo nei nuovi dispositivi in cui non è ancora installato alcun sistema operativo:

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Distribuisci immagini dei dispositivi**.

   Verificare che l'opzione **Visualizza Vulnerability e patch management** sia abilitata nella finestra **Configura interfaccia**. In caso contrario, la cartella di **Installazione remota** non viene visualizzata.

2. Fare clic sul pulsante **Azioni aggiuntive** e selezionare **Gestisci l'elenco dei server PXE nella rete** nell'elenco a discesa.

   Verrà aperta la finestra **Proprietà: Distribuisci immagini dei dispositivi** nella sezione **Server PXE**.

3. Nella sezione **Server PXE** fare clic sul pulsante **Aggiungi** e, nella finestra **Server PXE** visualizzata, selezionare il dispositivo da utilizzare come server PXE.

   Il dispositivo aggiunto verrà visualizzato nella sezione dei server PXE. I file WinPE creati vengono trasferiti nel dispositivo da Administration Server. Il processo di trasferimento dei file richiede in genere 10 minuti. Una volta completato il trasferimento, il valore visualizzato **Stato** viene modificato da **Operazioni preliminari** a **Pronto**.

4. Nella sezione **Server PXE** selezionare un server PXE, quindi fare clic sul pulsante **Proprietà**.

5. Nella finestra delle proprietà del server PXE selezionato, nella scheda **Impostazioni di connessione del server PXE**, configurare la connessione tra Administration Server e il server PXE.

6. Avviare il dispositivo client in cui si desidera distribuire il sistema operativo.

7. Nel BIOS del dispositivo client selezionare l'opzione per l'avvio dalla rete.

   Il dispositivo client si connette al server PXE e quindi viene visualizzato nell'area di lavoro della cartella **Distribuisci immagini dei dispositivi**.

8. Nella sezione **Azioni** fare clic sul collegamento **Assegna pacchetto di installazione** per selezionare il pacchetto di installazione da utilizzare per l'installazione del sistema operativo nel dispositivo selezionato.

   Utilizzare lo strumento DiskPart nel dispositivo selezionato per verificare i dischi disponibili. Al prompt dei comandi di Windows PE, digitare `diskpart` per aprire lo strumento DiskPart. Digitare `list disk` per elencare i dischi.

   Dopo avere aggiunto il dispositivo e avergli assegnato un pacchetto di installazione, verrà avviata automaticamente la distribuzione del sistema operativo nel dispositivo.

9. Per annullare la distribuzione del sistema operativo nel dispositivo client, fare clic sul collegamento **Annulla l'installazione dell'immagine del sistema operativo** nella sezione **Azioni**.

Per aggiungere i dispositivi tramite l'indirizzo MAC:

- Nella cartella **Distribuisci immagini dei dispositivi** fare clic su **Aggiungi l'indirizzo MAC del dispositivo** per aprire la finestra **Nuovo dispositivo** e specificare l'indirizzo MAC del dispositivo che si desidera aggiungere.
- Nella cartella **Distribuisci immagini dei dispositivi** fare clic su **Importa gli indirizzi MAC dei dispositivi da un file** per selezionare il file che contiene un elenco di indirizzi MAC di tutti i dispositivi in cui si desidera distribuire un sistema operativo.

Distribuzione di sistemi operativi nei dispositivi client

Per distribuire un sistema operativo nei dispositivi client in cui è già installato un altro sistema operativo:

1. Nella struttura della console aprire la cartella **Installazione remota** e fare clic sul collegamento **Distribuisci il pacchetto di installazione nei dispositivi gestiti (workstation)** per eseguire la Distribuzione guidata della protezione.
2. Nella finestra **Selezionare il pacchetto di installazione** della procedura guidata specificare un pacchetto di installazione con un'immagine del sistema operativo.
3. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, verrà creata un'attività di installazione remota per l'installazione del sistema operativo nei dispositivi client. È possibile avviare o arrestare l'attività nella cartella **Attività**.

Creazione di pacchetti di installazione delle applicazioni

Per creare un pacchetto di installazione dell'applicazione:

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Pacchetti di installazione**.
2. Fare clic sul pulsante **Crea pacchetto di installazione** per eseguire la Creazione guidata nuovo pacchetto.

3. Nella finestra **Selezionare il tipo di pacchetto di installazione** della procedura guidata fare clic su uno dei seguenti pulsanti:

- **Creare un pacchetto di installazione per un'applicazione Kaspersky**. Selezionare questa opzione se si desidera creare un pacchetto di installazione per un'applicazione Kaspersky.

- **Creare un pacchetto di installazione per il file eseguibile specificato**. Selezionare questa opzione se si desidera creare un pacchetto di installazione per un'applicazione di terze parti utilizzando un file eseguibile. In genere il file eseguibile è un file di configurazione dell'applicazione.

  - Copia intera cartella nel pacchetto di installazione

    Selezionare questa opzione se il file eseguibile è corredato da file aggiuntivi richiesti per l'installazione dell'applicazione. Prima di abilitare questa opzione, assicurarsi che tutti i file richiesti siano archiviati nella stessa cartella. Se questa opzione è abilitata, l'applicazione aggiunge tutti i contenuti nella cartella, incluso il file eseguibile specificato, nel pacchetto di installazione.

  - Specificare i parametri di installazione

    Affinché l'installazione remota vada a buon fine, per la maggior parte delle applicazioni l'installazione deve essere eseguita in modalità automatica. In questo caso, è necessario specificare il parametro per l'installazione automatica.

    Configurare le impostazioni di installazione:

    - **Riga di comando file eseguibile**

      Se l'applicazione richiede parametri aggiuntivi per l'installazione automatica, specificarli in questo campo. Fare riferimento alla documentazione del fornitore per ulteriori dettagli.

      È possibile immettere anche altri parametri.

    - **Convertire le impostazioni nei valori consigliati per le applicazioni riconosciute da Kaspersky Security Center**

      L'applicazione verrà installata con le impostazioni consigliate se le informazioni sull'applicazione specificata sono contenute nel database Kaspersky.

      Se nel campo **Riga di comando file eseguibile** sono stati immessi parametri, questi vengono riscritti con le impostazioni consigliate.

      Per impostazione predefinita, questa opzione è abilitata.

      Il database Kaspersky viene creato e gestito dagli analisti di Kaspersky. Per ogni applicazione aggiunta al database, gli analisti Kaspersky definiscono le impostazioni di installazione ottimali. Le impostazioni vengono definite in modo da garantire la corretta installazione remota di un'applicazione in un dispositivo client. Il database viene automaticamente aggiornato in Administration Server quando viene eseguita l'attività Scarica aggiornamenti nell'archivio dell'Administration Server.

- **Selezionare un'applicazione dal database di Kaspersky per creare un pacchetto di installazione**. Selezionare questa opzione se si desidera selezionare l'applicazione di terze parti richiesta dal database Kaspersky per creare un pacchetto di installazione. Il database viene creato automaticamente quando si esegue l'attività Scarica aggiornamenti nell'archivio di Administration Server; le applicazioni vengono visualizzate nell'elenco.

- **Creare un pacchetto di installazione con l'immagine del sistema operativo**. Selezionare questa opzione se è necessario creare un pacchetto di installazione del sistema operativo di un dispositivo di riferimento.

Al termine della procedura guidata, viene creata un'attività di Administration Server denominata **Crea pacchetto di installazione in base all'immagine del sistema operativo del dispositivo di riferimento**. Al termine di questa attività, verrà creato un pacchetto di installazione che è possibile utilizzare per distribuire l'immagine del sistema operativo tramite un server PXE o mediante l'attività di installazione remota.

4. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, verrà creato un pacchetto di installazione che è possibile utilizzare per installare l'applicazione nei dispositivi client. È possibile visualizzare il pacchetto di installazione selezionando **Pacchetti di installazione** nella struttura della console.

Emissione di un certificato per i pacchetti di installazione delle applicazioni

Per emettere un certificato per il pacchetto di installazione di un'applicazione:

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Pacchetti di installazione**.

   La cartella **Installazione remota** è una sottocartella della cartella **Avanzate** per impostazione predefinita.

2. Dal menu di scelta rapida della cartella **Pacchetti di installazione** selezionare **Avanzate**.

   Verrà visualizzata la finestra delle proprietà della cartella **Pacchetti di installazione**.

3. Nella finestra delle proprietà della cartella **Pacchetti di installazione** selezionare la sezione **Firma dei pacchetti indipendenti**.

4. Nella sezione **Firma dei pacchetti indipendenti** fare clic sul pulsante **Specifica**.

   Finestra **Certificato**.

5. Nel campo **Tipo di certificato** specificare il tipo di certificato, pubblico o privato:

   - Se è selezionato il valore **Contenitore PKCS #12**, specificare il file di certificato e la password.
   - Se è selezionato il valore **Certificato X.509**:

     a. Specificare il file della chiave privata (con l'estensione *.prk o *.pem).

     b. Specificare la password della chiave privata.

     c. Specificare il file della chiave pubblica (con l'estensione * cer).

6. Fare clic su **OK**.

Verrà emesso un certificato per il pacchetto di installazione dell'applicazione.

Installazione delle applicazioni nei dispositivi client

Per installare un'applicazione nei dispositivi client:

1. Nella struttura della console aprire la cartella **Installazione remota** e fare clic su **Distribuisci il pacchetto di installazione nei dispositivi gestiti (workstation)** per eseguire la Distribuzione guidata della protezione.
2. Nella finestra **Selezionare il pacchetto di installazione** della procedura guidata specificare il pacchetto di installazione di un'applicazione da installare.
3. Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, verrà creata un'attività di installazione remota per installare l'applicazione nei dispositivi client. È possibile avviare o arrestare l'attività nella cartella **Attività**.

Utilizzando la Distribuzione guidata della protezione, è possibile installare Network Agent nei dispositivi client che eseguono Windows, Linux e macOS.

Per gestire applicazioni di protezione a 64 bit utilizzando Kaspersky Security Center nei dispositivi che eseguono sistemi operativi Linux, è necessario utilizzare Network Agent a 64 bit per Linux. È possibile scaricare la versione necessaria di Network Agent dal sito Web del Servizio di assistenza tecnica.

Prima dell'installazione remota di Network Agent in un dispositivo Linux, è necessario preparare il dispositivo.

Gestione delle revisioni degli oggetti

Questa sezione contiene informazioni sulla gestione delle revisioni degli oggetti. Kaspersky Security Center consente di tenere traccia delle modifiche apportate agli oggetti. Ogni volta che si salvano le modifiche apportate a un oggetto, viene creata una *revisione*. Ogni revisione ha un numero.

Gli oggetti delle applicazioni che supportano la gestione delle revisioni includono:

- Proprietà di Administration Server
- Criteri
- Attività
- Gruppi di amministrazione
- Account utente
- Pacchetti di installazione

È possibile eseguire le seguenti azioni sulle revisioni degli oggetti:

- Confrontare una revisione selezionata con quella corrente
- Confrontare le revisioni selezionate
- Confrontare un oggetto con la revisione selezionata di un altro oggetto dello stesso tipo
- Visualizzare una revisione selezionata
- Eseguire il rollback delle modifiche apportate a un oggetto a una revisione selezionata
- Salvare le revisioni come file .txt

Nella finestra delle proprietà di un oggetto che supporta la gestione delle revisioni, la sezione **Cronologia revisioni** visualizza un elenco delle revisioni degli oggetti con i seguenti dettagli:

- Numero di revisione dell'oggetto
- Data e ora di modifica dell'oggetto
- Nome dell'utente che ha modificato l'oggetto
- Azione eseguita sull'oggetto
- Descrizione della revisione relativa alla modifica apportata alle impostazioni dell'oggetto

Informazioni sulle revisioni degli oggetti

È possibile eseguire le seguenti azioni sulle revisioni degli oggetti:

- Confrontare una revisione selezionata con quella corrente
- Confrontare le revisioni selezionate
- Confrontare un oggetto con la revisione selezionata di un altro oggetto dello stesso tipo
- Visualizzare una revisione selezionata
- Eseguire il rollback delle modifiche apportate a un oggetto a una revisione selezionata
- Salvare le revisioni come file .txt

Nella finestra delle proprietà di un oggetto che supporta la gestione delle revisioni, la sezione **Cronologia revisioni** visualizza un elenco delle revisioni degli oggetti con i seguenti dettagli:

- Numero di revisione dell'oggetto
- Data e ora di modifica dell'oggetto
- Nome dell'utente che ha modificato l'oggetto

- Azione eseguita sull'oggetto
- Descrizione della revisione relativa alla modifica apportata alle impostazioni dell'oggetto

Visualizzazione della sezione Cronologia revisioni

È possibile confrontare le revisioni di un oggetto con la revisione corrente, confrontare diverse revisioni selezionate nell'elenco o confrontare la revisione di un oggetto con la revisione di un altro oggetto dello stesso tipo.

*Per visualizzare la sezione **Cronologia revisioni** di un oggetto:*

1. Nella struttura della console selezionare uno dei seguenti oggetti:
   - Nodo **Administration Server**
   - Cartella **Criteri**
   - Cartella **Attività**
   - Cartella di un gruppo di amministrazione
   - Cartella **Account utente**
   - Cartella **Oggetti eliminati**
   - Sottocartella **Pacchetti di installazione**, nidificata nella cartella **Installazione remota**
2. A seconda della posizione dell'oggetto desiderato, eseguire una delle seguenti operazioni:
   - Se l'oggetto è incluso nel nodo **Administration Server** o in un gruppo di amministrazione, fare clic con il pulsante destro del mouse sul nodo, quindi selezionare **Proprietà** nel menu di scelta rapida.
   - Se l'oggetto si trova nella cartella **Criteri**, **Attività**, **Account utente**, **Oggetti eliminati** o **Pacchetti di installazione**, selezionare la cartella e, nell'area di lavoro corrispondente, selezionare l'oggetto.

   Verrà visualizzata la finestra delle proprietà dell'oggetto.
3. Nel riquadro sinistro **Sezioni** selezionare **Cronologia revisioni**.

   La cronologia delle revisioni verrà visualizzata nell'area di lavoro.

Confronto delle revisioni degli oggetti

È possibile confrontare le revisioni precedenti di un oggetto con la revisione corrente, confrontare diverse revisioni selezionate nell'elenco o confrontare la revisione di un oggetto con la revisione di un altro oggetto dello stesso tipo.

Per confrontare le revisioni di un oggetto:

1. Selezionare un oggetto, quindi aprire la finestra delle proprietà dell'oggetto.
2. Nella finestra delle proprietà passare alla sezione **Cronologia revisioni**.

3. Nell'area di lavoro, nell'elenco delle revisioni dell'oggetto selezionare la revisione per il confronto.

   Per selezionare più di una revisione dell'oggetto, utilizzare i tasti **MAIUSC** e **CTRL**.

4. Eseguire una delle seguenti operazioni:

   - Fare clic sul pulsante **Confronta** e selezionare uno dei valori nell'elenco a discesa:

     - **Confronta con la revisione corrente**

       Selezionare questa opzione per confrontare la revisione selezionata con quella corrente.

     - **Confronta revisioni selezionate**

       Selezionare questa opzione per confrontare due revisioni selezionate.

     - **Confronta con un'altra attività**

       Se si utilizzano revisioni delle attività, selezionare **Confronta con un'altra attività** per confrontare la revisione selezionata con la revisione di un'altra attività.

       Se si utilizzano revisioni dei criteri, selezionare **Confronta con un altro criterio** per confrontare la revisione selezionata con la revisione di un altro criterio.

   - Fare doppio clic sul nome di una revisione e nella finestra delle proprietà della revisione visualizzata fare clic su uno dei seguenti pulsanti:

     - **Confronta con attuale**

       Fare clic su questo pulsante per confrontare la revisione selezionata con quella corrente.

     - **Confronta con precedente**

       Fare clic su questo pulsante per confrontare la revisione selezionata con quella precedente.

   Verrà visualizzato un rapporto in formato HTML sul confronto delle revisioni nel browser predefinito.

   In questo rapporto è possibile comprimere alcune delle sezioni con le impostazioni della revisione. Per ridurre a icona una sezione con impostazioni di revisione dell'oggetto, fare clic sull'icona della freccia (▲) accanto al nome della sezione.

Le revisioni di Administration Server includono tutti i dettagli delle modifiche apportate, ad eccezione delle informazioni relative alle seguenti aree:

- Sezione **Traffico**
- Sezione **Regole di tagging**
- Sezione **Notifica**

- Sezione **Punti di distribuzione**
- Sezione **Epidemia di virus**

  Non vengono registrate informazioni dalla sezione **Epidemia di virus** sulla configurazione di un'attivazione del criterio che si verifica quando viene attivato un evento Epidemia di virus.

È possibile confrontare le revisioni di un oggetto eliminato con una revisione di un oggetto esistente, ma non il contrario: non è possibile confrontare le revisioni di un oggetto esistente con una revisione di un oggetto eliminato.

Impostazione del periodo di archiviazione per le revisioni degli oggetti e le informazioni sugli oggetti eliminati

Il periodo di archiviazione per le revisioni degli oggetti e per le informazioni sugli oggetti eliminati è lo stesso. Il periodo di archiviazione predefinito è 90 giorni. Rappresenta un tempo sufficiente per il controllo periodico del programma.

Solo gli utenti con l'autorizzazione **Modifica** nell'area **Oggetti eliminati** possono modificare il periodo di archiviazione.

Per modificare il periodo di archiviazione per le revisioni degli oggetti e per le informazioni sugli oggetti eliminati:

1. Nella struttura della console selezionare l'Administration Server per cui si desidera modificare il periodo di archiviazione.
2. Fare clic con il pulsante destro del mouse e, nel menu di scelta rapida, selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server visualizzata, nella sezione **Archivio cronologia delle revisioni**, immettere il periodo di archiviazione desiderato (numero di giorni).
4. Fare clic su **OK**.

Le revisioni degli oggetti e le informazioni sugli oggetti eliminati verranno archiviate per il numero di giorni specificato.

Visualizzazione di una revisione degli oggetti

Se è necessario sapere quali modifiche sono state apportate a un oggetto in un determinato periodo di tempo, è possibile visualizzare le revisioni dell'oggetto.

Per visualizzare le revisioni di un oggetto:

1. Passare alla sezione **Cronologia revisioni** dell'oggetto.
2. Nell'elenco delle revisioni degli oggetti selezionare la revisione per cui si desidera visualizzare le impostazioni.
3. Eseguire una delle seguenti operazioni:
   - Fare clic sul pulsante **Visualizza revisione**.
   - Aprire la finestra delle proprietà della revisione facendo doppio clic sul nome della revisione, quindi facendo clic sul pulsante **Visualizza revisione**.

Verrà visualizzato un rapporto in formato HTML con le impostazioni della revisione dell'oggetto selezionato. In questo rapporto è possibile comprimere alcune delle sezioni con le impostazioni della revisione dell'oggetto. Per ridurre a icona una sezione con impostazioni di revisione dell'oggetto, fare clic sull'icona della freccia (▲) accanto al nome della sezione.

Salvataggio di una revisione degli oggetti in un file

È possibile salvare la revisione di un oggetto come file di testo, ad esempio per inviarla tramite e-mail.

Per salvare la revisione di un oggetto in un file:

1. Passare alla sezione **Cronologia revisioni** dell'oggetto.
2. Nell'elenco delle revisioni di un oggetto selezionare quella di cui è necessario salvare le impostazioni.
3. Fare clic sul pulsante **Avanzate** e selezionare il valore **Salva su file** nell'elenco a discesa.

   La revisione verrà salvata come file .txt.

Rollback delle modifiche

È possibile eseguire il rollback delle modifiche apportate a un oggetto, se necessario. Potrebbe ad esempio essere necessario ripristinare lo stato delle impostazioni di un criterio in una data specifica.

Per eseguire il rollback delle modifiche apportate a un oggetto:

1. Passare alla sezione **Cronologia revisioni** dell'oggetto.
2. Nell'elenco delle revisioni dell'oggetto selezionare il numero della revisione a cui eseguire il rollback delle modifiche.
3. Fare clic sul pulsante **Avanzate** e selezionare il valore **Rollback** nell'elenco a discesa.

   Verrà eseguito il rollback dell'oggetto alla revisione selezionata. L'elenco delle revisioni dell'oggetto visualizza un record dell'azione eseguita. La descrizione della revisione indica il numero della revisione a cui è stato riportato l'oggetto.

Aggiunta di una descrizione della revisione

È possibile aggiungere una descrizione per la revisione, in modo da semplificare la ricerca delle revisioni nell'elenco.

Per aggiungere una descrizione per una revisione:

1. Passare alla sezione **Cronologia revisioni** dell'oggetto.
2. Nell'elenco delle revisioni di un oggetto selezionare la revisione per cui è necessario aggiungere una descrizione.
3. Fare clic sul pulsante **Descrizione**.

4. Nella finestra **Descrizione revisione oggetto** immettere il testo relativo alla descrizione della revisione.

   Per impostazione predefinita, la descrizione della revisione dell'oggetto è vuota.

5. Fare clic su **OK**.

Eliminazione di oggetti

Questa sezione fornisce informazioni sull'eliminazione degli oggetti.

È possibile eliminare oggetti come:

- Criteri
- Attività
- Pacchetti di installazione
- Administration Server virtuali
- Utenti
- Gruppi di protezione
- Gruppi di amministrazione

Per eliminare un oggetto:

1. Aprire la sezione richiesta di Kaspersky Security Center Web Console, quindi selezionare l'oggetto.
2. Nella barra degli strumenti, fare clic sul pulsante **Elimina**.
3. Nella finestra visualizzata fare clic su **OK** per confermare la selezione.

   L'oggetto selezionato verrà eliminato.

Quando si elimina un oggetto, le relative informazioni rimangono nel database. Il periodo di archiviazione per le informazioni sugli oggetti eliminati corrisponde al periodo di archiviazione per le revisioni degli oggetti (il periodo consigliato è di 90 giorni). È possibile modificare il periodo di archiviazione solo se si dispone dell'autorizzazione **Modifica** nell'area dei diritti **Oggetti eliminati**.

Informazioni sull'eliminazione dei dispositivi client

Quando si elimina un dispositivo gestito da un gruppo di amministrazione, l'applicazione sposta il dispositivo nel gruppo Dispositivi non assegnati. Dopo l'eliminazione del dispositivo, le applicazioni Kaspersky installate, Network Agent e qualsiasi applicazione di protezione, ad esempio Kaspersky Endpoint Security, rimangono nel dispositivo.

Kaspersky Security Center gestisce i dispositivi nel gruppo Dispositivi non assegnati in base alle seguenti regole:

- Se sono state configurate regole di spostamento dei dispositivi e un dispositivo soddisfa i criteri di una regola di spostamento, il dispositivo viene spostato automaticamente in un gruppo di amministrazione in base alla regola.

- Il dispositivo viene archiviato nel gruppo Dispositivi non assegnati e rimosso automaticamente dal gruppo in base alle regole di conservazione dei dispositivi.

  Le regole di conservazione dei dispositivi non influiscono sui dispositivi con una o più unità criptate con Criptaggio dell'intero disco. Tali dispositivi non vengono eliminati automaticamente; è possibile eliminarli solo manualmente. Se è necessario eliminare un dispositivo con un'unità criptata, decriptare prima l'unità, quindi eliminare il dispositivo.

  > Quando si elimina un dispositivo con un'unità criptata, vengono eliminati anche i dati necessari per decriptare l'unità. Se si seleziona la casella di controllo **Comprendo il rischio e desidero eliminare i dispositivi selezionati** nella finestra di conferma che si apre quando si eliminano tali dispositivi (dal gruppo **Dispositivi non assegnati** o **Dispositivi gestiti**), significa che si è a conoscenza della successiva eliminazione dei dati.

  Per decriptare l'unità, devono essere soddisfatte le seguenti condizioni:

  - Il dispositivo viene riconnesso ad Administration Server al fine di ripristinare i dati necessari per decriptare l'unità.
  - L'utente del dispositivo ricorda la password di decriptaggio.
  - L'applicazione di protezione utilizzata per criptare l'unità, ad esempio Kaspersky Endpoint Security for Windows, è ancora installata nel dispositivo.

  Se l'unità è stata criptata con la tecnologia Criptaggio disco Kaspersky, è inoltre possibile provare a recuperare i dati utilizzando l'utilità di ripristino FDERT.

> In VDI, se si dispone di un dispositivo con unità criptate, le informazioni nell'unità criptata vengono eliminate dopo l'eliminazione del dispositivo.

Quando si elimina manualmente un dispositivo dal gruppo Dispositivi non assegnati, l'applicazione rimuove il dispositivo dall'elenco. Dopo l'eliminazione del dispositivo, le eventuali applicazioni Kaspersky installate rimangono nel dispositivo. Quindi, se il dispositivo è ancora visibile in Administration Server ed è stato configurato il polling di rete periodico, Kaspersky Security Center rileva il dispositivo durante il polling di rete e lo aggiunge nuovamente al gruppo Dispositivi non assegnati. Pertanto, è ragionevole eliminare manualmente un dispositivo solo se il dispositivo è invisibile ad Administration Server.

Eliminazione di un oggetto

È possibile eliminare oggetti come criteri, attività, pacchetti di installazione, utenti interni e gruppi di sicurezza interni se si dispone dell'autorizzazione Modifica, che si trova nella categoria di diritti Funzionalità di base (per ulteriori informazioni, consultare l'articolo Assegnazione delle autorizzazioni a utenti e gruppi).

Non è possibile eliminare i pacchetti di installazione utilizzati nelle attività di installazione remota. È prima necessario interrompere le attività corrispondenti. Per ulteriori informazioni sulle attività di installazione automatica in un gruppo di amministrazione, consultare l'articolo Installazione automatica delle applicazioni nei dispositivi in un gruppo di amministrazione.

Per eliminare un oggetto:

1. Nella struttura della console selezionare un oggetto nell'area di lavoro della cartella desiderata.
2. Eseguire una delle seguenti operazioni:
   - Fare clic con il pulsante destro del mouse sull'oggetto e selezionare **Elimina**.
   - Premere **CANC**.

   L'oggetto verrà eliminato e le relative informazioni saranno memorizzate nel database.

Visualizzazione delle informazioni sugli oggetti eliminati

Le informazioni sugli oggetti eliminati sono archiviate nella cartella Oggetti eliminati per lo stesso periodo di tempo delle revisioni degli oggetti (il periodo consigliato è di 90 giorni).

Solo gli utenti con l'autorizzazione **Lettura** nell'area di diritti **Oggetti eliminati** possono visualizzare l'elenco degli oggetti eliminati (per ulteriori informazioni, vedere Assegnazione delle autorizzazioni a utenti e gruppi).

Per visualizzare l'elenco degli oggetti eliminati:

Nella struttura della console selezionare **Oggetti eliminati** (per impostazione predefinita, **Oggetti eliminati** è una sottocartella della cartella **Avanzate**).

Se non si dispone dell'autorizzazione Lettura nell'area di diritti **Oggetti eliminati**, viene visualizzato un elenco vuoto nella cartella **Oggetti eliminati**.

L'area di lavoro della cartella **Oggetti eliminati** contiene le seguenti informazioni sugli oggetti eliminati:

- **Nome**. Nome dell'oggetto.
- **Tipo**. Tipo di oggetto, ad esempio criterio, attività o pacchetto di installazione.
- **Data/ora**. Ora in cui è stato eliminato l'oggetto.
- **Utente**. Nome dell'account dell'utente che ha eliminato l'oggetto.

Per visualizzare ulteriori informazioni su un oggetto:

1. Nella struttura della console selezionare **Oggetti eliminati** (per impostazione predefinita, **Oggetti eliminati** è una sottocartella della cartella **Avanzate**).
2. Nell'area di lavoro **Oggetti eliminati** selezionare l'oggetto desiderato.

   Nella parte destra dell'area di lavoro verrà visualizzata la casella per l'utilizzo dell'oggetto selezionato.
3. Eseguire una delle seguenti operazioni:

   - Fare clic sul collegamento **Proprietà** nella casella.
   - Fare clic con il pulsante destro del mouse sull'oggetto selezionato nell'area di lavoro, quindi selezionare **Proprietà** nel menu di scelta rapida.

   Verrà visualizzata la finestra delle proprietà dell'oggetto, in cui sono visualizzate le seguenti schede:

   - **Generale**
   - Cronologia revisioni

Eliminazione definitiva di oggetti dall'elenco degli oggetti eliminati

Solo gli utenti con l'autorizzazione **Modifica** nell'area di diritti **Oggetti eliminati** possono eliminare definitivamente gli oggetti dall'elenco degli oggetti eliminati (per ulteriori informazioni, vedere Assegnazione delle autorizzazioni a utenti e gruppi).

Per eliminare un oggetto dall'elenco degli oggetti eliminati:

1. Nella struttura della console selezionare il nodo di Administration Server richiesto e quindi selezionare la cartella **Oggetti eliminati**.
2. Nell'area di lavoro selezionare uno o più oggetti da eliminare.
3. Eseguire una delle seguenti operazioni:

   - Premere **CANC**.
   - Nel menu di scelta rapida degli oggetti selezionati selezionare **Elimina**.
4. Nella finestra di conferma fare clic su **Sì**.

   L'oggetto verrà eliminato definitivamente dall'elenco degli oggetti eliminati. Tutte le informazioni sull'oggetto (incluse tutte le revisioni) saranno rimosse definitivamente dal database. Non è possibile ripristinare tali informazioni.

Mobile Device Management

La gestione della protezione per i dispositivi mobili tramite Kaspersky Security Center viene eseguita utilizzando la funzionalità Mobile Device Management, che richiede una licenza dedicata. Per gestire i dispositivi mobili appartenenti ai dipendenti dell'organizzazione, è necessario abilitare Mobile Device Management.

In questa sezione vengono fornite le istruzioni per l'abilitazione, la configurazione e la disabilitazione di Mobile Device Management. Questa sezione descrive inoltre come gestire i dispositivi mobili connessi ad Administration Server.

Per dettagli su Kaspersky Security for Mobile, vedere la *Guida di Kaspersky Security for Mobile*.

Scenario: Distribuzione di Mobile Device Management

Questa sezione fornisce uno scenario per la configurazione della funzionalità Mobile Device Management in Kaspersky Security Center.

Prerequisiti

Verificare di disporre di una licenza che consenta l'accesso alla funzionalità Mobile Device Management.

Passaggi

La distribuzione della funzionalità Mobile Device Management comprende le seguenti fasi:

1. **Preparazione delle porte**

   Assicurarsi che la porta 13292 sia disponibile in Administration Server. Questa porta è necessaria per la connessione dei dispositivi mobili. Inoltre, è possibile rendere disponibile la porta 17100. Questa porta è richiesta solo per l'attivazione del server proxy per i dispositivi mobili gestiti; se i dispositivi mobili gestiti hanno accesso a Internet, non è necessario rendere disponibile questa porta.

2. **Abilitazione di Mobile Device Management**

   È possibile abilitare Mobile Device Management quando si esegue l'Avvio rapido guidato di Administration Server o in un secondo momento.

3. **Specificazione dell'indirizzo esterno di Administration Server**

   È possibile specificare l'indirizzo esterno quando si esegue l'Avvio rapido guidato di Administration Server o in un secondo momento. Se Mobile Device Management non è stato selezionato per l'installazione e non è stato specificato l'indirizzo nell'installazione guidata, specificare l'indirizzo esterno nelle proprietà del pacchetto di installazione.

4. **Aggiunta di dispositivi mobili al gruppo Dispositivi gestiti**

   Aggiungere i dispositivi mobili al gruppo Dispositivi gestiti in modo da gestire i dispositivi tramite i criteri. È possibile creare una regola di spostamento in uno dei passaggi dell'Avvio rapido guidato di Administration Server. È inoltre possibile creare la regola di spostamento in un secondo momento. Se non si crea tale regola è possibile aggiungere manualmente i dispositivi mobili al gruppo Dispositivi gestiti.

   È possibile aggiungere i dispositivi mobili direttamente al gruppo Dispositivi gestiti, oppure è possibile creare un sottogruppo (o più sottogruppi).

   Successivamente, è possibile connettere un nuovo dispositivo mobile ad Administration Server utilizzando la Connessione guidata nuovo dispositivo mobile.

5. **Creazione di un criterio per i dispositivi mobili**

   Per gestire i dispositivi mobili, creare un criterio (o più criteri) nel gruppo di appartenenza di questi dispositivi. È possibile modificare le impostazioni di questo criterio in qualsiasi momento.

Risultati

Al termine di questo scenario, è possibile gestire i dispositivi Android e iOS tramite Kaspersky Security Center. È possibile lavorare utilizzare i certificati dei dispositivi mobili e inviare comandi ai dispositivi mobili.

Informazioni sul criterio di gruppo per la gestione dei dispositivi MDM iOS

Per gestire i dispositivi MDM iOS, è possibile utilizzare il plug-in di gestione di Kaspersky Device Management for iOS, incluso nel kit di distribuzione di Kaspersky Security Center. Kaspersky Device Management for iOS consente di creare criteri di gruppo per specificare le impostazioni di configurazione dei dispositivi MDM iOS senza utilizzare l'utilità di configurazione iPhone®.

Un criterio di gruppo per la gestione dei dispositivi MDM iOS fornisce all'amministratore le seguenti opzioni:

- Configurazione delle impostazioni di protezione della password del dispositivo.
- Configurazione delle limitazioni relative all'utilizzo delle funzionalità hardware del dispositivo e delle limitazioni sull'installazione e la rimozione delle app mobili.
- Configurazione delle limitazioni sull'utilizzo delle app mobili preinstallate, ad esempio YouTube™, iTunes® Store, o Safari.
- Configurazione delle limitazioni sui contenuti multimediali (ad esempio, film e programmi TV) visualizzati in base all'area geografica in cui si trova il dispositivo.
- Configurazione della connessione del dispositivo a Internet tramite il server proxy (proxy HTTP globale).
- Configurazione dell'account tramite il quale l'utente può accedere ad applicazioni e servizi aziendali (tecnologia Single Sign-On (SSO)).
- Monitoraggio dell'utilizzo di Internet (accessi ai siti Web) nei dispositivi mobili.
- Configurazione di reti wireless (Wi-Fi), punti di accesso (APNs) e reti private virtuali (VPN) che utilizzano diversi meccanismi di autenticazione e protocolli di rete.
- Configurazione delle impostazioni della connessione ai dispositivi AirPlay® per lo streaming di foto, musica e video.
- Configurazione delle impostazioni della connessione alle stampanti AirPrint™ per la stampa di documenti dal dispositivo in modalità wireless.
- Configurazione di sincronizzazione con il server Microsoft Exchange e gli account utente per l'utilizzo dell'e-mail aziendale nei dispositivi.
- Configurazione delle credenziali utente per la sincronizzazione con il servizio directory LDAP.
- Configurazione delle credenziali utente per la connessione ai servizi CalDAV e CardDAV che consentono agli utenti di accedere a elenchi contatti e calendari aziendali.
- Configurazione delle impostazioni dell'interfaccia iOS, ad esempio tipi di carattere o icone per i siti Web preferiti, nel dispositivo dell'utente.
- Aggiunta di nuovi certificati di sicurezza nei dispositivi.

- Configurazione del server SCEP (Simple Certificate Enrollment Protocol) per il recupero automatico dei certificati dall'autorità di certificazione da parte del dispositivo.
- Aggiunta delle impostazioni personalizzate per l'utilizzo delle app mobili.

Un criterio per la gestione dei dispositivi MDM iOS ha la particolarità di essere assegnato a un gruppo di amministrazione che include MDM iOS Server (denominato collettivamente "server per dispositivi mobili"). Tutte le impostazioni specificate in questo criterio vengono per prima cosa applicate al server per dispositivi mobili e quindi ai dispositivi mobili gestiti da tale server. Nel caso di una struttura gerarchica dei gruppi di amministrazione, i server per dispositivi mobili secondari ricevono le impostazioni dei criteri dai server per dispositivi mobili primari e li distribuiscono ai dispositivi mobili.

Per maggiori informazioni su come utilizzare i criteri di gruppo per la gestione dei dispositivi MDM iOS in Kaspersky Security Center Administration Console, vedere la documentazione *Guida di Kaspersky Security for Mobile*.

Abilitazione di Mobile Device Management

Per gestire i dispositivi mobili, è necessario abilitare Mobile Device Management. Se questa funzionalità non è stata attivata durante l'Avvio rapido guidato, è possibile abilitarla in un secondo momento. Mobile Device Management richiede una licenza.

L'abilitazione di Mobile Device Management è disponibile solo nell'Administration Server primario.

Per abilitare Mobile Device Management:

1. Nella struttura della console selezionare la cartella **Mobile Device Management**.
2. Nell'area di lavoro della cartella fare clic sul pulsante **Abilita Mobile Device Management**. Questo pulsante è disponibile solo se non è stato già attivato **Mobile Device Management**.

   Viene visualizzata la pagina **Componenti aggiuntivi** dell'Avvio rapido guidato di Administration Server.
3. Selezionare **Abilita Mobile Device Management** al fine di gestire i dispositivi mobili.
4. Nella pagina **Selezionare la modalità di attivazione dell'applicazione** attivare l'applicazione utilizzando un codice di attivazione o un file chiave.

   La gestione dei dispositivi mobili non sarà possibile finché non si attiva la funzionalità Mobile Device Management.
5. Nella pagina **Impostazioni del server proxy per ottenere l'accesso a Internet** selezionare la casella di controllo **Usa server proxy** se si desidera utilizzare un server proxy durante la connessione a Internet. Quando questa casella di controllo è selezionata, i campi diventano disponibili per l'immissione delle impostazioni. Specificare le impostazioni per la connessione al server proxy.

6. Nella pagina **Verificare la disponibilità di aggiornamenti per plug-in e pacchetti di installazione** selezionare una delle seguenti opzioni:

   - **Verificare che plug-in e pacchetti di installazione siano aggiornati**

     Avvio della verifica dello stato aggiornato. Se la verifica rileva versioni obsolete di alcuni plug-in o pacchetti di installazione, verrà richiesto di scaricare le versioni aggiornate in sostituzione di quelle obsolete.

   - **Ignora verifica**

     Procedere senza verificare che plug-in e pacchetti di installazione siano aggiornati. È possibile selezionare questa opzione se, ad esempio, non si ha accesso a Internet o per qualche motivo si desidera procedere con la versione obsoleta dell'applicazione.

     Ignorare il controllo degli aggiornamenti per i plug-in può determinare il malfunzionamento dell'applicazione.

7. Nella pagina **Sono disponibili le versioni più aggiornate dei plug-in** scaricare e installare le versioni più recenti dei plug-in nella lingua richiesta dalla versione dell'applicazione. L'aggiornamento dei plug-in non richiede una licenza.

   Dopo avere installato i plug-in e i pacchetti, l'applicazione controlla se sono stati installati tutti i plug-in necessari per il corretto funzionamento dei dispositivi mobili. Se vengono rilevate versioni obsolete di alcuni plug-in, verrà richiesto di scaricare le versioni aggiornate in sostituzione di quelle obsolete.

8. Nella pagina **Impostazioni di connessione per il dispositivo mobile** impostare le porte di Administration Server.

Al termine della procedura guidata, verranno apportate le seguenti modifiche:

- Verrà creato il criterio di Kaspersky Endpoint Security for Android.
- Verrà creato il criterio di Kaspersky Device Management for iOS.
- Verranno aperte le porte nell'Administration Server per i dispositivi mobili.

Modifica delle impostazioni per Mobile Device Management

Per abilitare il supporto dei dispositivi mobili:

1. Nella struttura della console selezionare la cartella **Mobile Device Management**.
2. Nell'area di lavoro della cartella fare clic sul collegamento **Porte di connessione per i dispositivi mobili**.

   Verrà visualizzata la sezione **Porte aggiuntive** della finestra delle proprietà di Administration Server.

3. Nella sezione **Porte aggiuntive** modificare le impostazioni desiderate:

   - **Porta SSL per il server proxy di attivazione**
   - **Apri porta per i dispositivi mobili**

     Verrà aperta una porta per la connessione dei dispositivi mobili al server di licensing. È possibile definire il numero della porta e altre impostazioni nei campi sottostanti.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Porta per la sincronizzazione del dispositivo mobile**

     Numero della porta utilizzata dai dispositivi mobili per la connessione ad Administration Server e lo scambio dei dati. Il numero di porta predefinito è 13292.

     È possibile assegnare una porta diversa se la porta 13292 viene utilizzata per altri scopi.

   - **Porta per l'attivazione del dispositivo mobile**

     Porta per la connessione di Kaspersky Endpoint Security for Android ai server di attivazione di Kaspersky.

     Il numero di porta predefinito è 17100.

4. Fare clic su **OK**.

Disabilitazione di Mobile Device Management

La disabilitazione di Mobile Device Management è disponibile solo nell'Administration Server primario.

Per disabilitare Mobile Device Management:

1. Nella struttura della console selezionare la cartella **Mobile Device Management**.
2. Nell'area di lavoro di questa cartella fare clic sul collegamento **Configura componenti aggiuntivi**.

   Viene visualizzata la pagina **Componenti aggiuntivi** dell'Avvio rapido guidato di Administration Server.
3. Selezionare **Non abilitare Mobile Device Management** se non si desidera più gestire i dispositivi mobili.
4. Fare clic su **OK**.

I dispositivi mobili connessi in precedenza non saranno in grado di connettersi ad Administration Server. La porta per la connessione dei dispositivi mobili e la porta per l'attivazione dei dispositivi mobili verranno chiuse automaticamente.

I criteri creati per Kaspersky Endpoint Security for Android e Kaspersky Device Management for iOS non verranno eliminati. Le regole di emissione certificati non verranno modificate. I plug-in installati non verranno rimossi. La regola di spostamento per i dispositivi mobili non verrà eliminata.

Dopo aver abilitato nuovamente Mobile Device Management nei dispositivi mobili gestiti, potrebbe essere necessario reinstallare le app mobili richieste per la gestione dei dispositivi mobili.

Utilizzo dei comandi per i dispositivi mobili

Questa sezione contiene informazioni sui comandi per la gestione dei dispositivi mobili supportati da Kaspersky Security Center. In questa sezione vengono fornite istruzioni su come inviare comandi ai dispositivi mobili, nonché visualizzarne gli stati di esecuzione nel log dei comandi.

Comandi per Mobile Device Management

Kaspersky Security Center supporta i comandi per Mobile Device Management.

Tali comandi sono utilizzati per la funzionalità remota Mobile Device Management. Ad esempio, in caso di smarrimento del dispositivo mobile, è possibile eliminare i dati aziendali dal dispositivo tramite un comando.

È possibile utilizzare i comandi per i seguenti tipi di dispositivi mobili gestiti:

- Dispositivi MDM iOS
- Dispositivi Kaspersky Endpoint Security (KES)

Ciascun tipo di dispositivo supporta un set di comandi dedicato.

Considerazioni speciali per determinati comandi

- Per tutti i tipi di dispositivo, se viene eseguito il comando **Ripristina le impostazioni predefinite**, tutti i dati verranno eliminati dal dispositivo e per le impostazioni del dispositivo verranno ripristinati i valori predefiniti.
- Dopo l'esecuzione del comando **Cancella dati aziendali** in un dispositivo MDM iOS, vengono rimossi dal dispositivo tutti i profili di configurazione installati, i profili di provisioning, il profilo MDM iOS e le applicazioni per cui è stata selezionata la casella di controllo **Rimuovi insieme al profilo MDM iOS**.
- Se il comando **Cancella dati aziendali** viene eseguito in un dispositivo KES, verranno eliminati dal dispositivo tutti i dati aziendali, le voci dei contatti, la cronologia SMS, il registro chiamate, il calendario, le impostazioni di connessione a Internet e gli account utente, a eccezione dell'account Google™. Per i dispositivi KES verranno inoltre eliminati tutti i dati della scheda di memoria.
- Prima di inviare il comando **Localizza** a un dispositivo KES, sarà necessario confermare che questo comando viene utilizzato per la ricerca autorizzata di un dispositivo smarrito appartenente alla propria organizzazione o a uno dei dipendenti. Un dispositivo mobile che riceve il comando **Localizza** non è bloccato.

Elenco dei comandi per i dispositivi mobili

Nella seguente tabella sono visualizzati set di comandi per i dispositivi MDM iOS.

Comandi supportati per la gestione dei dispositivi mobili: dispositivi MDM iOS

Comandi	Risultato dell'esecuzione del comando
Blocca	Il dispositivo mobile viene bloccato.
Sblocca	Il blocco del dispositivo mobile con un PIN è disabilitato. Il PIN specificato in precedenza è stato reimpostato.
Ripristina le impostazioni predefinite	Tutti i dati vengono eliminati dal dispositivo mobile e vengono ripristinati i valori predefiniti delle impostazioni.
Cancella dati aziendali	Vengono eliminati dal dispositivo tutti i profili di configurazione installati, i profili di provisioning, il profilo MDM iOS e le applicazioni per cui è stata selezionata la casella di controllo **Rimuovi insieme al profilo MDM iOS**.
Sincronizza dispositivo	I dati del dispositivo mobile vengono sincronizzati con Administration Server.
Installa profilo	Il profilo di configurazione viene installato nel dispositivo mobile.
Rimuovi profilo	Il profilo di configurazione viene eliminato dal dispositivo mobile.
Installa profilo di provisioning	Il profilo di provisioning viene installato nel dispositivo mobile.
Rimuovi profilo di provisioning	Il profilo di provisioning viene eliminato dal dispositivo mobile.
Installa app	L'app viene installata nel dispositivo mobile.
Rimuovi app	L'app viene rimossa dal dispositivo mobile.
Immetti codice di riscatto	Codice di riscatto immesso per un'app a pagamento.
Configura roaming	Roaming dati e roaming voce abilitati o disabilitati.

Nella seguente tabella sono visualizzati set di comandi per i dispositivi KES.

Comandi supportati per Mobile Device Management: dispositivi KES

Comando	Risultato dell'esecuzione del comando
Blocca	Il dispositivo mobile viene bloccato.
Sblocca	Il blocco del dispositivo mobile con un PIN è disabilitato. Il PIN specificato in precedenza è stato reimpostato.
Ripristina le impostazioni predefinite	Tutti i dati vengono eliminati dal dispositivo mobile e vengono ripristinati i valori predefiniti delle impostazioni.
Cancella dati aziendali	Vengono eliminati tutti i dati aziendali, le voci dei contatti, la cronologia SMS, il registro chiamate, il calendario, le impostazioni di connessione a Internet e gli account utente, a eccezione dell'account Google. I dati della scheda di memoria sono stati cancellati.
Sincronizza dispositivo	I dati del dispositivo mobile vengono sincronizzati con Administration Server.
Localizza dispositivo	Il dispositivo mobile viene localizzato e visualizzato in Google Maps™. L'operatore di telefonia mobile addebita un costo per l'invio dei messaggi SMS e per la fornitura della connessione Internet.
Foto utente	Il dispositivo mobile viene bloccato. La foto viene scattata dalla fotocamera anteriore ed è salvata in Administration Server. Le foto possono essere visualizzate nel registro dei comandi. L'operatore di telefonia mobile addebita un costo per l'invio dei messaggi SMS e per la fornitura della connessione Internet.
Allarme	Il dispositivo mobile riproduce un allarme.

Utilizzo di Firebase Cloud Messaging

Per garantire l'invio tempestivo dei comandi ai dispositivi KES gestiti dal sistema operativo Android, Kaspersky Security Center usa il meccanismo delle notifiche push. Le notifiche push vengono scambiate tra i dispositivi KES e Administration Server tramite Firebase Cloud Messaging (di seguito FCM). In Kaspersky Security Center Administration Console è possibile specificare le impostazioni di Cloud Firebase Messaging per la connessione dei dispositivi KES al servizio.

Per recuperare le impostazioni di Firebase Cloud Messaging, è necessario disporre di un account Google.

Per abilitare l'utilizzo di FCM:

1. In Administration Console selezionare il nodo **Mobile Device Management** e la cartella **Dispositivi mobili**.
2. Dal menu di scelta rapida della cartella **Dispositivi mobili** selezionare **Proprietà**.
3. Nelle proprietà della cartella selezionare la sezione **Impostazioni di Firebase Cloud Messaging**.
4. Nel campo **Numero progetto Firebase**, specificare l'ID del mittente FCM.
5. Nel campo **File della chiave privata (in formato JSON)**, selezionare il file della chiave privata.

   Alla successiva sincronizzazione con Administration Server, i dispositivi KES gestiti da sistemi operativi Android verranno connessi a Firebase Cloud Messaging.

È possibile modificare le impostazioni di Firebase Cloud Messaging facendo clic sul pulsante **Ripristina impostazioni**.

Invio di comandi

Per inviare un comando al dispositivo mobile dell'utente:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.
2. Selezionare il dispositivo mobile dell'utente a cui è necessario inviare un comando.
3. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

4. Nella finestra **Comandi per Mobile Device Management** passare alla sezione con il nome del comando che si desidera inviare al dispositivo mobile, quindi fare clic sul pulsante **Invia comando**.

   A seconda del comando selezionato, facendo clic sul pulsante **Invia comando** verrà visualizzata la finestra delle impostazioni avanzate dell'applicazione. Quando ad esempio si invia il comando per l'eliminazione di un profilo di provisioning da un dispositivo mobile, all'utente verrà richiesto di selezionare il profilo di provisioning da eliminare dal dispositivo. Definire le impostazioni avanzate del comando in tale finestra e confermare la selezione. Il comando sarà inviato al dispositivo mobile.

   È possibile fare clic sul pulsante **Rinvia** per inviare nuovamente il comando al dispositivo mobile dell'utente.

   È possibile fare clic sul pulsante **Rimuovi dalla coda** per annullare l'esecuzione di un comando inviato se il comando non è ancora stato eseguito.

   Nella sezione **Log dei comandi** vengono visualizzati i comandi che sono stati inviati al dispositivo mobile, con i rispettivi stati di esecuzione. Fare clic su **Aggiorna** per aggiornare l'elenco dei comandi.

5. Fare clic su **OK** per chiudere la finestra **Comandi per Mobile Device Management**.

Visualizzazione dello stato dei comandi nel log dei comandi

L'applicazione salva nel log dei comandi le informazioni su tutti i comandi che sono stati inviati ai dispositivi mobili. Nel log dei comandi sono contenute informazioni sulla data e l'ora in cui ciascun comando è stato inviato al dispositivo mobile, i relativi stati e descrizioni dettagliate dei risultati dell'esecuzione dei comandi. Ad esempio, nel caso in cui l'esecuzione di un comando non vada a buon fine, nel log sarà visualizzata la causa dell'errore. I record sono memorizzati nel log dei comandi per un massimo di 30 giorni.

I comandi inviati ai dispositivi mobili possono avere i seguenti stati:

- *In esecuzione* – Il comando è stato inviato al dispositivo mobile.
- *Completato* – L'esecuzione del comando è stata completata correttamente.
- *Completato con errori* – L'esecuzione del comando non è riuscita.
- *Eliminazione in corso* – È in corso la rimozione del comando dalla coda dei comandi inviati al dispositivo mobile.
- *Eliminato* – Il comando è stato rimosso dalla coda dei comandi inviati al dispositivo mobile.
- *Errore durante l'eliminazione* – È stato impossibile rimuovere il comando dalla coda dei comandi inviati al dispositivo mobile.

L'applicazione gestisce un log dei comandi per ogni dispositivo mobile.

Per visualizzare il registro dei comandi inviati a un dispositivo mobile:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

2. Nell'elenco dei dispositivi mobili selezionare quello per cui si desidera visualizzare il registro dei comandi.

3. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

   Verrà visualizzata la finestra **Comandi per Mobile Device Management**. Le sezioni della finestra **Comandi per Mobile Device Management** corrispondono ai comandi che possono essere inviati al dispositivo mobile.

4. Selezionare le sezioni contenenti i comandi necessari e visualizzare le informazioni su come tali comandi vengono inviati ed eseguiti nella sezione **Log dei comandi**.

Nella sezione **Log dei comandi** è possibile visualizzare l'elenco dei comandi che sono stati inviati al dispositivo mobile oltre a dettagli su tali comandi. Il filtro **Mostra comandi** consente di visualizzare nell'elenco solo i comandi con lo stato selezionato.

Utilizzo dei certificati dei dispositivi mobili

Questa sezione contiene informazioni sull'utilizzo dei certificati dei dispositivi mobili.

Il certificato root per i dispositivi mobili ha una scadenza fissa di 700 giorni dopo la generazione. Il certificato di riserva viene generato 60 giorni prima della data di scadenza. È possibile modificare il periodo di tempo per la generazione di un certificato di riserva con il seguente comando:

`klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <timeout in secondi>`

Il periodo di tempo per la generazione di un certificato di riserva deve essere sufficientemente lungo da consentire a tutti i dispositivi mobili gestiti di sincronizzarsi con Administration Server e recuperare il certificato.

L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

Il rinnovo manuale del certificato root per i dispositivi mobili non è supportato.

Avvio dell'Installazione guidata certificato

È possibile installare i seguenti tipi di certificati nel dispositivo mobile di un utente:

- Certificati condivisi per l'identificazione del dispositivo mobile
- Certificati di posta per la configurazione della posta aziendale nel dispositivo mobile
- Certificato VPN per la configurazione dell'accesso a una rete privata virtuale (VPN) nel dispositivo mobile

Per installare un certificato nel dispositivo mobile di un utente:

1. Nella struttura della console espandere la cartella **Mobile Device Management**, quindi selezionare la sottocartella **Certificati**.

2. Nell'area di lavoro della cartella **Certificati** fare clic sul collegamento **Aggiungi certificato** per eseguire l'Installazione guidata certificato.

   Seguire le istruzioni della procedura guidata.

Al termine della procedura guidata, verrà creato un certificato che sarà aggiunto all'elenco dei certificati dell'utente; verrà inoltre inviata una notifica all'utente contenente un collegamento per il download e l'installazione del certificato nel dispositivo mobile. È possibile visualizzare l'elenco di tutti i certificati ed esportarlo in un file. È possibile eliminare e riemettere i certificati, nonché visualizzarne le proprietà.

Passaggio 1. Selezionare il tipo di certificato

Specificare il tipo di certificato che deve essere installato nel dispositivo mobile dell'utente:

- **Certificato mobile**: per l'identificazione del dispositivo mobile
- **Certificato di posta**: per la configurazione della posta aziendale nel dispositivo mobile
- **Certificato VPN**: per la configurazione dell'accesso a una rete privata virtuale (VPN) nel dispositivo mobile

Passaggio 2. Selezione del tipo di dispositivo

Questa finestra viene visualizzata solo se è stato selezionato **Certificato di posta** o **Certificato VPN** come tipo di certificato.

Specificare il tipo di sistema operativo nel dispositivo:

- **Dispositivo MDM iOS**. Selezionare questa opzione se è necessario installare un certificato in un dispositivo mobile connesso al server MDM iOS utilizzando il protocollo MDM iOS.
- **Dispositivo KES gestito da Kaspersky Security for Mobile**. Selezionare questa opzione se è necessario installare un certificato in un dispositivo KES. In questo caso, il certificato verrà utilizzato per l'identificazione dell'utente a ogni connessione all'Administration Server.
- **Dispositivo KES connesso ad Administration Server senza l'autenticazione del certificato utente**. Selezionare questa opzione se è necessario installare un certificato in un dispositivo KES senza l'utilizzo dell'autenticazione del certificato. In questo caso, durante il passaggio finale della procedura guidata, nella finestra **Metodo di notifica all'utente** l'amministratore deve selezionare il tipo di autenticazione utente utilizzato a ogni connessione ad Administration Server.

Passaggio 3. Selezione di un utente

Nell'elenco selezionare gli utenti, i gruppi di sicurezza o i gruppi di sicurezza Active Directory per cui è necessario installare il certificato.

Nella finestra **Selezione utente** è possibile eseguire una ricerca degli utenti interni di Kaspersky Security Center. È possibile fare clic su **Aggiungi** per aggiungere un utente interno.

Passaggio 4. Selezione dell'origine del certificato

In questa finestra è possibile selezionare l'origine del certificato che verrà utilizzato da Administration Server per identificare il dispositivo mobile. È possibile specificare un certificato utilizzando uno dei seguenti metodi:

- Creare un certificato automaticamente, tramite gli strumenti di Administration Server, quindi inviare il certificato al dispositivo.

- Specificare un file di certificato che è stato creato in precedenza. Questo metodo non è disponibile se sono stati selezionati più utenti nel passaggio precedente.

Se è necessario inviare a un utente una notifica relativa alla creazione di un certificato per il dispositivo mobile, selezionare la casella di controllo **Pubblica certificato**.

Se il dispositivo mobile dell'utente è già stato autenticato in precedenza tramite un certificato, quindi non è necessario specificare il nome di un account e la password per ricevere un nuovo certificato, deselezionare la casella di controllo **Pubblica certificato**. In questo caso, la finestra **Metodo di notifica all'utente** non verrà visualizzata.

Passaggio 5. Assegnazione di un tag al certificato

La finestra **Tag certificato** viene visualizzata se **Dispositivo MDM iOS** è stato selezionato in **Tipo di dispositivo**.

Nell'elenco a discesa è possibile assegnare un tag al certificato del dispositivo MDM iOS dell'utente. Il certificato con il tag assegnato può avere specifici parametri impostati per il tag nelle proprietà del criterio di Kaspersky Device Management for iOS.

L'elenco a discesa richiede di selezionare il tag *Modello di certificato 1*, *Modello di certificato 2* o *Modello di certificato 3*. È possibile configurare i tag nelle seguenti sezioni:

- Se è stato selezionato **Certificato di posta** nella finestra **Tipo di certificato**, i relativi tag possono essere configurati nelle proprietà dell'account Exchange ActiveSync per i dispositivi mobili (**Dispositivi gestiti** → **Criteri** → Proprietà del criterio di Kaspersky Device Management for iOS → sezione **Exchange ActiveSync** → **Aggiungi** → **Avanzate**).

- Se è stato selezionato **Certificato VPN** nella finestra **Tipo di certificato**, i relativi tag possono essere configurati nelle proprietà della VPN per i dispositivi mobili (**Dispositivi gestiti** → **Criteri** → Proprietà del criterio di Kaspersky Device Management for iOS → sezione **VPN** → **Aggiungi** →**Avanzate**). Non è possibile configurare i tag utilizzati per i certificati VPN se è selezionato il tipo di connessione L2TP, PPTP o IPSec (Cisco™) per la VPN.

Passaggio 6. Specificazione delle impostazioni di pubblicazione del certificato

In questa finestra è possibile specificare le seguenti impostazioni di pubblicazione del certificato:

- **Non inviare una notifica all'utente su un nuovo certificato**

  Abilitare questa opzione se non si desidera inviare a un utente una notifica sulla creazione di un certificato per il dispositivo mobile dell'utente. In questo caso, la finestra **Metodo di notifica all'utente** non verrà visualizzata.

  Questa opzione è disponibile solo per i dispositivi in cui è installato Kaspersky Endpoint Security for Android.

  È consigliabile abilitare questa opzione, ad esempio se il dispositivo mobile dell'utente è già stato precedentemente autenticato tramite un certificato, in modo da evitare di dover specificare un nome account e la password per ricevere un nuovo certificato.

- **Consenti al dispositivo di avere più ricezioni di un singolo certificato (solo per i dispositivi in cui è installato Kaspersky Endpoint Security for Android)**

  Abilitare questa opzione se si desidera che Kaspersky Security Center reinvii automaticamente il certificato ogni volta che sta per scadere o quando non viene trovato nel dispositivo di destinazione.

  Il certificato viene reinviato automaticamente diversi giorni prima della data di scadenza del certificato. È possibile impostare il numero di giorni nella finestra Regole di emissione certificati.

  In alcuni casi, è impossibile trovare il certificato nel dispositivo. Questo può ad esempio verificarsi quando l'utente reinstalla l'applicazione di protezione Kaspersky nel dispositivo o reimposta le impostazioni e i dati del dispositivo alle impostazioni predefinite. In questo caso, Kaspersky Security Center controlla l'ID dispositivo al successivo tentativo del dispositivo di connettersi all'Administration Server. Se il dispositivo ha lo stesso ID che aveva nel momento in cui è stato emesso il certificato, l'applicazione reinvia il certificato al dispositivo.

Passaggio 7. Selezione del metodo di notifica all'utente

Questa finestra non viene visualizzata se è stato selezionato **Dispositivo MDM iOS** come tipo di dispositivo o se è stata selezionata l'opzione **Non inviare una notifica all'utente su un nuovo certificato**.

Nella finestra **Metodo di notifica all'utente** è possibile configurare la notifica utente in merito all'installazione del certificato nel dispositivo mobile.

Nel campo **Metodo di autenticazione** specificare il tipo di autenticazione utente:

- **Credenziali (dominio o alias)**

  In questo caso, l'utente utilizza la password di dominio o la password di un utente interno di Kaspersky Security Center per ricevere un nuovo certificato.

- **Password monouso**

  In questo caso, l'utente riceve una password monouso che verrà inviata tramite e-mail o SMS. È necessario immettere questa password per ricevere un nuovo certificato.

  Questa opzione diventa **Password** se è stata abilitata (selezionata) l'opzione **Consenti al dispositivo più ricezioni di un singolo certificato (solo per i dispositivi in cui sono installate applicazioni di protezione Kaspersky per dispositivi mobili)** nella finestra **Impostazioni di pubblicazione del certificato**.

- **Password**

  In questo caso, la password viene utilizzata ogni volta che il certificato viene inviato all'utente.

  Questa opzione diventa **Password monouso** se è stata disabilitata (deselezionata) l'opzione **Consenti al dispositivo più ricezioni di un singolo certificato (solo per i dispositivi in cui sono installate applicazioni di protezione Kaspersky per dispositivi mobili)** nella finestra **Impostazioni di pubblicazione del certificato**.

Questo campo viene visualizzato se è stato selezionato **Certificato mobile** nella finestra **Tipo di certificato** o se è stato selezionato **Dispositivo KES connesso ad Administration Server senza l'autenticazione del certificato utente** come tipo di dispositivo.

Selezionare l'opzione per la notifica all'utente:

- **Mostra la password di autenticazione al termine della procedura guidata**

  Se si seleziona questa opzione, nel passaggio finale dell'Installazione guidata certificato verranno visualizzati il nome utente, il nome utente in Security Account Manager (SAM) e la password per il recupero del certificato per ogni utente selezionato. La configurazione della notifica all'utente dell'installazione di un certificato non sarà disponibile.

  Quando si aggiungono certificati per più utenti, è possibile salvare le credenziali specificate in un file facendo clic sul pulsante **Esporta** durante l'ultimo passaggio dell'Installazione guidata certificato.

  Questa opzione non è disponibile se è stata selezionata l'opzione **Credenziali (dominio o alias)** durante il passaggio **Metodo di notifica all'utente** dell'Installazione guidata certificato.

- **Invia una notifica all'utente sul nuovo certificato**

  Se si seleziona questa opzione, è possibile configurare la notifica all'utente su un nuovo certificato.

  - **Tramite e-mail**

    In questo gruppo di impostazioni è possibile configurare la notifica all'utente dell'installazione di un nuovo certificato nel dispositivo mobile tramite messaggi e-mail. Questo metodo di notifica è disponibile solo se l'opzione Server SMTP è abilitata.

    Fare clic sul collegamento **Modifica messaggio** per visualizzare e modificare il messaggio di notifica, se necessario.

  - **Tramite SMS**

    In questo gruppo di impostazioni è possibile configurare la notifica all'utente sull'utilizzo di un SMS per l'installazione di un certificato nei dispositivi mobili. Questo metodo di notifica è disponibile solo se l'opzione Notifica tramite SMS è abilitata.

    Fare clic sul collegamento **Modifica messaggio** per visualizzare e modificare il messaggio di notifica, se necessario.

Passaggio 8. Generazione del certificato

In questo passaggio viene creato il certificato.

È possibile fare clic su **Fine** per uscire dalla procedura guidata.

Il certificato viene generato e visualizzato nell'elenco dei certificati nell'area di lavoro della cartella **Certificati**.

Configurazione delle regole di emissione dei certificati

I certificati vengono utilizzati per l'autenticazione dei dispositivi in Administration Server. Tutti i dispositivi mobili gestiti devono disporre di certificati. È possibile configurare la modalità di emissione dei certificati.

Per configurare le regole di emissione dei certificati:

1. Nella struttura della console espandere la cartella **Mobile Device Management**, quindi selezionare la sottocartella **Certificati**.

2. Nell'area di lavoro della cartella **Certificati** fare clic sul pulsante **Configura regole di emissione certificati** per aprire la finestra **Regole di emissione certificati**.

3. Passare alla sezione con il nome di un tipo di certificato:

   Emissione di certificati mobili: per configurare l'emissione dei certificati per i dispositivi mobili.

   Emissione di certificati di posta: per configurare l'emissione dei certificati di posta.

   Emissione di certificati VPN: per configurare l'emissione dei certificati VPN.

4. Nella sezione **Impostazioni di emissione** configurare l'emissione del certificato:

   - Specificare la durata del certificato in giorni.

     I certificati per i dispositivi mobili sono limitati dalla data di scadenza del certificato root. Se si specifica una durata del certificato più lunga della data di scadenza del certificato root, la durata del certificato verrà adattata automaticamente al momento della generazione.

   - Selezionare un'origine certificato (**Administration Server** o **Certificati specificati manualmente**).

     Administration Server è selezionato come origine predefinita dei certificati.

   - Specificare un modello di certificato (**Modello predefinito**, **Altro modello**).

     La configurazione dei modelli è disponibile se nella sezione **Integrazione con PKI** è abilitata l'integrazione con infrastruttura a chiave pubblica (PKI).

5. Nella sezione **Impostazioni degli aggiornamenti automatici** configurare gli aggiornamenti automatici del certificato:

   - Nel campo **Rinnova quando la scadenza del certificato è prevista tra (giorni)** specificare con quanti giorni di anticipo prima della scadenza deve essere rinnovato il certificato.

   - Per abilitare gli aggiornamenti automatici dei certificati, selezionare la casella di controllo **Riemetti automaticamente il certificato se possibile**.

6. Nella sezione **Protezione tramite password** abilitare e configurare l'utilizzo di una password durante il decriptaggio dei certificati.

   > Protezione tramite password è disponibile solo per i certificati mobili.

   a. Selezionare la casella di controllo **Richiedi la password durante l'installazione del certificato**.

   b. Utilizzare l'indicatore scorrevole per definire il numero massimo di simboli nella password per il criptaggio.

7. Fare clic su **OK**.

Integrazione con PKI (Public Key Infrastructure)

Per semplificare l'emissione dei certificati di dominio agli utenti è richiesta l'integrazione dell'applicazione con PKI (Public Key Infrastructure). In seguito all'integrazione, i certificati vengono rilasciati automaticamente.

La versione minima supportata del server PKI è Windows Server 2008.

È necessario configurare l'account per l'integrazione con PKI. L'account deve soddisfare i seguenti requisiti:

- Essere un utente di dominio e un amministratore in un dispositivo in cui è installato Administration Server.
- Disporre del privilegio SeServiceLogonRight nel dispositivo in cui è installato Administration Server.

Per creare un profilo utente permanente, eseguire l'accesso almeno una volta utilizzando l'account configurato nel dispositivo in cui è installato Administration Server. Nell'archivio dei certificati dell'utente nel dispositivo Administration Server installare l'Enrollment Agent Certificate fornito dagli amministratori del dominio.

Per configurare l'integrazione con PKI (Public Keys Infrastructure):

1. Nella struttura della console espandere la cartella **Mobile Device Management**, quindi selezionare la sottocartella **Certificati**.
2. Nell'area di lavoro fare clic sul pulsante **Integra con infrastruttura a chiave pubblica (PKI)** per aprire la sezione **Integrazione con PKI** della finestra **Regole di emissione certificati**.

   Verrà visualizzata la sezione **Integrazione con PKI** della finestra **Regole di emissione certificati**.
3. Selezionare la casella di controllo **Integra emissione certificati con PKI**.
4. Nel campo **Account** specificare il nome dell'account utente da utilizzare per l'integrazione con l'infrastruttura a chiave pubblica (PKI).
5. Nel campo **Password** immettere la password di dominio per l'account.
6. Nell'elenco **Nome del modello di certificato nel sistema PKI** selezionare il modello di certificato che verrà utilizzato per l'emissione dei certificati per gli utenti di dominio.

   In Kaspersky Security Center verrà eseguito un servizio dedicato con l'account specificato. Tale servizio si occupa dell'emissione dei certificati di dominio degli utenti. Il servizio viene eseguito quando l'elenco dei modelli di certificato viene caricato facendo clic sul pulsante **Aggiorna elenco** o quando si genera un certificato.
7. Fare clic su **OK** per salvare le impostazioni.

In seguito all'integrazione, i certificati vengono rilasciati automaticamente.

Abilitazione del supporto per la delega vincolata Kerberos

L'applicazione supporta l'utilizzo della delega vincolata Kerberos.

Per abilitare il supporto per la delega vincolata Kerberos:

1. Nella struttura della console aprire la cartella **Mobile Device Management**.
2. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Server per dispositivi mobili**.
3. Nell'area di lavoro della cartella **Server per dispositivi mobili** selezionare un server per dispositivi mobili MDM iOS.
4. Nel menu di scelta rapida del server per dispositivi mobili MDM iOS selezionare **Proprietà**.
5. Nella finestra delle proprietà del server per dispositivi mobili MDM iOS selezionare la sezione **Impostazioni**.
6. Nella sezione **Impostazioni** selezionare la casella di controllo **Assicura la compatibilità con la delega vincolata Kerberos**.
7. Fare clic su **OK**.

Aggiunta dei dispositivi mobili iOS all'elenco dei dispositivi gestiti

Per aggiungere un dispositivo mobile iOS all'elenco dei dispositivi gestiti, è necessario inviare e installare un certificato condiviso nel dispositivo. I certificati condivisi vengono utilizzati da Administration Server per l'identificazione dei dispositivi mobili. Un certificato condiviso per un dispositivo mobile iOS viene distribuito all'interno di un profilo MDM iOS. In seguito all'invio e all'installazione di un certificato condiviso in un dispositivo mobile, il dispositivo viene visualizzato nell'elenco dei dispositivi gestiti.

Kaspersky non supporta più Kaspersky Safe Browser.

È possibile aggiungere dispositivi mobili degli utenti all'elenco dei dispositivi gestiti tramite la Connessione guidata nuovo dispositivo mobile.

Per connettere un dispositivo iOS ad Administration Server utilizzando un certificato condiviso:

1. Avviare la Connessione guidata nuovo dispositivo mobile in uno dei seguenti modi:

   - Utilizzare il menu di scelta rapida nella cartella **Account utente**:

     1. Nella struttura della console espandere la cartella **Avanzate** e selezionare la sottocartella **Account utente**.

     2. Nell'area di lavoro della cartella **Account utente** selezionare gli utenti, i gruppi di sicurezza o gruppi di sicurezza Active Directory per cui si desidera aggiungere i dispositivi mobili all'elenco dei dispositivi gestiti.

     3. Fare clic con il pulsante destro del mouse e, nel menu di scelta rapida dell'account utente, selezionare **Aggiungi dispositivo mobile**.

        Verrà avviata la Connessione guidata nuovo dispositivo mobile.

   - Nell'area di lavoro della cartella **Dispositivi mobili** fare clic sul pulsante **Aggiungi dispositivo mobile**:

     1. Nella struttura della console espandere la cartella **Mobile Device Management**, quindi selezionare la sottocartella **Dispositivi mobili**.

     2. Nell'area di lavoro della sottocartella **Dispositivi mobili** fare clic sul pulsante **Aggiungi dispositivo mobile**.

        Verrà avviata la Connessione guidata nuovo dispositivo mobile.

2. Nella pagina **Sistema operativo** della procedura guidata selezionare **iOS** come tipo di sistema operativo del dispositivo mobile.

3. Nella pagina **Selezionare un server per dispositivi mobili MDM iOS** selezionare il server per dispositivi mobili MDM iOS.

4. Nella pagina **Selezionare gli utenti di cui si desidera gestire i dispositivi mobili** selezionare gli utenti, i gruppi di sicurezza o gruppi di sicurezza Active Directory per cui si desidera aggiungere i dispositivi mobili all'elenco dei dispositivi gestiti.

   Questo passaggio viene ignorato se la procedura guidata viene avviata selezionando **Aggiungi dispositivo mobile** nel menu di scelta rapida della cartella **Account utente**.

   Se si desidera aggiungere un nuovo account utente nell'elenco, fare clic sul pulsante **Aggiungi** e inserire le proprietà dell'account utente nella finestra visualizzata. Se si desidera modificare o esaminare le proprietà dell'account utente, selezionare l'account utente nell'elenco e fare clic sul pulsante **Proprietà**.

5. Nella pagina **Origine certificato** della procedura guidata specificare il metodo per la creazione del certificato condiviso che Administration Server utilizzerà per identificare il dispositivo mobile. È possibile specificare un certificato condiviso utilizzando una delle seguenti modalità:

   - **Emetti il certificato utilizzando gli strumenti di Administration Server**

     Selezionare questa opzione per creare un nuovo certificato tramite gli strumenti di Administration Server se non è stato creato in precedenza.

     Se questa opzione è selezionata, il profilo MDM iOS verrà firmato automaticamente con un certificato generato da Administration Server.

     Questa opzione è selezionata per impostazione predefinita.

   - **Specifica un file di certificato**

     Selezionare questa opzione per specificare un file di certificato creato in precedenza.

     Questo metodo non è disponibile se sono stati selezionati più utenti nel passaggio precedente.

6. Nella pagina **Metodo di notifica all'utente** della procedura guidata definire le impostazioni per la notifica all'utente del dispositivo mobile tramite SMS o e-mail relativa alla creazione del certificato:

   - **Mostra codice QR nella procedura guidata**

     Se si seleziona questa opzione, verrà visualizzato un collegamento al pacchetto di installazione nel passaggio finale della Connessione guidata nuovo dispositivo.

     Questa opzione non è disponibile se sono stati selezionati più utenti per la connessione del dispositivo.

   - **Invia codice QR all'utente**

     Questa opzione consente di configurare la notifica per l'utente della connessione di un nuovo dispositivo mobile.

     È possibile selezionare il tipo di indirizzo e-mail, specificare un indirizzo e-mail aggiuntivo e modificare il testo del messaggio. È anche possibile selezionare il tipo di telefono dell'utente per l'invio di un messaggio SMS, specificare un numero di telefono aggiuntivo e modificare il testo del messaggio SMS.

     Se il server SMTP non è stato configurato, non è possibile inviare messaggi e-mail agli utenti. Se le notifiche SMS non sono state configurate, non è possibile inviare messaggi SMS agli utenti.

7. Nella pagina **Risultato**, fare clic su **Fine** per chiudere la procedura guidata.

Il profilo MDM iOS verrà automaticamente pubblicato nel server Web di Kaspersky Security Center. L'utente del dispositivo mobile riceve una notifica con un collegamento per scaricare il profilo MDM iOS dal server Web. L'utente fa clic sul collegamento. Successivamente, il sistema operativo del dispositivo mobile richiede all'utente di accettare l'installazione del profilo MDM iOS. L'utente deve accettare di installare il profilo MDM iOS prima di avviare il download del profilo MDM iOS nel dispositivo mobile. Dopo aver scaricato il profilo MDM iOS e aver sincronizzato il dispositivo mobile con Administration Server, il dispositivo verrà visualizzato in **Dispositivi mobili**, una sottocartella di **Mobile Device Management** nella struttura della console.

Per consentire all'utente di passare al server Web di Kaspersky Security Center utilizzando il collegamento, la connessione con Administration Server tramite la porta 8061 deve essere disponibile nel dispositivo mobile.

Aggiunta dei dispositivi mobili Android all'elenco dei dispositivi gestiti

Per aggiungere un dispositivo mobile Android all'elenco dei dispositivi gestiti, nel dispositivo mobile devono essere distribuiti e installati Kaspersky Endpoint Security for Android e un certificato condiviso. I certificati condivisi vengono utilizzati da Administration Server per l'identificazione dei dispositivi mobili. In seguito all'invio e all'installazione di un certificato condiviso in un dispositivo mobile, il dispositivo viene visualizzato nell'elenco dei dispositivi gestiti.

È possibile aggiungere dispositivi mobili degli utenti all'elenco dei dispositivi gestiti tramite la Connessione guidata nuovo dispositivo mobile. La procedura guidata offre due opzioni per la distribuzione e l'installazione di un certificato condiviso e di Kaspersky Endpoint Security for Android:

- Utilizzando un collegamento a Google Play
- Tramite un collegamento del Server Web di Kaspersky Security Center

  Il pacchetto di installazione di Kaspersky Endpoint Security for Android archiviato per la distribuzione in Administration Server viene utilizzato per l'installazione

Avvio della Connessione guidata nuovo dispositivo mobile

Per avviare la Connessione guidata nuovo dispositivo mobile, effettuare una delle seguenti operazioni:

- Utilizzare il menu di scelta rapida nella cartella **Account utente**:

  1. Nella struttura della console espandere la cartella **Avanzate** e selezionare la sottocartella **Account utente**.
  2. Nell'area di lavoro della cartella **Account utente** selezionare gli utenti, i gruppi di sicurezza o gruppi di sicurezza Active Directory per cui si desidera aggiungere i dispositivi mobili all'elenco dei dispositivi gestiti.
  3. Fare clic con il pulsante destro del mouse e, nel menu di scelta rapida dell'account utente, selezionare **Aggiungi dispositivo mobile**.

     Verrà avviata la Connessione guidata nuovo dispositivo mobile.

- Nell'area di lavoro della cartella **Dispositivi mobili** fare clic sul pulsante **Aggiungi dispositivo mobile**:

  1. Nella struttura della console espandere la cartella **Mobile Device Management**, quindi selezionare la sottocartella **Dispositivi mobili**.
  2. Nell'area di lavoro della sottocartella **Dispositivi mobili** fare clic sul pulsante **Aggiungi dispositivo mobile**.

     Verrà avviata la Connessione guidata nuovo dispositivo mobile.

Aggiunta di un dispositivo mobile Android tramite un collegamento a Google Play

Per installare Kaspersky Endpoint Security for Android e un certificato condiviso in un dispositivo mobile utilizzando un collegamento a Google Play:

1. Avviare la Connessione guidata nuovo dispositivo mobile.
2. Nella pagina **Sistema operativo** della procedura guidata selezionare **Android** come tipo di sistema operativo del dispositivo mobile.
3. Nella pagina **Metodo per installare Kaspersky Endpoint Security for Android nei dispositivi** della procedura guidata selezionare **Scarica l'app da Google Play**.
4. Nella pagina **Selezionare gli utenti di cui si desidera gestire i dispositivi mobili** della procedura guidata selezionare gli utenti, i gruppi di sicurezza o gruppi di sicurezza Active Directory per cui si desidera aggiungere i dispositivi mobili all'elenco dei dispositivi gestiti.

   Questo passaggio viene ignorato se la procedura guidata viene avviata selezionando **Aggiungi dispositivo mobile** nel menu di scelta rapida della cartella **Account utente**.

   Se si desidera aggiungere un nuovo account utente nell'elenco, fare clic sul pulsante **Aggiungi** e inserire le proprietà dell'account utente nella finestra visualizzata. Se si desidera modificare o esaminare le proprietà dell'account utente, selezionare l'account utente nell'elenco e fare clic sul pulsante **Proprietà**.
5. Nella pagina **Origine certificato** della procedura guidata specificare il metodo per la creazione del certificato condiviso che Administration Server utilizzerà per identificare il dispositivo mobile. È possibile specificare un certificato condiviso utilizzando una delle seguenti modalità:

   - **Emetti il certificato utilizzando gli strumenti di Administration Server**

     Selezionare questa opzione per creare un nuovo certificato tramite gli strumenti di Administration Server se non è stato creato in precedenza.

     Se questa opzione è selezionata, il certificato viene rilasciato automaticamente utilizzando gli strumenti di Administration Server.

     Questa opzione è selezionata per impostazione predefinita.

   - **Specifica un file di certificato**

     Selezionare questa opzione per specificare un file di certificato creato in precedenza.

     Questo metodo non è disponibile se sono stati selezionati più utenti nel passaggio precedente.

6. Nella pagina **Metodo di notifica all'utente** della procedura guidata definire le impostazioni per la notifica all'utente del dispositivo mobile tramite SMS o e-mail relativa alla creazione del certificato:

   - **Mostra codice QR nella procedura guidata**

     Se si seleziona questa opzione, verrà visualizzato un collegamento al pacchetto di installazione nel passaggio finale della Connessione guidata nuovo dispositivo.

     Questa opzione non è disponibile se sono stati selezionati più utenti per la connessione del dispositivo.

   - **Invia codice QR all'utente**

     Questa opzione consente di configurare la notifica per l'utente della connessione di un nuovo dispositivo mobile.

     È possibile selezionare il tipo di indirizzo e-mail, specificare un indirizzo e-mail aggiuntivo e modificare il testo del messaggio. È anche possibile selezionare il tipo di telefono dell'utente per l'invio di un messaggio SMS, specificare un numero di telefono aggiuntivo e modificare il testo del messaggio SMS.

     Se il server SMTP non è stato configurato, non è possibile inviare messaggi e-mail agli utenti. Se le notifiche SMS non sono state configurate, non è possibile inviare messaggi SMS agli utenti.

7. Nella pagina **Risultato**, fare clic su **Fine** per chiudere la procedura guidata.

Al termine della procedura guidata, al dispositivo mobile dell'utente verranno inviati un collegamento e un codice QR per consentire il download di Kaspersky Endpoint Security for Android. L'utente fa clic sul collegamento o esamina il codice QR. Successivamente, il sistema operativo del dispositivo mobile richiede all'utente di accettare l'installazione di Kaspersky Endpoint Security for Android. Dopo il download e l'installazione di Kaspersky Endpoint Security for Android, il dispositivo mobile si connette ad Administration Server e scarica un certificato condiviso. Dopo l'installazione del certificato nel dispositivo mobile, il dispositivo verrà visualizzato nella cartella **Dispositivi mobili**, una sottocartella di **Mobile Device Management** nella struttura della console.

Aggiunta di un dispositivo mobile Android tramite un collegamento del Server Web di Kaspersky Security Center

Per l'installazione viene utilizzato il pacchetto di installazione di Kaspersky Endpoint Security for Android pubblicato in Administration Server.

Per installare Kaspersky Endpoint Security for Android e un certificato condiviso in un dispositivo mobile utilizzando un collegamento del server Web:

1. Avviare la Connessione guidata nuovo dispositivo mobile.

2. Nella pagina **Sistema operativo** della procedura guidata selezionare **Android** come tipo di sistema operativo del dispositivo mobile.

3. Nella pagina **Metodo per installare Kaspersky Endpoint Security for Android nei dispositivi** della procedura guidata selezionare **Scarica il pacchetto di installazione dell'app da Kaspersky Security Center**.

   Nel campo sottostante selezionare un pacchetto di installazione o crearne uno nuovo facendo clic su **Nuovo**.

4. Nella pagina **Selezionare gli utenti di cui si desidera gestire i dispositivi mobili** della procedura guidata selezionare gli utenti, i gruppi di sicurezza o gruppi di sicurezza Active Directory per cui si desidera aggiungere i dispositivi mobili all'elenco dei dispositivi gestiti.

   Questo passaggio viene ignorato se la procedura guidata viene avviata selezionando **Aggiungi dispositivo mobile** nel menu di scelta rapida della cartella **Account utente**.

   Se si desidera aggiungere un nuovo account utente nell'elenco, fare clic sul pulsante **Aggiungi** e inserire le proprietà dell'account utente nella finestra visualizzata. Se si desidera modificare o esaminare le proprietà dell'account utente, selezionare l'account utente nell'elenco e fare clic sul pulsante **Proprietà**.

5. Nella pagina **Origine certificato** della procedura guidata specificare il metodo per la creazione del certificato condiviso che Administration Server utilizzerà per identificare il dispositivo mobile. È possibile specificare un certificato condiviso utilizzando una delle seguenti modalità:

   - **Emetti il certificato utilizzando gli strumenti di Administration Server**

     Selezionare questa opzione per creare un nuovo certificato tramite gli strumenti di Administration Server se non è stato creato in precedenza.

     Se questa opzione è selezionata, il certificato viene rilasciato automaticamente utilizzando gli strumenti di Administration Server.

     Questa opzione è selezionata per impostazione predefinita.

   - **Specifica un file di certificato**

     Selezionare questa opzione per specificare un file di certificato creato in precedenza.

     Questo metodo non è disponibile se sono stati selezionati più utenti nel passaggio precedente.

6. Nella pagina **Metodo di notifica all'utente** della procedura guidata definire le impostazioni per la notifica all'utente del dispositivo mobile tramite SMS o e-mail relativa alla creazione del certificato:

   - **Mostra codice QR nella procedura guidata**

     Se si seleziona questa opzione, verrà visualizzato un collegamento al pacchetto di installazione nel passaggio finale della Connessione guidata nuovo dispositivo.

     Questa opzione non è disponibile se sono stati selezionati più utenti per la connessione del dispositivo.

   - **Invia codice QR all'utente**

     Questa opzione consente di configurare la notifica per l'utente della connessione di un nuovo dispositivo mobile.

     È possibile selezionare il tipo di indirizzo e-mail, specificare un indirizzo e-mail aggiuntivo e modificare il testo del messaggio. È anche possibile selezionare il tipo di telefono dell'utente per l'invio di un messaggio SMS, specificare un numero di telefono aggiuntivo e modificare il testo del messaggio SMS.

     Se il server SMTP non è stato configurato, non è possibile inviare messaggi e-mail agli utenti. Se le notifiche SMS non sono state configurate, non è possibile inviare messaggi SMS agli utenti.

7. Nella pagina **Risultato**, fare clic su **Fine** per chiudere la procedura guidata.

   Il pacchetto applicazioni mobili di Kaspersky Endpoint Security for Android verrà pubblicato automaticamente nel Server Web di Kaspersky Security Center. Il pacchetto applicazioni mobili contiene l'app, le impostazioni per la connessione del dispositivo mobile ad Administration Server e un certificato. L'utente del dispositivo mobile riceverà una notifica contenente un collegamento per scaricare il pacchetto dal server Web. L'utente fa clic sul collegamento. Il sistema operativo del dispositivo richiede all'utente di accettare l'installazione del pacchetto applicazioni mobili. Se l'utente accetta, il pacchetto verrà scaricato nel dispositivo mobile. Dopo aver scaricato il pacchetto e aver sincronizzato il dispositivo mobile con Administration Server, il dispositivo verrà visualizzato nella cartella **Dispositivi mobili**, una sottocartella di **Mobile Device Management** nella struttura della console.

Gestione dei dispositivi MDM iOS

In questa sezione vengono descritte le funzionalità avanzate per la gestione dei dispositivi MDM iOS tramite Kaspersky Security Center. L'applicazione supporta le seguenti funzionalità per la gestione dei dispositivi MDM iOS:

- Definire le impostazioni dei dispositivi MDM iOS gestiti in modalità centralizzata e limitare le funzionalità dei dispositivi attraverso i profili di configurazione. È possibile aggiungere o modificare i profili di configurazione e installarli nei dispositivi mobili.
- Installare app nei dispositivi mobili tramite profili di provisioning, anziché dall'App Store. È ad esempio possibile utilizzare profili di provisioning per l'installazione di app aziendali interne nei dispositivi mobili degli utenti. Un profilo di provisioning contiene informazioni su un'app e un dispositivo mobile.
- Installare app in un dispositivo MDM iOS tramite l'App Store. Prima di installare un'app in un dispositivo MDM iOS, è necessario aggiungere l'app a un server MDM iOS.

Ogni 24 ore viene inviata una notifica push a tutti i dispositivi MDM iOS connessi per la sincronizzazione dei dati con il server per dispositivi mobili MDM iOS.

Per informazioni sul profilo di configurazione e sul profilo di provisioning, nonché sulle app installate in un dispositivo MDM iOS, fare riferimento alla finestra delle proprietà del dispositivo.

Firma di un profilo MDM iOS tramite un certificato

È possibile firmare un profilo MDM iOS tramite un certificato. È possibile utilizzare un certificato rilasciato personalmente oppure ricevere un certificato da autorità di certificazione attendibili.

I dispositivi iOS visualizzano una dichiarazione di non responsabilità per i profili non firmati e chiedono all'utente di considerare attendibile il firmatario durante l'installazione del profilo.

Per firmare un profilo MDM iOS tramite un certificato:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.
2. Dal menu di scelta rapida della cartella **Dispositivi mobili** selezionare **Proprietà**.
3. Nella finestra delle proprietà della cartella selezionare la sezione **Impostazioni di connessione per i dispositivi iOS**.
4. Fare clic sul pulsante **Sfoglia** nel campo **Selezionare un file di certificato**.

   Finestra **Certificato**.
5. Nel campo **Tipo di certificato** specificare il tipo di certificato, pubblico o privato:
   - Se è selezionato il valore **Contenitore PKCS #12**, specificare il file di certificato e la password.
   - Se è selezionato il valore **Certificato X.509**:
     a. Specificare il file della chiave privata (con l'estensione *.prk o *.pem).
     b. Specificare la password della chiave privata.
     c. Specificare il file della chiave pubblica (con l'estensione * cer).
6. Fare clic su **OK**.

Il profilo MDM iOS viene firmato tramite un certificato.

Aggiunta di un profilo di configurazione

Per creare un profilo di configurazione, è possibile utilizzare Apple Configurator 2, disponibile sul sito Web di Apple Inc. Apple Configurator 2 funziona solo nei dispositivi che eseguono macOS; se non si dispone di tali dispositivi, è invece possibile utilizzare l'utilità di configurazione iPhone nel dispositivo con Administration Console. Tuttavia, Apple Inc. non supporta più l'utilità di configurazione iPhone.

Per creare un profilo di configurazione utilizzando l'utilità di configurazione iPhone e aggiungerlo a un server per dispositivi mobili MDM iOS:

1. Nella struttura della console selezionare la cartella **Mobile Device Management**.
2. Nell'area di lavoro della cartella **Mobile Device Management** selezionare la sottocartella **Server per dispositivi mobili**.
3. Nell'area di lavoro della cartella **Server per dispositivi mobili** selezionare un server per dispositivi mobili MDM iOS.
4. Nel menu di scelta rapida del server per dispositivi mobili MDM iOS selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del server per dispositivi mobili.
5. Nella finestra delle proprietà del server per dispositivi mobili MDM iOS selezionare la sezione **Profili di configurazione**.
6. Nella sezione **Profili di configurazione** fare clic sul pulsante **Crea**.

   Verrà visualizzata la finestra **Nuovo profilo di configurazione**.
7. Nella finestra **Nuovo profilo di configurazione** specificare un nome e un ID per il profilo.

   L'ID del profilo di configurazione deve essere univoco. Il valore deve essere specificato nel formato Reverse-DNS, ad esempio *com.nomeazienda.identificatore*.
8. Fare clic su **OK**.

   L'utilità di configurazione iPhone quindi si avvia se è stata eseguita l'installazione.
9. Riconfigurare il profilo nell'utilità di configurazione iPhone.

   Per una descrizione delle impostazioni del profilo e le istruzioni su come configurare il profilo, fare riferimento alla documentazione inclusa nell'utilità di configurazione iPhone.

Dopo aver configurato il profilo con l'utilità di configurazione iPhone, il nuovo profilo di configurazione viene visualizzato nella sezione **Profili di configurazione** nella finestra delle proprietà del server per dispositivi mobili MDM iOS.

È possibile fare clic sul pulsante **Modifica** per modificare il profilo di configurazione.

È possibile fare clic sul pulsante **Importa** per caricare il profilo di configurazione in un programma.

È possibile fare clic sul pulsante **Esporta** per salvare il profilo di configurazione in un file.

Il profilo creato deve essere installato nei dispositivi MDM iOS.

Installazione di un profilo di configurazione in un dispositivo

Per installare un profilo di configurazione in un dispositivo mobile:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

2. Nell'area di lavoro filtrare i dispositivi MDM iOS in base al tipo di protocollo (*MDM iOS*).

3. Selezionare il dispositivo mobile dell'utente in cui è necessario installare un profilo di configurazione.

   È possibile selezionare più dispositivi mobili per installare il profilo contemporaneamente.

4. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

5. Nella finestra **Comandi per Mobile Device Management** passare alla sezione **Installa profilo** e fare clic sul pulsante **Invia comando**.

   È anche possibile inviare il comando al dispositivo mobile selezionando **Tutti i comandi** nel menu di scelta rapida del dispositivo mobile, quindi **Installa profilo**.

   Verrà visualizzata la finestra **Seleziona profili** con un elenco di profili. Selezionare dall'elenco il profilo da installare nel dispositivo mobile. È possibile selezionare più profili da installare nel dispositivo mobile contemporaneamente. Per selezionare un intervallo di profili, utilizzare il tasto **MAIUSC**. Per combinare più profili in un gruppo, utilizzare il tasto **CTRL**.

6. Fare clic su **OK** per inviare il comando al dispositivo mobile.

   Quando il comando viene eseguito, il profilo di configurazione selezionato verrà installato nel dispositivo mobile dell'utente. Se il comando viene eseguito, lo stato corrente del comando nel log dei comandi verrà visualizzato come *Fine*.

   È possibile fare clic sul pulsante **Rinvia** per inviare nuovamente il comando al dispositivo mobile dell'utente.

   È possibile fare clic sul pulsante **Rimuovi dalla coda** per annullare l'esecuzione di un comando inviato se il comando non è ancora stato eseguito.

   Nella sezione **Log dei comandi** vengono visualizzati i comandi che sono stati inviati al dispositivo mobile, con i rispettivi stati di esecuzione. Fare clic su **Aggiorna** per aggiornare l'elenco dei comandi.

7. Fare clic su **OK** per chiudere la finestra **Comandi per Mobile Device Management**.

È possibile visualizzare il profilo installato e rimuoverlo, se necessario.

Rimozione del profilo di configurazione da un dispositivo

Per rimuovere un profilo di configurazione da un dispositivo mobile:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

2. Nell'area di lavoro filtrare i dispositivi MDM iOS facendo clic sul collegamento **MDM iOS**.

3. Selezionare il dispositivo mobile dell'utente da cui è necessario rimuovere il profilo di configurazione.

   È possibile selezionare più dispositivi mobili per rimuovere il profilo contemporaneamente.

4. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

5. Nella finestra **Comandi per Mobile Device Management** passare alla sezione **Rimuovi profilo** e fare clic sul pulsante **Invia comando**.

   È anche possibile inviare il comando al dispositivo mobile selezionando **Tutti i comandi** nel menu di scelta rapida del dispositivo, quindi **Rimuovi profilo**.

   Verrà visualizzata la finestra **Rimuovi profili** con un elenco di profili.

6. Selezionare dall'elenco il profilo che si desidera rimuovere dal dispositivo mobile. È possibile selezionare più profili da rimuovere dal dispositivo mobile contemporaneamente. Per selezionare un intervallo di profili, utilizzare il tasto **MAIUSC**. Per combinare più profili in un gruppo, utilizzare il tasto **CTRL**.

7. Fare clic su **OK** per inviare il comando al dispositivo mobile.

   Quando il comando viene eseguito, il profilo di configurazione selezionato verrà rimosso dal dispositivo mobile dell'utente. Se il comando viene eseguito, lo stato corrente del comando verrà visualizzato come *Completato*.

   È possibile fare clic sul pulsante **Rinvia** per inviare nuovamente il comando al dispositivo mobile dell'utente.

   È possibile fare clic sul pulsante **Rimuovi dalla coda** per annullare l'esecuzione di un comando inviato se il comando non è ancora stato eseguito.

   Nella sezione **Log dei comandi** vengono visualizzati i comandi che sono stati inviati al dispositivo mobile, con i rispettivi stati di esecuzione. Fare clic su **Aggiorna** per aggiornare l'elenco dei comandi.

8. Fare clic su **OK** per chiudere la finestra **Comandi per Mobile Device Management**.

Aggiunta di un nuovo dispositivo tramite la pubblicazione di un collegamento a un profilo

In Administration Console, l'amministratore crea un nuovo profilo MDM iOS utilizzando l'Installazione guidata certificato. La procedura guidata esegue le seguenti operazioni:

- Il profilo MDM iOS viene automaticamente pubblicato sul server Web.
- All'utente viene inviato un collegamento al profilo MDM iOS tramite SMS o via e-mail. Dopo ricezione del collegamento, l'utente installa il profilo MDM iOS nel dispositivo mobile.
- Il dispositivo mobile si connette al server MDM iOS.

A causa di un criterio di protezione più rigoroso introdotto da Apple, è necessario configurare le versioni del protocollo TLS 1.1 e TLS 1.2 durante la connessione di un dispositivo mobile che esegue iOS 11 a un Administration Server in cui è abilitata l'integrazione con l'infrastruttura a chiave pubblica (PKI).

Aggiunta di un nuovo dispositivo tramite l'installazione del profilo da parte dell'amministratore

Per connettere un dispositivo mobile a un server MDM iOS installando un profilo MDM iOS nel dispositivo mobile, l'amministratore deve eseguire le seguenti operazioni:

1. In Administration Console, aprire l'Installazione guidata certificato.

2. Creare un nuovo profilo MDM iOS selezionando la casella di controllo **Mostra certificato al termine della procedura guidata** completes nella finestra della procedura guidata.

3. Salvare il profilo MDM iOS.
4. Installare il profilo MDM iOS nel dispositivo mobile dell'utente tramite l'utilità Apple Configurator.

   Il dispositivo mobile si connette al server MDM iOS.

A causa di un criterio di protezione più rigoroso introdotto da Apple, è necessario configurare le versioni del protocollo TLS 1.1 e TLS 1.2 durante la connessione di un dispositivo mobile che esegue iOS 11 a un Administration Server in cui è abilitata l'integrazione con l'infrastruttura a chiave pubblica (PKI).

Aggiunta di un profilo di provisioning

Per aggiungere un profilo di provisioning a un server MDM iOS:

1. Nella struttura della console aprire la cartella **Mobile Device Management**.
2. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Server per dispositivi mobili**.
3. Nell'area di lavoro della cartella **Server per dispositivi mobili** selezionare un server per dispositivi mobili MDM iOS.
4. Nel menu di scelta rapida del server per dispositivi mobili MDM iOS selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del server per dispositivi mobili.
5. Nella finestra delle proprietà del **server per dispositivi mobili MDM iOS** passare alla sezione **Profili di provisioning**.
6. Nella sezione **Profili di provisioning** fare clic sul pulsante **Importa** e specificare il percorso del file di un profilo di provisioning.

   Il profilo verrà aggiunto alle impostazioni del server MDM iOS.

   È possibile fare clic sul pulsante **Esporta** per salvare il profilo di provisioning in un file.

È possibile installare il profilo di provisioning importato nei dispositivi MDM iOS.

Installazione di un profilo di provisioning in un dispositivo

Per installare un profilo di provisioning in un dispositivo mobile:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.
2. Nell'area di lavoro filtrare i dispositivi MDM iOS in base al tipo di protocollo (*MDM iOS*).
3. Selezionare il dispositivo mobile dell'utente in cui è necessario installare il profilo di provisioning.

   È possibile selezionare più dispositivi mobili per installare il profilo di provisioning contemporaneamente.

4. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

5. Nella finestra **Comandi per Mobile Device Management** passare alla sezione **Installa profilo di provisioning** e fare clic sul pulsante **Invia comando**.

   È anche possibile inviare il comando al dispositivo mobile selezionando **Tutti i comandi** dal menu di scelta rapida del dispositivo mobile, quindi **Installa profilo di provisioning**.

   Verrà visualizzata la finestra **Seleziona profili di provisioning** con un elenco di profili di provisioning. Selezionare dall'elenco il profilo di provisioning che si desidera installare nel dispositivo mobile. È possibile selezionare più profili di provisioning da installare nel dispositivo mobile contemporaneamente. Per selezionare un intervallo di profili di provisioning, utilizzare il tasto **MAIUSC**. Per combinare più profili di provisioning in un gruppo, utilizzare il tasto **CTRL**.

6. Fare clic su **OK** per inviare il comando al dispositivo mobile.

   Quando il comando viene eseguito, il profilo di provisioning selezionato verrà installato nel dispositivo mobile dell'utente. Se il comando viene eseguito, lo stato corrente nel log dei comandi viene visualizzato come *Completato*.

   È possibile fare clic sul pulsante **Rinvia** per inviare nuovamente il comando al dispositivo mobile dell'utente.

   È possibile fare clic sul pulsante **Rimuovi dalla coda** per annullare l'esecuzione di un comando inviato se il comando non è ancora stato eseguito.

   Nella sezione **Log dei comandi** vengono visualizzati i comandi che sono stati inviati al dispositivo mobile, con i rispettivi stati di esecuzione. Fare clic su **Aggiorna** per aggiornare l'elenco dei comandi.

7. Fare clic su **OK** per chiudere la finestra **Comandi per Mobile Device Management**.

È possibile visualizzare il profilo installato e rimuoverlo, se necessario.

Rimozione di un profilo di provisioning da un dispositivo

Per rimuovere un profilo di provisioning da un dispositivo mobile:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

2. Nell'area di lavoro filtrare i dispositivi MDM iOS in base al tipo di protocollo (*MDM iOS*).

3. Selezionare il dispositivo mobile dell'utente da cui è necessario rimuovere il profilo di provisioning.

   È possibile selezionare più dispositivi mobili per rimuovere il profilo di provisioning contemporaneamente.

4. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

5. Nella finestra **Comandi per Mobile Device Management** passare alla sezione **Rimuovi profilo di provisioning** e fare clic sul pulsante **Invia comando**.

   È anche possibile inviare il comando al dispositivo mobile selezionando **Tutti i comandi** dal menu di scelta rapida, quindi **Rimuovi profilo di provisioning**.

   Verrà visualizzata la finestra **Rimuovi profili di provisioning** con un elenco di profili.

6. Selezionare dall'elenco il profilo di provisioning che si desidera rimuovere dal dispositivo mobile. È possibile selezionare più profili di provisioning da rimuovere dal dispositivo mobile contemporaneamente. Per selezionare un intervallo di profili di provisioning, utilizzare il tasto **MAIUSC**. Per combinare più profili di provisioning in un gruppo, utilizzare il tasto **CTRL**.

7. Fare clic su **OK** per inviare il comando al dispositivo mobile.

   Quando il comando viene eseguito, il profilo di provisioning selezionato verrà rimosso dal dispositivo mobile dell'utente. Le applicazioni correlate al profilo di provisioning eliminato non potranno più essere utilizzate. Se il comando viene eseguito, lo stato corrente del comando verrà visualizzato come *Completato*.

   È possibile fare clic sul pulsante **Rinvia** per inviare nuovamente il comando al dispositivo mobile dell'utente.

   È possibile fare clic sul pulsante **Rimuovi dalla coda** per annullare l'esecuzione di un comando inviato se il comando non è ancora stato eseguito.

   Nella sezione **Log dei comandi** vengono visualizzati i comandi che sono stati inviati al dispositivo mobile, con i rispettivi stati di esecuzione. Fare clic su **Aggiorna** per aggiornare l'elenco dei comandi.

8. Fare clic su **OK** per chiudere la finestra **Comandi per Mobile Device Management**.

Aggiunta di un'applicazione gestita

Prima di installare un'app in un dispositivo MDM iOS, è necessario aggiungere l'app a un server MDM iOS. Un'applicazione viene considerata gestita se è stata installata in un dispositivo tramite Kaspersky Security Center. Un'applicazione gestita può essere gestita in remoto tramite Kaspersky Security Center.

Per aggiungere un'applicazione gestita a un server MDM iOS:

1. Nella struttura della console aprire la cartella **Mobile Device Management**.
2. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Server per dispositivi mobili**.
3. Nell'area di lavoro della cartella **Server per dispositivi mobili** selezionare un server per dispositivi mobili MDM iOS.
4. Nel menu di scelta rapida del server per dispositivi mobili MDM iOS selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del server MDM iOS.
5. Nella finestra delle proprietà del server per dispositivi mobili MDM iOS selezionare la sezione **Applicazioni gestite**.
6. Fare clic sul pulsante **Aggiungi** nella sezione **Applicazioni gestite**.

   Verrà visualizzata la finestra **Aggiungi applicazione**.
7. Nella finestra **Aggiungi applicazione**, nel campo **Nome app**, specificare il nome dell'applicazione da aggiungere.
8. Nel campo **ID Apple o collegamento al file manifesto** specificare l'ID Apple dell'applicazione da aggiungere oppure specificare un collegamento a un file manifesto utilizzabile per scaricare l'applicazione.
9. Se si desidera che un'applicazione gestita venga rimossa dal dispositivo mobile dell'utente durante la rimozione del profilo MDM IOS, selezionare la casella di controllo **Rimuovi insieme al profilo MDM iOS**.
10. Se si desidera bloccare il backup dei dati dell'applicazione tramite iTunes, selezionare la casella di controllo **Blocca il backup dei dati**.
11. Fare clic su **OK**.

L'applicazione aggiunta verrà visualizzata nella sezione **Applicazioni gestite** della finestra delle proprietà del server per dispositivi mobili MDM iOS.

Installazione di un'app in un dispositivo mobile

Per installare un'app in un dispositivo mobile MDM iOS:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

2. Selezionare il dispositivo MDM iOS in cui si desidera installare un'app.

   È possibile selezionare più dispositivi mobili in cui installare contemporaneamente l'applicazione.

3. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

4. Nella finestra **Comandi per Mobile Device Management** passare alla sezione **Installa app** e fare clic sul pulsante **Invia comando**.

   È anche possibile inviare il comando al dispositivo mobile selezionando **Tutti i comandi** dal menu di scelta rapida del dispositivo mobile, quindi **Installa app**.

   Verrà visualizzata la finestra **Seleziona app** con un elenco di profili. Selezionare dall'elenco l'applicazione da installare nel dispositivo mobile. È possibile selezionare più applicazioni per installarle contemporaneamente nel dispositivo mobile. Per selezionare un intervallo di app, utilizzare il tasto **MAIUSC**. Per combinare più app in un gruppo, utilizzare il tasto **CTRL**.

5. Fare clic su **OK** per inviare il comando al dispositivo mobile.

   Quando il comando viene eseguito, l'applicazione selezionata verrà installata nel dispositivo mobile dell'utente. Se il comando viene eseguito, lo stato corrente nel log dei comandi verrà visualizzato come *Completato*.

   È possibile fare clic sul pulsante **Rinvia** per inviare nuovamente il comando al dispositivo mobile dell'utente. È possibile fare clic sul pulsante **Rimuovi dalla coda** per annullare l'esecuzione di un comando inviato se il comando non è ancora stato eseguito.

   Nella sezione **Log dei comandi** vengono visualizzati i comandi che sono stati inviati al dispositivo mobile, con i rispettivi stati di esecuzione. Fare clic su **Aggiorna** per aggiornare l'elenco dei comandi.

6. Fare clic su **OK** per chiudere la finestra **Comandi per Mobile Device Management**.

Le informazioni sull'applicazione installata sono visualizzate nelle proprietà del dispositivo mobile MDM iOS. È possibile rimuovere l'applicazione dal dispositivo mobile utilizzando il log dei comandi o il menu di scelta rapida del dispositivo mobile.

Rimozione di un'app da un dispositivo

Per rimuovere un'app da un dispositivo mobile:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

2. Nell'area di lavoro filtrare i dispositivi MDM iOS in base al tipo di protocollo (*MDM iOS*).

3. Selezionare il dispositivo mobile dell'utente da cui è necessario rimuovere l'app.

   È possibile selezionare più dispositivi mobili da cui rimuovere l'app contemporaneamente.

4. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

5. Nella finestra **Comandi per Mobile Device Management** passare alla sezione **Rimuovi app** e fare clic sul pulsante **Invia comando**.

   È anche possibile inviare il comando al dispositivo mobile selezionando **Tutti i comandi** dal menu di scelta rapida del dispositivo mobile, quindi **Rimuovi app**.

   Verrà visualizzata la finestra **Rimuovi app** con un elenco di applicazioni.

6. Selezionare dall'elenco l'app che si desidera rimuovere dal dispositivo mobile. È possibile selezionare più app per rimuoverle contemporaneamente. Per selezionare un intervallo di app, utilizzare il tasto **MAIUSC**. Per combinare più app in un gruppo, utilizzare il tasto **CTRL**.

7. Fare clic su **OK** per inviare il comando al dispositivo mobile.

   Quando il comando viene eseguito, l'app selezionata verrà rimossa dal dispositivo mobile dell'utente. Se il comando viene eseguito, lo stato corrente del comando verrà visualizzato come *Completato*.

   È possibile fare clic sul pulsante **Rinvia** per inviare nuovamente il comando al dispositivo mobile dell'utente.

   È possibile fare clic sul pulsante **Rimuovi dalla coda** per annullare l'esecuzione di un comando inviato se il comando non è ancora stato eseguito.

   Nella sezione **Log dei comandi** vengono visualizzati i comandi che sono stati inviati al dispositivo mobile, con i rispettivi stati di esecuzione. Fare clic su **Aggiorna** per aggiornare l'elenco dei comandi.

8. Fare clic su **OK** per chiudere la finestra **Comandi per Mobile Device Management**.

Configurazione del roaming in un dispositivo mobile MDM iOS

Per configurare il roaming:

1. Nella struttura della console aprire la cartella **Mobile Device Management**.

2. Nella cartella **Mobile Device Management** selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

3. Selezionare il dispositivo MDM iOS di proprietà dell'utente per cui è necessario configurare il roaming.

   È possibile selezionare più dispositivi mobili per configurarvi contemporaneamente il roaming.

4. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

5. Nella finestra **Comandi per Mobile Device Management** passare alla sezione **Configura roaming** e fare clic sul pulsante **Invia comando**.

   È inoltre possibile inviare il comando al dispositivo mobile selezionando **Tutti i comandi** → **Configura roaming** dal menu di scelta rapida del dispositivo.

6. Nella finestra **Impostazioni roaming** specificare le impostazioni attinenti:

   - **Abilita roaming dati**

     Se questa opzione è abilitata, il roaming dati è abilitato nel dispositivo mobile MDM iOS. L'utente del dispositivo mobile MDM iOS può esplorare Internet in modalità roaming.

     Per impostazione predefinita, questa opzione è disabilitata.

Viene configurato il roaming per i dispositivi selezionati.

Visualizzazione delle informazioni su un dispositivo MDM iOS

Per visualizzare le informazioni su un dispositivo MDM iOS:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

2. Nell'area di lavoro filtrare i dispositivi MDM iOS facendo clic sul collegamento **MDM iOS**.

3. Selezionare il dispositivo mobile di cui si desidera visualizzare le informazioni.

4. Nel menu di scelta rapida del dispositivo mobile selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del dispositivo MDM iOS.

Nella finestra delle proprietà del dispositivo mobile verranno visualizzate le informazioni sul dispositivo MDM iOS connesso.

Disconnessione di un dispositivo MDM iOS dalla gestione

Per disconnettere un dispositivo MDM iOS dal server MDM iOS:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

2. Nell'area di lavoro filtrare i dispositivi MDM iOS facendo clic sul collegamento **MDM iOS**.

3. Selezionare il dispositivo mobile da disconnettere.

4. Nel menu di scelta rapida del dispositivo mobile selezionare **Elimina**.

   Il dispositivo MDM iOS sarà contrassegnato nell'elenco per la rimozione. Il dispositivo verrà rimosso automaticamente dall'elenco dei dispositivi gestiti dopo essere stato rimosso dal database del server MDM iOS. Il dispositivo mobile sarà rimosso dal database del server MDM iOS entro un minuto.

Dopo che il dispositivo MDM iOS viene disconnesso dalla gestione, verranno rimossi dal dispositivo mobile tutti i profili di configurazione installati, il profilo MDM iOS e le applicazioni per cui è stata abilitata l'opzione **Rimuovi insieme al profilo MDM iOS**.

Invio di comandi a un dispositivo

Per inviare un comando a un dispositivo MDM iOS:

1. In Administration Console aprire il nodo **Mobile Device Management**.

2. Selezionare la cartella **Dispositivi mobili**.

3. Nella cartella **Dispositivi mobili** selezionare il dispositivo mobile a cui è necessario inviare i comandi.
4. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.
5. Nell'elenco visualizzato selezionare il comando da inviare al dispositivo mobile.

Controllo dello stato di esecuzione dei comandi inviati

Per verificare lo stato di esecuzione di un comando inviato a un dispositivo mobile:

1. In Administration Console aprire il nodo **Mobile Device Management**.
2. Selezionare la cartella **Dispositivi mobili**.
3. Nella cartella **Dispositivi mobili** selezionare il dispositivo mobile per cui è necessario verificare lo stato di esecuzione dei comandi selezionati.
4. Nel menu di scelta rapida del dispositivo mobile selezionare **Mostra log dei comandi**.

Gestione dei dispositivi KES

In Kaspersky Security Center è possibile gestire i dispositivi mobili KES nei seguenti modi:

- Gestire in modo centralizzato i dispositivi KES utilizzando specifici comandi.
- Visualizzare le informazioni sulle impostazioni per la gestione dei dispositivi KES.
- Installare applicazioni tramite i pacchetti app mobili.
- Disconnettere i dispositivi KES dalla gestione.

Creazione di un pacchetto applicazioni mobili per i dispositivi KES

Per creare un pacchetto applicazioni mobili per i dispositivi KES è richiesta una licenza Kaspersky Endpoint Security for Android.

Per creare un pacchetto applicazioni mobili:

1. Nella cartella **Installazione remota** della struttura della console selezionare la sottocartella **Pacchetti di installazione**.

   La cartella **Installazione remota** è una sottocartella della cartella **Avanzate** per impostazione predefinita.
2. Fare clic sul pulsante **Azioni aggiuntive** e selezionare **Gestisci pacchetti app mobili** nell'elenco a discesa.
3. Nella finestra **Gestione pacchetti app mobili** fare clic sul pulsante **Nuovo**.
4. Viene avviata la Creazione guidata nuovo pacchetto. Seguire le istruzioni della procedura guidata.

Il nuovo pacchetto applicazioni mobili creato è visualizzato nella finestra **Gestione pacchetti app mobili**.

Abilitazione dell'autenticazione basata su certificato dei dispositivi KES

Per abilitare l'autenticazione basata su certificato di un dispositivo KES:

1. Aprire il Registro di sistema del dispositivo client in cui è installato Administration Server (ad esempio in locale, utilizzando il comando regedit nel menu **Start** → **Esegui**).
2. Passare al seguente hive:
   - Per i sistemi a 32 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Per i sistemi a 64 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Creare una chiave con il nome LP_MobileMustUseTwoWayAuthOnPort13292.
4. Specificare REG_DWORD come tipo di chiave.
5. Impostare il valore della chiave su 1.
6. Riavviare il servizio Administration Server.

L'autenticazione basata su certificato obbligatoria del dispositivo KES tramite un certificato condiviso verrà abilitata dopo l'esecuzione del servizio Administration Server.

La prima connessione del dispositivo KES all'Administration Server non richiede un certificato.

Per impostazione predefinita, l'autenticazione basata su certificato dei dispositivi KES è disabilitata.

Visualizzazione delle informazioni su un dispositivo KES

Per visualizzare le informazioni su un dispositivo KES:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.
2. Nell'area di lavoro filtrare i dispositivi KES in base al tipo di protocollo (*KES*).
3. Selezionare il dispositivo mobile di cui si desidera visualizzare le informazioni.
4. Nel menu di scelta rapida del dispositivo mobile selezionare **Proprietà**.

Verrà visualizzata la finestra delle proprietà del dispositivo KES.

Nella finestra delle proprietà del dispositivo mobile verranno visualizzate le informazioni sul dispositivo KES connesso.

Disconnessione di un dispositivo KES dalla gestione

Per disconnettere un dispositivo KES dalla gestione, l'utente deve rimuovere Network Agent dal dispositivo mobile. Dopo che l'utente ha rimosso Network Agent, i dettagli del dispositivo mobile vengono rimossi dal database di Administration Server e l'amministratore può rimuovere il dispositivo mobile dall'elenco dei dispositivi gestiti.

Per rimuovere un dispositivo KES dall'elenco dei dispositivi gestiti:

1. Nella cartella **Mobile Device Management** della struttura della console selezionare la sottocartella **Dispositivi mobili**.

   Nell'area di lavoro della cartella è visualizzato un elenco dei dispositivi mobili gestiti.

2. Nell'area di lavoro filtrare i dispositivi KES in base al tipo di protocollo (*KES*).

3. Selezionare il dispositivo mobile da disconnettere dalla gestione.

4. Nel menu di scelta rapida del dispositivo mobile selezionare **Elimina**.

Il dispositivo mobile viene rimosso dall'elenco dei dispositivi gestiti.

Se Kaspersky Endpoint Security for Android non è stato rimosso dal dispositivo mobile, quest'ultimo sarà nuovamente visualizzato nell'elenco dei dispositivi gestiti dopo la sincronizzazione con Administration Server.

Criptaggio e protezione dei dati

Il criptaggio dei dati riduce il rischio di divulgazione accidentale in caso di furto o smarrimento di un portatile, un'unità rimovibile o un disco rigido oppure qualora venga eseguito l'accesso ai dati da parte di utenti e applicazioni non autorizzati.

Kaspersky Endpoint Security for Windows offre funzionalità di criptaggio. Kaspersky Endpoint Security for Windows consente il criptaggio dei file archiviati nelle unità locali dei dispositivi e nelle unità rimovibili, oltre al criptaggio di interi dischi rigidi e unità rimovibili.

Le regole di criptaggio sono configurate utilizzando Kaspersky Security Center, tramite i criteri. Il criptaggio e il decriptaggio in base alle regole specificate vengono eseguiti al momento dell'applicazione di un criterio.

La disponibilità della funzionalità di gestione del criptaggio è determinata dalle impostazioni dell'interfaccia utente.

L'amministratore può eseguire le seguenti azioni:

- Configurare ed eseguire il criptaggio o decriptaggio dei file nelle unità locali del dispositivo.
- Configurare ed eseguire il criptaggio dei file nelle unità rimovibili.
- Creare regole per l'accesso ai file criptati da parte delle applicazioni.

- Creare e inviare all'utente un file chiave per l'accesso ai file criptati, se il criptaggio dei file è limitato nel dispositivo dell'utente.
- Configurare ed eseguire il criptaggio del disco rigido.
- Gestire l'accesso dell'utente alle unità rimovibili e ai dischi rigidi criptati (gestire gli account per l'Agente di Autenticazione, creare e inviare informazioni agli utenti su richiesta per il ripristino di nome e password dell'account, oltre a chiavi di accesso per i dispositivi criptati).
- Visualizzare gli stati di criptaggio e i rapporti sul criptaggio dei file.

Queste operazioni vengono eseguite utilizzando strumenti integrati in Kaspersky Endpoint Security for Windows. Per istruzioni dettagliate sull'esecuzione delle operazioni e una descrizione delle funzionalità di criptaggio, consultare la Guida in linea di Kaspersky Endpoint Security for Windows.

Kaspersky Security Center supporta la funzionalità di gestione del criptaggio per i dispositivi che eseguono sistemi operativi macOS. Il criptaggio viene configurato utilizzando gli strumenti di Kaspersky Endpoint Security for Mac per le versioni delle applicazioni che supportano la funzionalità di criptaggio. Per istruzioni dettagliate sull'esecuzione delle operazioni e una descrizione delle funzionalità di criptaggio, consultare la *Guida per l'amministratore di Kaspersky Endpoint Security for Mac*.

Visualizzazione dell'elenco dei dispositivi criptati

Per visualizzare l'elenco dei dispositivi che contengono informazioni criptate:

1. Nella struttura della console di Administration Server selezionare la cartella **Criptaggio e protezione dei dati**.
2. Aprire l'elenco dei dispositivi criptati con uno dei seguenti metodi:
   - Facendo clic sul collegamento **Vai all'elenco delle unità criptate** nella sezione **Gestisci unità criptate**.
   - Selezionando la cartella **Unità criptate** nella struttura della console.

Nell'area di lavoro vengono visualizzate le informazioni sui dispositivi in rete che contengono file criptati e sui dispositivi criptati a livello di unità. Una volta decriptate le informazioni in un dispositivo, il dispositivo viene automaticamente rimosso dall'elenco.

È possibile ordinare le informazioni nell'elenco dei dispositivi, in ordine crescente o decrescente in ogni colonna.

> Le impostazioni dell'interfaccia utente determinano se la cartella **Criptaggio e protezione dei dati** appare nella struttura della console.

Visualizzazione dell'elenco degli eventi di criptaggio

Durante l'esecuzione delle attività di criptaggio o decriptaggio dei dati nei dispositivi, Kaspersky Endpoint Security for Windows invia a Kaspersky Security Center informazioni sui seguenti tipi di eventi:

- Impossibile criptare o decriptare un file o creare un archivio criptato perché lo spazio sul disco rigido non è sufficiente.
- Impossibile criptare o decriptare un file o creare un archivio criptato a causa dei problemi di licenza.

- Impossibile criptare o decriptare un file o creare un archivio criptato a causa di diritti di accesso insufficienti.
- All'applicazione è stato negato l'accesso a un file criptato.
- Errori sconosciuti.

Per visualizzare un elenco degli eventi che si sono verificati durante il criptaggio dei dati nei dispositivi:

1. Nella struttura della console di Administration Server selezionare la cartella **Criptaggio e protezione dei dati**.
2. Aprire l'elenco degli eventi che si sono verificati durante il criptaggio con uno dei seguenti metodi:
   - Facendo clic sul collegamento **Vai all'elenco degli errori** nella sezione **Errori di criptaggio dei dati**.
   - Selezionando la cartella **Unità criptate** nella struttura della console.

Nell'area di lavoro verranno visualizzate le informazioni sui problemi che si sono verificati durante il criptaggio dei dati nei dispositivi.

È possibile eseguire le seguenti operazioni sull'elenco degli eventi di criptaggio:

- Ordinare i record di dati in ordine crescente o decrescente in qualsiasi colonna.
- Eseguire una ricerca rapida dei record (in base alla corrispondenza del testo con una sottostringa in qualsiasi campo dell'elenco).
- Esportare l'elenco degli eventi in un file di testo.

Le impostazioni dell'interfaccia utente determinano se la cartella **Criptaggio e protezione dei dati** appare nella struttura della console.

Esportazione dell'elenco degli eventi di criptaggio in un file di testo

Per esportare l'elenco degli eventi di criptaggio in un file di testo:

1. Creare un elenco di eventi di criptaggio.
2. Dal menu di scelta rapida dell'elenco di eventi selezionare **Esporta elenco**.

   Verrà visualizzata la finestra **Esporta elenco**.
3. Nella finestra **Esporta elenco** specificare il nome del file di testo con l'elenco degli eventi, selezionare una cartella in cui salvarlo e fare clic sul pulsante **Salva**.

   L'elenco degli eventi di criptaggio verrà salvato nel file specificato.

Creazione e visualizzazione di rapporti sul criptaggio

È possibile generare i seguenti rapporti:

- Rapporto sullo stato di criptaggio dei dispositivi gestiti. Questo rapporto include informazioni dettagliate sul criptaggio dei dati di vari dispositivi gestiti. Il rapporto mostra ad esempio il numero di dispositivi a cui si applica il criterio con regole di criptaggio configurate. È inoltre possibile scoprire, ad esempio, quanti dispositivi devono essere riavviati. Il rapporto contiene inoltre le informazioni sulla tecnologia di criptaggio e sull'algoritmo di ogni dispositivo.

- Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa. Questo rapporto contiene informazioni simili a quelle del rapporto sullo stato di criptaggio dei dispositivi gestiti, ma fornisce solo i dati relativi a dispositivi di archiviazione di massa e unità rimovibili.

- Rapporto sui diritti di accesso alle unità criptate. Questo rapporto mostra quali account utente hanno accesso alle unità criptate.

- Rapporto sugli errori di criptaggio dei file. Questo rapporto contiene informazioni sugli errori che si sono verificati durante l'esecuzione delle attività di criptaggio o decriptaggio dei dati nei dispositivi.

- Rapporto sul blocco dell'accesso ai file criptati. Questo rapporto contiene informazioni sul blocco dell'accesso delle applicazioni ai file criptati. Questo rapporto è utile se un utente o un'applicazione non autorizzati tentano di accedere a unità o file criptati.

Per generare il rapporto sul criptaggio dei dispositivi:

1. Nella struttura della console selezionare la cartella **Criptaggio e protezione dei dati**.

2. Eseguire una delle seguenti operazioni:

   - Per generare il rapporto sullo stato di criptaggio dei dispositivi gestiti, fare clic sul collegamento **Visualizza rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa**.

     Se questo rapporto non è ancora stato configurato, verrà avviata la Creazione guidata nuovo modello di rapporto. Seguire le istruzioni della procedura guidata.

   - Per generare il rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa, nella struttura della console selezionare la sottocartella **Unità criptate**, quindi fare clic sul pulsante **Visualizza rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa**.

Verrà avviata la generazione del rapporto. Il rapporto verrà visualizzato nella scheda **Rapporti** nel nodo **Administration Server**.

Per generare il rapporto sui diritti di accesso ai dispositivi criptati:

1. Nella struttura della console selezionare la cartella **Criptaggio e protezione dei dati**.
2. Eseguire una delle seguenti operazioni:
   - Fare clic sul collegamento **Rapporto sui diritti di accesso alle unità criptate** nella sezione **Gestisci unità criptate** per avviare la Creazione guidata nuovo modello di rapporto.
   - Selezionare la sottocartella **Unità criptate**, quindi fare clic sul pulsante **Rapporto sui diritti di accesso alle unità criptate** per avviare la Creazione guidata nuovo modello di rapporto.
3. Attenersi ai passaggi della Creazione guidata nuovo modello di rapporto.

Verrà avviata la generazione del rapporto. Il rapporto verrà visualizzato nella scheda **Rapporti** nel nodo **Administration Server**.

Per generare il rapporto sugli errori di criptaggio dei file:

1. Nella struttura della console selezionare la cartella **Criptaggio e protezione dei dati**.
2. Eseguire una delle seguenti operazioni:
   - Fare clic sul collegamento **Visualizza il rapporto sugli errori di criptaggio dei file** nella sezione **Errori di criptaggio dei dati** per avviare la Creazione guidata nuovo modello di rapporto.
   - Selezionare la sottocartella **Eventi di criptaggio**, quindi fare clic sul collegamento **Rapporto sugli errori di criptaggio dei file** per avviare la Creazione guidata nuovo modello di rapporto.
3. Attenersi ai passaggi della Creazione guidata nuovo modello di rapporto.

Verrà avviata la generazione del rapporto. Il rapporto verrà visualizzato nella scheda **Rapporti** nel nodo **Administration Server**.

Per generare il rapporto sullo stato di criptaggio dei dispositivi gestiti:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Fare clic sul pulsante **Nuovo modello di rapporto** per avviare la Creazione guidata nuovo modello di rapporto.
4. Attenersi alle istruzioni della Creazione guidata nuovo modello di rapporto. Nella finestra **Selezione del tipo di modello di rapporto**, nella sezione **Altro** selezionare **Rapporto sullo stato di criptaggio dei dispositivi gestiti**.

   Al termine della Creazione guidata nuovo modello di rapporto, verrà visualizzato un nuovo modello di rapporto nella scheda **Rapporti** del nodo Administration Server.
5. Nella scheda **Rapporti** del nodo dell'Administration Server appropriato selezionare il modello di rapporto che è stato creato durante i passaggi precedenti.

Verrà avviata la generazione del rapporto. Il rapporto verrà visualizzato nella scheda **Rapporti** nel nodo **Administration Server**.

È inoltre possibile scoprire se gli stati di criptaggio di dispositivi e unità rimovibili soddisfano il criterio di criptaggio visualizzando i riquadri informazioni nella scheda **Statistiche** del nodo Administration Server.

Per generare il rapporto sul blocco dell'accesso ai file criptati:

1. Nella struttura della console selezionare il nodo con il nome dell'Administration Server desiderato.
2. Nell'area di lavoro del nodo selezionare la scheda **Rapporti**.
3. Fare clic sul pulsante **Nuovo modello di rapporto** per avviare la Creazione guidata nuovo modello di rapporto.
4. Attenersi alle istruzioni della Creazione guidata nuovo modello di rapporto. Nella finestra **Selezione del tipo di modello di rapporto**, nella sezione **Altro** selezionare **Rapporto sul blocco dell'accesso ai file criptati**.

   Al termine della Creazione guidata nuovo modello di rapporto, verrà visualizzato un nuovo modello di rapporto nella scheda **Reports** del nodo Rapporti.
5. Nella scheda **Rapporti** del nodo **Administration Server** selezionare il modello di rapporto che è stato creato durante i passaggi precedenti.

Verrà avviata la generazione del rapporto. Il rapporto verrà visualizzato nella scheda **Rapporti** nel nodo **Administration Server**.

Trasmissione delle chiavi di criptaggio tra Administration Server

Se la funzionalità di criptaggio dei dati è abilitata in un dispositivo gestito, la chiave di criptaggio è archiviata in Administration Server. La chiave di criptaggio viene utilizzata per accedere ai dati criptati e per gestire il criterio di criptaggio.

La chiave di criptaggio deve essere trasmessa a un altro Administration Server nei seguenti casi:

- Si riconfigura Network Agent in un dispositivo gestito per assegnare il dispositivo a un altro Administration Server. Se questo dispositivo contiene dati criptati, la chiave di criptaggio deve essere trasmessa all'Administration Server di destinazione. In caso contrario, i dati non possono essere decriptati.
- Si cripta un'unità rimovibile connessa a un dispositivo D1 gestito dall'Administration Server S1 e quindi si collega questa unità rimovibile a un dispositivo D2 gestito dall'Administration Server S2. Per accedere ai dati sull'unità rimovibile, la chiave di criptaggio deve essere trasmessa dall'Administration Server S1 all'Administration Server S2.
- Si cripta un file in un dispositivo D1 gestito dall'Administration Server S1 e quindi si tenta di accedere al file in un dispositivo D2 gestito dall'Administration Server S2. Per accedere al file, la chiave di criptaggio deve essere trasmessa dall'Administration Server S1 all'Administration Server S2.

È possibile trasmettere le chiavi di criptaggio nei seguenti modi:

- Automaticamente, abilitando l'opzione **Usa gerarchia di Administration Server per ottenere le chiavi di criptaggio** nelle proprietà di due Administration Server tra i quali deve essere trasmessa una chiave di criptaggio. Se questa opzione è disabilitata per uno degli Administration Server, la trasmissione automatica delle chiavi di criptaggio non è possibile.

  Quando si abilita l'opzione **Usa gerarchia di Administration Server per ottenere le chiavi di criptaggio** nelle proprietà di un Administration Server, Administration Server invia tutte le chiavi di criptaggio archiviate nel proprio archivio all'Administration Server primario (se disponibile) superiore di un livello nella gerarchia.

  Quando si tenta di accedere ai dati criptati, l'Administration Server cerca innanzitutto la chiave di criptaggio nel proprio archivio. Se l'opzione **Usa gerarchia di Administration Server per ottenere le chiavi di criptaggio** è abilitata e la chiave di criptaggio richiesta non è stata rilevata nell'archivio, Administration Server invia inoltre una richiesta agli Administration Server primari (se disponibili) per fornire la chiave di criptaggio richiesta. La richiesta verrà inviata a tutti gli Administration Server primari fino al server nel livello più alto della gerarchia.

L'opzione **Usa gerarchia di Administration Server per ottenere le chiavi di criptaggio** non è attualmente disponibile nell'interfaccia di Web Console. Se non si dispone dell'accesso ad Administration Console, utilizzare l'Administration Server primario per gestire i dispositivi criptati.

- Manualmente da un Administration Server a un altro esportando e importando il file contenente le chiavi di criptaggio.

  L'esportazione e l'importazione delle chiavi di criptaggio sono azioni incluse nella funzionalità di gestione delle chiavi di criptaggio. Per eseguire queste azioni, configurare i diritti di accesso alla funzionalità per gli utenti di Kaspersky Security Center come segue:

  - Concedere il diritto di accesso di **lettura** alla funzionalità di gestione delle chiavi di criptaggio per un utente che esporta le chiavi di criptaggio dall'Administration Server secondario.
  - Concedere il diritto di accesso di **scrittura** alla funzionalità di gestione delle chiavi di criptaggio per un utente che importa le chiavi di criptaggio nell'Administration Server di destinazione.

Per abilitare la trasmissione automatica delle chiavi di criptaggio tra gli Administration Server all'interno della gerarchia:

1. Nella struttura della console selezionare l'Administration Server per cui si desidera abilitare la trasmissione automatica delle chiavi di criptaggio.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà selezionare la sezione **Algoritmo di criptaggio**.
4. Abilitare l'opzione **Usa gerarchia di Administration Server per ottenere le chiavi di criptaggio**.
5. Fare clic su **OK** per applicare le modifiche.

Le chiavi di criptaggio verranno trasmesse agli Administration Server primari (se disponibili) alla successiva sincronizzazione (heartbeat). Questo Administration Server fornirà inoltre, su richiesta, una chiave di criptaggio dell'archivio a un Administration Server secondario.

Per trasmettere le chiavi di criptaggio tra gli Administration Server manualmente:

1. Nella struttura della console di Administration Server selezionare l'Administration Server secondario dal quale si desidera trasmettere le chiavi di criptaggio.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà selezionare la sezione **Algoritmo di criptaggio**.
4. Fare clic su **Esporta chiavi di criptaggio da Administration Server**.

   Assicurarsi che a un utente che esporta le chiavi di criptaggio dal server sia concesso il diritto di accesso di **lettura** alla funzionalità di gestione delle chiavi di criptaggio.
5. Nella finestra **Esporta chiavi di criptaggio**:
   - Fare clic sul pulsante **Sfoglia**, quindi specificare dove salvare il file.
   - Specificare una password per proteggere il file dall'accesso non autorizzato.

     Memorizzare la password. Non è possibile recuperare una password persa. In caso di smarrimento della password, è necessario ripetere la procedura di esportazione. Annotare quindi la password e tenerla a portata di mano.
6. Trasmettere il file a un altro Administration Server, ad esempio tramite una cartella condivisa o un'unità rimovibile.
7. Nell'Administration Server di destinazione assicurarsi che Kaspersky Security Center Administration Console sia in esecuzione.
8. Nella struttura della console di Administration Server selezionare l'Administration Server di destinazione a cui si desidera trasmettere le chiavi di criptaggio.
9. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
10. Nella finestra delle proprietà selezionare la sezione **Algoritmo di criptaggio**.
11. Fare clic su **Importa chiavi di criptaggio in Administration Server**.

    Assicurarsi che a un utente che importa le chiavi di criptaggio nel server sia concesso il diritto di accesso di **scrittura** alla funzionalità di gestione delle chiavi di criptaggio.
12. Nella finestra **Importa chiavi di criptaggio**:
    - Fare clic sul pulsante **Sfoglia**, quindi selezionare il file contenente le chiavi di criptaggio.
    - Specificare la password.
13. Fare clic su **OK**.

Le chiavi di criptaggio vengono trasmesse all'Administration Server di destinazione.

Archivi dati

Questa sezione fornisce informazioni sui dati memorizzati in Administration Server e utilizzati per il monitoraggio delle condizioni e per la manutenzione dei dispositivi client.

La cartella **Archivi** della struttura della console visualizza i dati utilizzati per tenere traccia degli stati dei dispositivi client.

La cartella **Archivi** contiene i seguenti oggetti:

- Aggiornamenti scaricati da Administration Server distribuiti ai dispositivi client
- Elenco dei dispositivi rilevati nella rete
- Chiavi di licenza rilevate nei dispositivi client
- File inseriti nelle cartelle Quarantena nei dispositivi dalle applicazioni di protezione
- File inseriti in Backup nei dispositivi client
- File di cui è stata rimandata la scansione dalle applicazioni di protezione

Esportazione di un elenco di oggetti di un archivio in un file di testo

È possibile esportare l'elenco di oggetti dall'archivio in un file di testo.

Per esportare l'elenco di oggetti dall'archivio in un file di testo:

1. Nella struttura della console selezionare la sottocartella dell'archivio desiderato nella cartella **Archivi**.
2. Nella sottocartella dell'archivio selezionare **Esporta elenco** nel menu di scelta rapida.

   Verrà visualizzata la finestra **Esporta elenco**, in cui è possibile specificare il nome del file di testo e il percorso della cartella in cui è stato inserito.

Pacchetti di installazione

Kaspersky Security Center sposta negli archivi dati i pacchetti di installazione per le applicazioni Kaspersky e di altri produttori.

Un *pacchetto di installazione* è un set di file necessari per installare un'applicazione. Un pacchetto di installazione contiene le impostazioni di installazione e la configurazione iniziale dell'applicazione da installare.

Se si desidera installare un'applicazione in un dispositivo client, creare un pacchetto di installazione per l'applicazione o utilizzarne uno esistente. L'elenco dei pacchetti di installazione disponibili è contenuto nella sottocartella **Pacchetti di installazione** della cartella **Installazione remota** della struttura della console.

Stati principali dei file nell'archivio

Le applicazioni di protezione eseguono la scansione dei file nei dispositivi alla ricerca di virus noti e altri programmi che possono costituire una minaccia, assegnano gli stati ai file e ne collocano alcuni nell'archivio.

Le applicazioni di protezione, ad esempio, possono eseguire le seguenti operazioni:

- Salvare una copia di un file nell'archivio prima dell'eliminazione
- Isolare i file potenzialmente infetti nell'archivio

Gli stati principali dei file sono presentati nella tabella di seguito. È possibile ottenere informazioni più dettagliate sulle azioni da eseguire sui file nelle rispettive Guide delle applicazioni di protezione.

Stati dei file nell'archivio

Nome stato	Descrizione stato
Infetto	Il file contiene una sezione di codice di un virus noto o di altro malware le cui informazioni sono disponibili nei database anti-virus di Kaspersky.
Non infetto	Nel file non sono stati rilevati virus o altri malware noti.
Avviso	Il file contiene un frammento di codice che corrisponde parzialmente a un frammento di codice di una minaccia nota.
Potenzialmente infetto	Il file contiene codice modificato di un virus noto oppure codice somigliante a un virus non ancora noto a Kaspersky.
Inserito nella cartella dall'utente	L'utente ha inserito manualmente il file nell'archivio poiché il comportamento del file ha fatto sospettare che contenesse minacce. L'utente può eseguire la scansione del file per rilevare la presenza di minacce utilizzando i database aggiornati.
Falso positivo	Un'applicazione Kaspersky ha assegnato lo stato Infetto a un file non infetto perché il relativo codice è simile a quello di un virus. Dopo una scansione con i database aggiornati, il file viene identificato come non infetto.
Disinfettato	Il file è stato disinfettato.
Eliminato	Il file è stato eliminato durante l'elaborazione.
Protetto da password	Il file non può essere elaborato poiché è protetto con una password.

Attivazione delle regole in modalità Smart Training

Questa sezione fornisce informazioni sui rilevamenti eseguiti in base alle regole di Controllo adattivo delle anomalie in Kaspersky Endpoint Security for Windows nei dispositivi client.

Le regole rilevano i comportamenti anomali nei dispositivi client e possono bloccarli. Se le regole operano in modalità Smart Training, rilevano i comportamenti anomali e inviano i rapporti su ognuna di tali occorrenze a Kaspersky Security Center Administration Server. Queste informazioni sono archiviate come elenco nella sottocartella **Attivazioni di regole nello stato Smart Training** della cartella **Archivi**. È possibile confermare i rilevamenti come corretti o aggiungerli come esclusioni, in modo che questo tipo di comportamento non venga più considerato anomalo.

Le informazioni sui rilevamenti vengono memorizzate nel registro eventi di Administration Server (insieme ad altri eventi) e nel rapporto di Controllo adattivo delle anomalie.

Per ulteriori informazioni su Controllo adattivo delle anomalie, le regole, le relative modalità e gli stati, fare riferimento alla Guida di Kaspersky Endpoint Security for Windows.

Visualizzazione dell'elenco dei rilevamenti eseguiti tramite Controllo adattivo delle anomalie

Per visualizzare l'elenco dei rilevamenti eseguiti tramite le regole di Controllo adattivo delle anomalie:

1. Nella struttura della console selezionare il nodo dell'Administration Server desiderato.
2. Selezionare la sottocartella **Attivazioni di regole nello stato Smart Training** (per impostazione predefinita è una sottocartella di **Avanzate** → **Archivi**).

   L'elenco visualizza le seguenti informazioni sui rilevamenti eseguiti tramite le regole di Controllo adattivo delle anomalie:

   - **Gruppo di amministrazione**

     Nome del gruppo di amministrazione a cui appartiene il dispositivo.

   - **Nome dispositivo**

     Nome del dispositivo client a cui è stata applicata la regola.

   - **Nome**

     Nome della regola che è stata applicata.

   - **Stato**

     Esclusione in corso - Se l'amministratore ha elaborato questo elemento e lo ha aggiunto come un'esclusione alle regole. Questo stato rimane fino alla successiva sincronizzazione del dispositivo client con Administration Server. Dopo la sincronizzazione, l'elemento viene rimosso dall'elenco.

     Conferma in corso - Se l'amministratore ha elaborato e confermato questo elemento. Questo stato rimane fino alla successiva sincronizzazione del dispositivo client con Administration Server. Dopo la sincronizzazione, l'elemento viene rimosso dall'elenco.

     Vuoto - Se l'amministratore non ha elaborato questo elemento.

   - **Numero totale di volte in cui le regole sono state attivate**

     Numero di rilevamento in una regola euristica, un processo e un dispositivo client. Questo numero viene conteggiato da Kaspersky Endpoint Security.

   - **Nome utente**

     Nome dell'utente del dispositivo client che ha eseguito il processo che ha generato il rilevamento.

   - **Percorso del processo di origine**

     Percorso del processo di origine, ovvero del processo che esegue l'azione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Hash del processo di origine**

  Hash SHA256 del file del processo di origine (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Percorso dell'oggetto di origine**

  Percorso dell'oggetto che ha avviato il processo (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Hash dell'oggetto di origine**

  Hash SHA256 del file di origine (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Percorso del processo di destinazione**

  Percorso del processo di destinazione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Hash del processo di destinazione**

  Hash SHA256 del file di destinazione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Percorso dell'oggetto di destinazione**

  Percorso dell'oggetto di destinazione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Hash dell'oggetto di destinazione**

  Hash SHA256 del file di destinazione (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security).

- **Elaborati**

  Data di rilevamento dell'anomalia.

Per visualizzare le proprietà di ogni elemento di informazioni:

1. Nella struttura della console selezionare il nodo dell'Administration Server desiderato.
2. Selezionare la sottocartella **Attivazioni di regole nello stato Smart Training** (per impostazione predefinita è una sottocartella di **Avanzate** → **Archivi**).

3. Nell'area di lavoro **Attivazioni di regole nello stato Smart Training** selezionare l'oggetto desiderato.

4. Eseguire una delle seguenti operazioni:

   - Nella finestra di informazioni visualizzata nella parte destra della finestra fare clic sul collegamento **Proprietà**.
   - Fare clic con il pulsante destro del mouse e, nel menu di scelta rapida, selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà dell'oggetto, in cui sono visualizzate le informazioni relative all'elemento selezionato.

È possibile confermare o aggiungere alle esclusioni qualsiasi elemento nell'elenco dei rilevamenti delle regole di Controllo adattivo delle anomalie.

Per confermare un elemento:

Selezionare uno o più elementi nell'elenco dei rilevamenti e fare clic sul pulsante **Conferma**.

Lo stato degli elementi verrà modificato in **Conferma in corso**.

La conferma dell'utente contribuisce alle statistiche utilizzate dalle regole (per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Endpoint Security 11 for Windows).

Per aggiungere un elemento come un'esclusione:

Fare clic con il pulsante destro del mouse su uno o più elementi nell'elenco dei rilevamenti e selezionare **Aggiungi alle esclusioni**.

Verrà avviata l'Aggiunta guidata esclusioni. Seguire le istruzioni della procedura guidata.

Se si rifiuta o si conferma un elemento, questo verrà escluso dall'elenco dei rilevamenti dopo la successiva sincronizzazione del dispositivo client con Administration Server e non sarà più visualizzato nell'elenco.

Aggiunta di esclusioni dalle regole di Controllo adattivo delle anomalie

L'Aggiunta guidata esclusioni consente di aggiungere esclusioni dalle regole di Controllo adattivo delle anomalie per Kaspersky Endpoint Security.

È possibile avviare la procedura guidata tramite una delle tre procedure riportate di seguito.

Per avviare l'Aggiunta guidata esclusioni tramite il nodo Controllo adattivo delle anomalie:

1. Nella struttura della console selezionare il nodo dell'Administration Server desiderato.

2. Selezionare **Attivazioni di regole nello stato Smart Training** (per impostazione predefinita è una sottocartella di **Avanzate** → **Archivi**).

3. Nell'area di lavoro fare clic con il pulsante destro del mouse su uno o più elementi nell'elenco dei rilevamenti e selezionare **Aggiungi alle esclusioni**.

   È possibile aggiungere fino a 1.000 esclusioni alla volta. Se si selezionano più elementi e si tenta di aggiungerli alle esclusioni, viene visualizzato un messaggio di errore.

Verrà avviata l'Aggiunta guidata esclusioni.

È possibile avviare l'Aggiunta guidata esclusioni da altri nodi della struttura della console:

- Scheda **Eventi** della finestra principale di Administration Server (quindi scegliere l'opzione **Richieste utente** o **Eventi recenti**).
- **Rapporto sullo stato delle regole di controllo adattivo delle anomalie**, colonna **Numero di rilevamenti**.

Passaggio 1. Selezione dell'applicazione

Se si utilizza una sola versione di Kaspersky Endpoint Security for Windows e non sono presenti altre applicazioni che supportano le regole di Controllo adattivo delle anomalie, è possibile saltare questo passaggio.

L'Aggiunta guidata esclusioni mostra l'elenco delle applicazioni Kaspersky con plug-in di gestione che consentono di aggiungere esclusioni ai criteri per tali applicazioni. Selezionare un'applicazione da questo elenco e fare clic su **Avanti** per procedere alla selezione del criterio a cui aggiungere l'esclusione.

Passaggio 2. Selezione del criterio (criteri)

La procedura guidata mostra l'elenco dei criteri (con i profili criterio) per Kaspersky Endpoint Security.

Selezionare tutti i criteri e i profili per cui si desidera aggiungere le esclusioni e fare clic su **Avanti**.

Passaggio 3. Elaborazione del criterio (criteri)

La procedura guidata mostra una barra di avanzamento mentre i criteri vengono elaborati. È possibile interrompere l'elaborazione dei criteri facendo clic sul pulsante **Annulla**.

I criteri ereditati non possono essere aggiornati. Se non si dispone dei diritti per la modifica di un criterio, tale criterio non verrà aggiornato.

Al termine dell'elaborazione di tutti i criteri (o se si interrompe l'elaborazione), viene visualizzato un rapporto. Il rapporto mostra i criteri che sono stati aggiornati correttamente (icona verde) e quelli che non sono stati aggiornati (icona rossa).

Questo è l'ultimo passaggio della procedura guidata. Fare clic su **Fine** per chiudere la procedura guidata.

Quarantena e Backup

Le applicazioni anti-virus Kaspersky installate nei dispositivi client possono spostare file in Quarantena o nella cartella Backup durante la scansione del dispositivo.

La *Quarantena* è uno speciale archivio per i file potenzialmente infetti da virus e per i file che non è possibile disinfettare al momento del rilevamento.

Backup archivia le copie di backup dei file che sono stati eliminati o modificati durante il processo di disinfezione.

Kaspersky Security Center crea un elenco di riepilogo dei file spostati in Quarantena o nella cartella Backup dalle applicazioni Kaspersky nei dispositivi. I Network Agent nei dispositivi client trasmettono le informazioni relative ai file in Quarantena e nella cartella Backup all'Administration Server. È possibile utilizzare Administration Console per visualizzare le proprietà dei file presenti negli archivi sui dispositivi, eseguire scansioni malware di tali archivi ed eliminare i file che contengono. Nell'appendice sono descritte le icone degli stati dei file.

Per Kaspersky Endpoint Security sono supportate le operazioni con Quarantena e Backup.

Kaspersky Security Center non esegue la copia di file dagli archivi all'Administration Server. Tutti i file sono memorizzati negli archivi sui dispositivi. È possibile ripristinare un file solo nel dispositivo con l'applicazione anti-virus che ha spostato il file nell'archivio.

Abilitazione della gestione remota per i file negli archivi

Per impostazione predefinita, non è possibile gestire i file inseriti negli archivi sui dispositivi client.

Per abilitare la gestione remota dei file inseriti negli archivi sui dispositivi client:

1. Nella struttura della console selezionare un gruppo di amministrazione per cui si desidera abilitare la gestione remota per i file contenuti nell'archivio.
2. Nell'area di lavoro del gruppo aprire la scheda **Criteri**.
3. Nella scheda **Criteri** selezionare il criterio di un'applicazione di protezione che ha inserito i file negli archivi sui dispositivi.
4. Nel gruppo di impostazioni **Trasferimento dei dati ad Administration Server** della finestra delle impostazioni dei criteri selezionare le caselle di controllo corrispondenti agli archivi per cui si desidera abilitare la gestione remota.

   La posizione del gruppo di impostazioni **Trasferimento dei dati ad Administration Server** nella finestra delle proprietà dei criteri e i nomi delle caselle di controllo variano a seconda dell'applicazione di protezione in uso.

Visualizzazione delle proprietà di un file inserito in un archivio

Per visualizzare le proprietà di un file nella cartella Quarantena o Backup:

1. Nella struttura della console selezionare la cartella **Archivi**, quindi la sottocartella **Quarantena** o **Backup**.
2. Nell'area di lavoro della cartella **Quarantena** (**Backup**) selezionare il file per cui si desidera visualizzare le proprietà.
3. Selezionando **Proprietà** nel menu di scelta rapida del file.

Eliminazione di file dagli archivi

Per eliminare un file dalla cartella Quarantena o Backup:

1. Nella struttura della console, nella cartella **Archivi** selezionare la sottocartella **Quarantena** o **Backup**.
2. Nell'area di lavoro della cartella **Quarantena** (o **Backup**) selezionare i file che si desidera eliminare utilizzando i tasti **MAIUSC** e **CTRL**.
3. Eliminare i file in uno dei seguenti modi:
   - Selezionando **Elimina** nel menu di scelta rapida dei file.
   - Facendo clic sul collegamento **Elimina** (**Elimina**) se si desidera eliminare un solo file) nella finestra di informazioni dei file selezionati.

I file verranno eliminati dagli archivi dalle applicazioni di protezione che hanno inserito i file negli archivi sui dispositivi client.

Ripristino di file dagli archivi

Per ripristinare un file dalla cartella Quarantena o Backup:

1. Nella struttura della console selezionare la cartella **Archivi**, quindi la sottocartella **Quarantena** o **Backup**.
2. Nell'area di lavoro della cartella **Quarantena** (**Backup**) selezionare i file che si desidera ripristinare utilizzando i tasti **MAIUSC** e **CTRL**.
3. Avviare il ripristino dei file in uno dei seguenti modi:
   - Selezionando **Ripristina** nel menu di scelta rapida dei file.
   - Facendo clic sul collegamento **Ripristina** nella finestra di informazioni dei file selezionati.

I file verranno ripristinati nelle cartelle di origine dalle applicazioni di protezione che hanno inserito i file negli archivi sui dispositivi client.

Salvataggio di un file su disco dagli archivi

Kaspersky Security Center consente di salvare su disco le copie dei file che sono state inserite nella cartella Quarantena o Backup su un dispositivo client da un'applicazione di protezione. I file vengono copiati nel dispositivo in cui è installato Kaspersky Security Center, nella cartella specificata.

Per salvare una copia del file dalla cartella Quarantena o Backup sul disco rigido:

1. Nella struttura della console selezionare la cartella **Archivi**, quindi la sottocartella **Quarantena** o **Backup**.
2. Nell'area di lavoro della cartella **Quarantena** (**Backup**) selezionare un file che si desidera copiare sul disco rigido.
3. Avviare la copia in uno dei seguenti modi:
   - Selezionando **Salva su disco** nel menu di scelta rapida del file.
   - Facendo clic sul collegamento **Salva su disco** nella finestra di informazioni del file selezionato.

Una copia del file verrà salvata nella cartella specificata dall'applicazione di protezione che ha collocato il file in Quarantena nel dispositivo client.

Scansione dei file in quarantena

Per eseguire la scansione dei file in quarantena:

1. Nella struttura della console selezionare la cartella **Archivi**, quindi la sottocartella **Quarantena**.
2. Nell'area di lavoro della cartella **Quarantena** selezionare i file di cui si desidera eseguire la scansione utilizzando i tasti **MAIUSC** e **CTRL**.
3. Avviare la scansione del file in uno dei seguenti modi:
   - Selezionando **Scansione** nel menu di scelta rapida dei file.
   - Facendo clic sul collegamento **Scansione** nella finestra di informazioni dei file selezionati.

   Verrà avviata l'attività di scansione su richiesta per le applicazioni di protezione che hanno inserito i file selezionati in Quarantena nei dispositivi in cui sono archiviati tali file.

Minacce attive

Le informazioni relative ai file non elaborati rilevati nei dispositivi client sono memorizzate nella sottocartella **Minacce attive** della cartella **Archivi**.

L'elaborazione rimandata e la disinfezione vengono eseguite dall'applicazione di protezione su richiesta o dopo un evento specificato. È possibile configurare l'elaborazione rimandata.

Disinfezione di un file non elaborato

Per avviare la disinfezione di un file non elaborato:

1. Nella struttura della console, nella cartella **Archivi** selezionare la sottocartella **Minacce attive**.
2. Nell'area di lavoro della cartella **Minacce attive** selezionare il file da disinfettare.
3. Avviare la disinfezione del file in uno dei seguenti modi:
   - Selezionando **Disinfetta** nel menu di scelta rapida dei file.
   - Facendo clic sul collegamento **Disinfetta** nella finestra di informazioni del file selezionato.

   Verrà eseguito un tentativo di disinfezione del file.

Se il file viene disinfettato, l'applicazione di protezione installata nel dispositivo client lo ripristina nella cartella originale. Il record del file viene rimosso dall'elenco nella cartella **Minacce attive**. Se il file non può essere disinfettato, l'applicazione di protezione installata nel dispositivo lo elimina dal dispositivo. Il record del file viene rimosso dall'elenco nella cartella **Minacce attive**.

La capacità di disinfezione ed eliminazione dei file può variare a seconda dell'applicazione di protezione installata, della sua versione e delle impostazioni.

Salvataggio su disco di un file non elaborato

Kaspersky Security Center consente di salvare su disco le copie dei file non elaborati rilevati nei dispositivi client. Questo si riferisce ai file trattati o eliminati dall'applicazione. I file vengono copiati nel dispositivo in cui è installato Kaspersky Security Center, nella cartella specificata.

È possibile salvare copie dei file se i file sono stati eliminati o modificati durante la disinfezione e le relative copie sono archiviate nell'archivio di Kaspersky Endpoint Security for Windows sul dispositivo gestito.

Per salvare su disco una copia di un file non elaborato:

1. Nella struttura della console, nella cartella **Archivi** selezionare la sottocartella **Minacce attive**.
2. Nell'area di lavoro della cartella **Minacce attive** selezionare i file da copiare sul disco.
3. Avviare la copia in uno dei seguenti modi:
   - Selezionando **Salva su disco** nel menu di scelta rapida del file.
   - Facendo clic sul collegamento **Salva su disco** nella finestra di informazioni del file selezionato.

Una copia del file viene salvata nella cartella specificata dall'applicazione di protezione installata nel dispositivo client in cui è stato rilevato il file non elaborato.

Eliminazione dei file dalla cartella "Minacce attive"

*Per eliminare un file dalla cartella **Minacce attive**:*

1. Nella struttura della console, nella cartella **Archivi** selezionare la sottocartella **Minacce attive**.
2. Nell'area di lavoro della cartella **Minacce attive** selezionare i file da eliminare utilizzando i tasti **MAIUSC** e **CTRL**.
3. Eliminare i file in uno dei seguenti modi:
   - Selezionando **Elimina** nel menu di scelta rapida dei file.
   - Facendo clic sul collegamento **Elimina** (**Elimina** se si desidera eliminare un solo file) nella finestra di informazioni dei file selezionati.

I file verranno eliminati dagli archivi dalle applicazioni di protezione che hanno inserito i file negli archivi sui dispositivi client. I record dei file vengono rimossi dall'elenco nella cartella **Minacce attive**.

Finestra Kaspersky Security Network (KSN)

In questa sezione viene descritto come utilizzare un'infrastruttura di servizi online denominata Kaspersky Security Network (KSN). Vengono fornite informazioni dettagliate su KSN e istruzioni su come abilitare KSN, configurare l'accesso a KSN e visualizzare le statistiche di utilizzo del server proxy KSN.

Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Informazioni su KSN

Kaspersky Security Network (KSN) è un'infrastruttura di servizi online che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora l'efficacia di alcuni componenti della protezione e riduce il rischio di falsi positivi. KSN consente di utilizzare i database di reputazione di Kaspersky per recuperare informazioni sulle applicazioni installate nei dispositivi gestiti.

Kaspersky Security Center supporta le seguenti soluzioni di infrastruttura:

- *KSN* è una soluzione che consente di scambiare informazioni con Kaspersky Security Network. Se si partecipa a KSN, si autorizza l'invio automatico a Kaspersky di informazioni sul funzionamento delle applicazioni Kaspersky installate nei dispositivi client gestiti tramite Kaspersky Security Center. Le informazioni vengono trasferite in base alle impostazioni di accesso a KSN correnti. Gli analisti di Kaspersky analizzano inoltre le informazioni ricevute e le includono nei database statistici e di reputazione di Kaspersky Security Network. Kaspersky Security Center utilizza questa soluzione per impostazione predefinita.

- *Kaspersky Private Security Network (KPSN)* è una soluzione che consente agli utenti di dispositivi con applicazioni Kaspersky installate di ottenere l'accesso ai database di reputazione di Kaspersky Security Network e ad altri dati statistici, senza inviare dati a KSN Globale dai propri dispositivi. KPSN è progettato per i clienti aziendali che non sono in grado di partecipare al programma Kaspersky Security Network per uno dei seguenti motivi:

  - I dispositivi dell'utente non sono connessi a Internet.

  - La trasmissione dei dati all'esterno del paese o all'esterno della rete LAN aziendale è vietata dalla legge o limitata dai criteri di protezione aziendali.

  È possibile configurare le impostazioni di accesso di Kaspersky Private Security Network nella sezione **Impostazioni proxy KSN** della finestra delle proprietà di Administration Server.

All'utente verrà richiesto di partecipare a KSN durante l'esecuzione dell'Avvio rapido guidato. È possibile iniziare o smettere di utilizzare KSN in qualsiasi momento durante l'utilizzo dell'applicazione.

È necessario utilizzare KSN in conformità con l'Informativa KSN letta e accettata durante l'attivazione di KSN. Se l'Informativa KSN viene aggiornata, viene visualizzata quando si esegue l'upgrade di una versione di Administration Server. È possibile accettare o rifiutare l'Informativa KSN aggiornata. In caso di rifiuto, si continuerà a utilizzare KSN in conformità con la versione precedente dell'Informativa KSN già accettata.

Quando KSN è abilitato, Kaspersky Security Center verifica se i server KSN sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. Ciò è necessario per garantire il mantenimento del livello di sicurezza per i dispositivi gestiti.

I dispositivi client gestiti da Administration Server interagiscono con KSN attraverso il server proxy KSN. Il server proxy KSN fornisce le seguenti funzionalità:

- I dispositivi client possono inviare richieste a KSN, ottenere informazioni da KSN e trasferire informazioni a KSN anche se non hanno accesso diretto a Internet.

- Il server proxy KSN memorizza nella cache i dati elaborati, riducendo in tal modo il carico sul canale in uscita e il tempo di attesa per ottenere le informazioni richieste da un dispositivo client.

È possibile configurare il server proxy KSN nella sezione **Impostazioni proxy KSN** della finestra delle proprietà di Administration Server.

Impostazione dell'accesso a Kaspersky Security Network

È possibile configurare l'accesso a Kaspersky Security Network (KSN) in Administration Server e in un punto di distribuzione.

Per configurare l'accesso di Administration Server a Kaspersky Security Network (KSN):

1. Nella struttura della console selezionare l'Administration Server per cui si desidera configurare l'accesso a KSN.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni** selezionare **Proxy KSN** → **Impostazioni proxy KSN**.
4. Nell'area di lavoro, abilitare l'opzione **Usa Administration Server come server proxy** per utilizzare il servizio proxy KSN.

   I dati vengono inviati dai dispositivi client a KSN in conformità con il criterio di Kaspersky Endpoint Security attivo in tali dispositivi client. Se questa casella di controllo è deselezionata, non verranno inviati dati a KSN da Administration Server e dai dispositivi client tramite Kaspersky Security Center. I dispositivi client possono comunque inviare dati a KSN direttamente (ignorando Kaspersky Security Center), in base alle relative impostazioni. Il criterio di Kaspersky Endpoint Security for Windows attivo nei dispositivi client determina quali dati saranno inviati a KSN direttamente (ignorando Kaspersky Security Center) da tali dispositivi.

5. Abilitare l'opzione **Accetto di utilizzare Kaspersky Security Network**.

   Se questa opzione è abilitata, i dispositivi client invieranno i risultati dell'installazione delle patch a Kaspersky. Quando si abilita questa opzione, leggere e accettare le condizioni dell'informativa KSN.

   Se si utilizza Kaspersky Private Security Network, abilitare l'opzione **Configura KPSN** e fare clic sul pulsante **Selez. file con imp. del proxy KSN** per scaricare le impostazioni di KPSN (file con estensioni pkcs7 e pem). Una volta scaricate le impostazioni, l'interfaccia mostra il nome e i contatti del provider, nonché la data di creazione del file con le impostazioni di KPSN.

   > Quando si abilita KPSN, prestare attenzione ai punti di distribuzione configurati per l'invio di richieste KSN direttamente a KSN Cloud. I punti di distribuzione in cui è installato Network Agent versione 11 (o precedente) continueranno a inviare richieste KSN a KSN Cloud. Per riconfigurare i punti di distribuzione per l'invio di richieste KSN a KPSN, abilitare l'opzione **Inoltra richieste KSN ad Administration Server** per ciascun punto di distribuzione. È possibile abilitare questa opzione nelle proprietà del punto di distribuzione o nel criterio di Network Agent.

   Quando si seleziona la casella di controllo **Configura KPSN**, viene visualizzato un messaggio con informazioni dettagliate su KPSN.

   Se si abilita l'opzione **Configura KPSN** in Kaspersky Security Center, tali applicazioni ricevono informazioni sul supporto di KPSN. Nella finestra delle impostazioni dell'applicazione, nella sottosezione **Kaspersky Security Network** della sezione **Protezione Minacce Avanzata**, vengono visualizzate le informazioni sul provider KSN selezionato: KSN o KPSN.

   > Se si utilizzano versioni delle applicazioni precedenti a Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 oppure a Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent durante l'esecuzione di KPSN, è consigliabile utilizzare Administration Server secondari per cui l'utilizzo di KPSN Privato non è stato abilitato.

   > Kaspersky Security Center non invia dati statistici a Kaspersky Security Network se KPSN è configurato nella sezione **Proxy KSN** → **Impostazioni proxy KSN** della finestra delle proprietà di Administration Server.

   Se sono state configurate le impostazioni del server proxy nelle proprietà di Administration Server, ma l'architettura di rete richiede di utilizzare direttamente KPSN, abilitare l'opzione **Ignora impostazioni del server proxy durante la connessione a KPSN**. In caso contrario, le richieste dalle applicazioni gestite non possono raggiungere KPSN.

6. Configurare la connessione di Administration Server al servizio proxy KSN:

   - In **Impostazioni di connessione**, per **Porta TCP** specificare il numero della porta TCP che verrà utilizzata per la connessione al server proxy KSN. La porta predefinita per la connessione al server proxy KSN è la 13111.
   - Se si desidera che Administration Server si connetta al server proxy KSN attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** port e specificare il numero della porta in **Porta UDP**. Per impostazione predefinita, questa opzione è disabilitata e viene utilizzata la porta TCP. Se l'opzione è attivata, la porta UDP predefinita per la connessione al server KSN Proxy è 15111.
   - Se si desiderza che Administration Server si connetta al server proxy KSN attraverso una porta HTTPS, abilitare l'opzione **Usa HTTPS tramite porta** e specificare il numero di porta. Per impostazione predefinita, questa opzione è disabilitata e viene utilizzata la porta TCP. Se l'opzione è attivata, la porta HTTPS predefinita per la connessione al server KSN Proxy è 17111.

7. Abilitare l'opzione **Connetti Administration Server secondari a KSN tramite Administration Server primario**.

   Se questa opzione è abilitata, gli Administration Server secondari di qualsiasi livello di gerarchia utilizzano l'Administration Server primario come server proxy KSN. Se questa opzione è disabilitata, gli Administration Server secondari si connettono a KSN autonomamente. In questo caso, i dispositivi gestiti utilizzano gli Administration Server secondari come server proxy KSN.

   > Gli Administration Server secondari utilizzano l'Administration Server primario come server proxy se è selezionata la casella di controllo **Usa Administration Server come server proxy** nel riquadro destro della sezione **Impostazioni proxy KSN** nelle proprietà degli Administration Server secondari.

8. Fare clic su **OK**.

Le impostazioni di accesso a KSN verranno salvate.

È inoltre possibile impostare l'accesso del punto di distribuzione a KSN, ad esempio se si desidera ridurre il carico sull'Administration Server. Il punto di distribuzione che opera come server proxy KSN invia richieste KSN direttamente dai dispositivi gestiti a Kaspersky, senza utilizzare l'Administration Server.

Per configurare l'accesso del punto di distribuzione a Kaspersky Security Network (KSN):

1. Accertarsi che il punto di distribuzione sia assegnato manualmente.
2. Nella struttura della console selezionare il nodo **Administration Server**.
3. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
4. Nella finestra delle proprietà di Administration Server selezionare la sezione **Punti di distribuzione**.
5. Selezionare il punto di distribuzione nell'elenco e fare clic sul pulsante **Proprietà** per aprire la relativa finestra delle proprietà.
6. Nella finestra delle proprietà del punto di distribuzione, nella sezione **Proxy KSN** selezionare **Accedi a KSN Cloud/KPSN direttamente tramite Internet**.
7. Fare clic su **OK**.

Il punto di distribuzione opererà come un server proxy KSN.

Abilitazione e disabilitazione di KSN

Per abilitare KSN:

1. Nella struttura della console selezionare l'Administration Server per cui si desidera abilitare KSN.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella sezione **Proxy KSN** della finestra delle proprietà di Administration Server selezionare la sottosezione **Impostazioni proxy KSN**.
4. Selezionare **Usa Administration Server come server proxy**.

   Il server proxy KSN viene abilitato.

5. Selezionare la casella di controllo **Accetto di utilizzare Kaspersky Security Network**.

   KSN verrà abilitato.

   Se questa casella di controllo è selezionata, i dispositivi client invieranno i risultati dell'installazione delle patch a Kaspersky. Quando si seleziona questa casella di controllo, è necessario leggere e accettare le condizioni dell'informativa KSN.

6. Fare clic su **OK**.

Per disabilitare KSN:

1. Nella struttura della console selezionare l'Administration Server per cui si desidera abilitare KSN.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella sezione **Proxy KSN** della finestra delle proprietà di Administration Server selezionare la sottosezione **Impostazioni proxy KSN**.
4. Deselezionare la casella di controllo **Usa Administration Server come server proxy** per disabilitare il servizio proxy KSN oppure deselezionare la casella di controllo **Accetto di utilizzare Kaspersky Security Network**.

   Se questa casella di controllo è deselezionata, i dispositivi client non invieranno i risultati dell'installazione delle patch a Kaspersky.

   Se si utilizza KPSN, deselezionare la casella di controllo **Configura KPSN**.

   KSN verrà disabilitato.

5. Fare clic su **OK**.

Visualizzazione dell'Informativa KSN accettata

Quando si abilita Kaspersky Security Network (KSN), è necessario leggere e accettare l'Informativa KSN. È possibile visualizzare l'Informativa KSN accettata in qualsiasi momento.

Per visualizzare l'Informativa KSN accettata:

1. Nella struttura della console selezionare l'Administration Server per cui è stato abilitato KSN.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella sezione **Proxy KSN** della finestra delle proprietà di Administration Server selezionare la sottosezione **Impostazioni proxy KSN**.
4. Fare clic sul collegamento **Visualizza l'Informativa KSN accettata**.

Nella finestra visualizzata è possibile visualizzare il testo dell'Informativa KSN accettata.

Visualizzazione delle statistiche del server proxy KSN

Server proxy KSN è un servizio che assicura l'interazione tra l'infrastruttura di Kaspersky Security Network e i dispositivi client gestiti tramite Administration Server.

L'utilizzo di un server proxy KSN fornisce le seguenti funzionalità:

- I dispositivi client possono inviare richieste a KSN e trasferire informazioni a KSN anche se non hanno accesso diretto a Internet.
- Il server proxy KSN memorizza nella cache i dati elaborati, riducendo in tal modo il carico sul canale in uscita e il tempo di attesa per ottenere le informazioni richieste da un dispositivo client.

Nella finestra delle proprietà dell'Administration Server è possibile configurare il server proxy KSN e visualizzare le statistiche sull'utilizzo del server proxy KSN.

Per visualizzare le statistiche del server proxy KSN:

1. Nella struttura della console selezionare l'Administration Server per cui si desidera visualizzare le statistiche KSN.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra delle proprietà di Administration Server, nella sezione **Proxy KSN**, selezionare la sottosezione **Statistiche Proxy KSN**.

   In questa sezione vengono visualizzate le statistiche effettive sull'esecuzione del server proxy KSN (il numero di record della cache, i pacchetti elaborati nella cache e i pacchetti ricevuti). Inoltre, se Administration Server è connesso a KSN, viene visualizzato il messaggio informativo corrispondente.

   Se necessario, eseguire queste azioni aggiuntive:

   - Fare clic su **Aggiorna** per aggiornare le statistiche sull'utilizzo del server proxy KSN.
   - Fare clic sul pulsante **Esporta in un file** per esportare le statistiche in un file CSV.
   - Fare clic sul pulsante **Verifica connessione a KSN** per verificare se Administration Server al momento è connesso a KSN.
4. Fare clic sul pulsante **OK** per chiudere la finestra delle proprietà di Administration Server.

Accettazione di un'Informativa KSN aggiornata

È necessario utilizzare KSN in conformità con l'Informativa KSN letta e accettata durante l'attivazione di KSN. Se l'Informativa KSN viene aggiornata, viene visualizzata quando si esegue l'aggiornamento o l'upgrade di Administration Server. È possibile accettare o rifiutare l'Informativa KSN aggiornata. In caso di rifiuto, si continuerà a utilizzare KSN in conformità con la versione dell'Informativa KSN accettata precedentemente.

Dopo aver eseguito l'aggiornamento o l'upgrade di Administration Server, l'Informativa KSN aggiornata verrà visualizzata automaticamente. Se si rifiuta l'Informativa KSN aggiornata, sarà comunque possibile visualizzarla e accettarla in un secondo momento.

Per visualizzare e successivamente accettare o rifiutare un'Informativa KSN aggiornata:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Nella scheda **Monitoraggio**, nella sezione **Monitoraggio** fare clic sul collegamento **L'Informativa di Kaspersky Security Network accettata è obsoleta**.

   Verrà visualizzata la finestra **Informativa KSN**.
3. Leggere attentamente l'Informativa KSN e successivamente prendere una decisione. Se si accetta l'Informativa KSN aggiornata, fare clic sul pulsante **Accetto i termini del Contratto di licenza**. Se si rifiuta l'Informativa KSN aggiornata, fare clic sul pulsante **Annulla**.

A seconda della scelta, KSN continuerà a funzionare in conformità con i termini dell'Informativa KSN corrente o aggiornata. È possibile visualizzare il testo dell'Informativa KSN accettata nelle proprietà di Administration Server in qualsiasi momento.

Protezione avanzata con Kaspersky Security Network

Kaspersky offre agli utenti un livello di protezione aggiuntivo mediante Kaspersky Security Network. Questo metodo di protezione è progettato per contrastare le minacce persistenti di livello avanzato e gli attacchi zero-day. Le tecnologie cloud integrate e l'esperienza degli analisti anti-virus di Kaspersky rendono Kaspersky Endpoint Security la soluzione migliore in assoluto per la protezione dalle minacce di rete più complesse.

Informazioni dettagliate sulla protezione avanzata in Kaspersky Endpoint Security sono disponibili nel sito Web di Kaspersky.

Verifica per stabilire se il punto di distribuzione funziona come server proxy KSN

In un dispositivo gestito a cui è assegnato il ruolo di punto di distribuzione è possibile abilitare il server proxy KSN. Un dispositivo gestito funziona come server proxy KSN quando il servizio ksnproxy è in esecuzione nel dispositivo. È possibile controllare, attivare o disattivare questo servizio nel dispositivo in locale.

È possibile assegnare un dispositivo basato su Windows o Linux come punto di distribuzione. Il metodo di controllo del punto di distribuzione dipende dal sistema operativo di questo punto di distribuzione.

Per verificare se il punto di distribuzione basato su Windows funziona come server proxy KSN:

1. Nel dispositivo del punto di distribuzione, in Windows, aprire **Servizi** (**Tutti i programmi** → **Strumenti di amministrazione** → **Servizi**).
2. Nell'elenco dei servizi verificare se il servizio ksnproxy è in esecuzione.

   Se il servizio ksnproxy è in esecuzione, Network Agent nel dispositivo partecipa a Kaspersky Security Network e funziona come server proxy KSN per i dispositivi gestiti inclusi nell'ambito del punto di distribuzione.

Se si desidera, è possibile disattivare il servizio ksnproxy. In questo caso Network Agent nel punto di distribuzione interrompe la partecipazione a Kaspersky Security Network. Sono necessari i diritti di amministratore locale.

Per verificare se il punto di distribuzione basato su Linux funziona come server proxy KSN:

1. Nel dispositivo del punto di distribuzione, visualizzare l'elenco dei processi in esecuzione.
2. Nell'elenco dei processi in esecuzione, controllare se il processo `/opt/kaspersky/ksc64/sbin/ksnproxy` è in esecuzione.

Se il processo `/opt/kaspersky/ksc64/sbin/ksnproxy` è in esecuzione, Network Agent nel dispositivo partecipa a Kaspersky Security Network e funziona come server proxy KSN per i dispositivi gestiti inclusi nell'ambito del punto di distribuzione.

Passaggio dalla Guida in linea alla Guida offline e viceversa

Se non si dispone dell'accesso a Internet, è possibile utilizzare la Guida offline.

Per passare dalla Guida in linea alla Guida offline e viceversa:

1. Nella finestra principale di Kaspersky Security Center selezionare nella struttura della console **Kaspersky Security Center 15.1**.
2. Fare clic sul collegamento **Impostazioni dell'interfaccia globale**.

   Verrà visualizzata la finestra delle impostazioni.
3. Nella finestra delle impostazioni fare clic su **Usa Guida offline**.
4. Fare clic su **OK**.

Le impostazioni verranno applicate e salvate. Se lo si desidera, è possibile modificare nuovamente le impostazioni e iniziare a utilizzare la Guida in linea in qualsiasi momento.

Esportazione di eventi nei sistemi SIEM

In questa sezione viene descritto come esportare gli eventi registrati da Kaspersky Security Center in sistemi SIEM (Security Information and Event Management) esterni.

Configurazione dell'esportazione di eventi nei sistemi SIEM

Kaspersky Security Center consente la configurazione con uno dei seguenti metodi: esportazione in qualsiasi sistema SIEM che utilizza il formato Syslog, esportazione in sistemi QRadar, Splunk, ArcSight SIEM che utilizzano i formati LEEF e CEF o esportazione di eventi in sistemi SIEM direttamente dal database di Kaspersky Security Center. Al termine di questo scenario, Administration Server invia automaticamente gli eventi al sistema SIEM.

Prerequisiti

Prima di avviare la configurazione dell'esportazione degli eventi in Kaspersky Security Center:

- Ulteriori informazioni sui metodi di esportazione degli eventi.
- Assicurarsi di disporre dei valori delle impostazioni di sistema.

È possibile eseguire i passaggi di questo scenario in qualsiasi ordine.

Il processo di esportazione degli eventi nel sistema SIEM prevede i seguenti passaggi:

- **Configurazione del sistema SIEM per la ricezione di eventi da Kaspersky Security Center**

  Istruzioni dettagliate: Configurazione dell'esportazione di eventi in un sistema SIEM

- **Selezione degli eventi che si desidera esportare nel sistema SIEM:**

  Istruzioni dettagliate:

  - Administration Console: Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog, Contrassegno di eventi generici per l'esportazione nel formato Syslog
  - Kaspersky Security Center Web Console: Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog, Contrassegno di eventi generali per l'esportazione nel formato Syslog

- **Configurazione dell'esportazione degli eventi nel sistema SIEM utilizzando uno dei seguenti metodi:**

  - Utilizzo dei protocolli TCP, UDP o TLS su TCP.

    Istruzioni dettagliate:

    - Administration Console: Configurazione dell'esportazione di eventi nei sistemi SIEM
    - Kaspersky Security Center Web Console: Configurazione dell'esportazione di eventi nei sistemi SIEM

  - Utilizzo dell'esportazione di eventi direttamente dal database di Kaspersky Security Center. È disponibile un set di visualizzazioni pubbliche nel database di Kaspersky Security Center. È possibile trovare la descrizione di queste visualizzazioni pubbliche nel documento klakdb.chm.

Risultati

Dopo aver configurato l'esportazione degli eventi nel sistema SIEM, è possibile visualizzare i risultati dell'esportazione se sono stati selezionati gli eventi da esportare.

Prima di iniziare

Durante la configurazione dell'esportazione automatica degli eventi in Kaspersky Security Center, è necessario specificare alcune impostazioni del sistema SIEM. È consigliabile verificare preventivamente queste impostazioni per la preparazione della configurazione di Kaspersky Security Center.

Per configurare l'invio automatico degli eventi in un sistema SIEM, è necessario conoscere le seguenti impostazioni:

- **Indirizzo server del sistema SIEM**

  L'indirizzo IP del server in cui è installato il sistema SIEM utilizzato attualmente. Verificare questo valore nelle impostazioni del sistema SIEM.

- **Porta server del sistema SIEM**

  Numero della porta utilizzato per stabilire la connessione tra Kaspersky Security Center e il server del sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center e nelle impostazioni del destinatario del sistema SIEM.

- **Protocollo**

  Protocollo utilizzato per il trasferimento dei messaggi da Kaspersky Security Center al sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center e nelle impostazioni del destinatario del sistema SIEM.

Informazioni sugli eventi in Kaspersky Security Center

Kaspersky Security Center consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Le informazioni sugli eventi vengono salvate nel database di Administration Server. È possibile esportare queste informazioni in sistemi SIEM esterni. L'esportazione delle informazioni sugli eventi nei sistemi SIEM esterni consente agli amministratori dei sistemi SIEM di rispondere tempestivamente agli eventi del sistema di protezione che si verificano nei gruppi di amministrazione o dispositivi gestiti.

Tipi di evento

In Kaspersky Security Center sono disponibili i seguenti tipi di eventi:

- Eventi generici. Questi eventi si verificano in tutte le applicazioni Kaspersky gestite. Un esempio di evento generico è l'Epidemia di virus. Gli eventi generici hanno sintassi e semantica rigorosamente definite. Gli eventi generici vengono ad esempio utilizzati nei rapporti e nei dashboard.

- Eventi specifici delle applicazioni gestiti da Kaspersky. Ogni applicazione Kaspersky gestita dispone di uno specifico set di eventi.

Origini eventi

Gli eventi possono essere generati dalle seguenti applicazioni:

- Componenti di Kaspersky Security Center:
  - Administration Server
  - Network Agent
  - Server per dispositivi mobili MDM iOS
- Applicazioni Kaspersky gestite

  Per i dettagli sugli eventi generati dalle applicazioni gestite da Kaspersky, consultare la documentazione dell'applicazione corrispondente.

È possibile visualizzare l'elenco completo degli eventi che possono essere generati da un'applicazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare l'elenco degli eventi nelle proprietà dell'Administration Server.

Livello di importanza degli eventi

Ogni evento dispone di uno specifico livello di importanza. In base alle condizioni in cui si verifica, a un evento possono essere assegnati diversi livelli di importanza. Esistono quattro livelli di importanza degli eventi:

- Un *evento critico* è un evento che indica la presenza di un problema critico che può determinare una perdita dei dati, un malfunzionamento o un errore critico.
- Un *errore funzionale* è un evento che indica la presenza di un problema grave, un errore o un malfunzionamento che si è verificato durante l'esecuzione dell'applicazione o di una procedura.
- Un *avviso* è un evento che non è necessariamente grave, ma indica comunque un potenziale problema futuro. La maggior parte degli eventi viene designata come avviso se l'applicazione può essere ripristinata senza perdite di dati o funzionalità importanti dopo che si sono verificati tali eventi.
- Un *evento informativo* è un evento che si verifica allo scopo di segnalare il completamento di un'operazione, il corretto funzionamento dell'applicazione o il completamento di una procedura.

Ogni evento ha un periodo di archiviazione definito, durante il quale può essere visualizzato o modificato in Kaspersky Security Center. Alcuni eventi non vengono salvati nel database di Administration Server per impostazione predefinita, poiché il relativo periodo di archiviazione definito è pari a zero. Solo gli eventi che verranno memorizzati nel database di Administration Server per almeno un giorno possono essere esportati in sistemi esterni.

Informazioni sull'esportazione degli eventi

È possibile utilizzare l'esportazione degli eventi in sistemi centralizzati che gestiscono i problemi di protezione a livello tecnico e organizzativo, garantiscono servizi di monitoraggio della sicurezza e consolidano informazioni da diverse soluzioni. Si tratta di sistemi SIEM, che offrono analisi in tempo reale degli avvisi e degli eventi di protezione generati da applicazioni e hardware di rete o SOC (Security Operation Center).

Questi sistemi ricevono i dati da numerose origini, tra cui reti, sicurezza, server, database e applicazioni. I sistemi SIEM forniscono anche funzionalità per consolidare i dati monitorati ed evitare la perdita di eventi critici. Inoltre, questi sistemi eseguono analisi automatizzate di avvisi ed eventi correlati per inviare immediatamente agli amministratori una notifica dei problemi di protezione. Gli avvisi possono essere implementati tramite un dashboard o inviati tramite canali di terzi, ad esempio via e-mail.

Il processo di esportazione degli eventi da Kaspersky Security Center ai sistemi SIEM esterni coinvolge due parti: un mittente degli eventi (Kaspersky Security Center) e il destinatario di un evento (il sistema SIEM). Per eseguire l'esportazione degli eventi, è necessario configurare questa funzionalità nel sistema SIEM e in Kaspersky Security Center. Non è importante quale lato viene configurato per primo. È possibile configurare la trasmissione degli eventi in Kaspersky Security Center, quindi configurare la ricezione degli eventi dal sistema SIEM o viceversa.

Metodi per l'invio degli eventi da Kaspersky Security Center

Esistono tre metodi per l'invio degli eventi da Kaspersky Security Center ai sistemi esterni:

- Invio degli eventi tramite il protocollo Syslog a qualsiasi sistema SIEM

  Utilizzando il protocollo Syslog è possibile inviare gli eventi che si verificano in Kaspersky Security Center Administration Server e nelle applicazioni Kaspersky installate nei dispositivi gestiti. Il protocollo Syslog è un protocollo standard per la registrazione dei messaggi. Può essere utilizzato per esportare gli eventi in qualsiasi sistema SIEM.

  A tale scopo, è necessario contrassegnare gli eventi che si desidera inoltrare al sistema SIEM. È possibile contrassegnare gli eventi in Administration Console o Kaspersky Security Center Web Console. Solo gli eventi contrassegnati verranno inoltrati al sistema SIEM. Se non è stato contrassegnato nulla, nessun evento verrà inoltrato.

- Invio degli eventi tramite i protocolli CEF e LEEF ai sistemi QRadar, Splunk e ArcSight

  È possibile utilizzare i protocolli CEF e LEEF per esportare eventi generali. Durante l'esportazione degli eventi tramite i protocolli CEF e LEEF, non si ha la possibilità di selezionare gli eventi specifici da esportare. Al contrario, vengono esportati tutti gli eventi generali. Per convertire gli eventi Kaspersky Security Center in eventi nei formati CEF e LEEF, è necessario utilizzare il file siem_conversion_rules.xml. Questo file contiene l'elenco degli attributi degli eventi Kaspersky Security Center e gli attributi corrispondenti degli eventi nei formati CEF e LEEF. Inoltre, il file siem_conversion_rules.xml contiene le regole per generare messaggi corrispondenti agli eventi. Questo file è incluso nel kit di distribuzione di Kaspersky Security Center.

  A differenza del protocollo Syslog, i protocolli CEF e LEEF non sono universali. I protocolli CEF e LEEF sono destinati ai sistemi SIEM appropriati (QRadar, Splunk e ArcSight). Di conseguenza, quando si sceglie di esportare gli eventi in uno di questi protocolli, utilizzare il parser richiesto per il sistema SIEM.

- Direttamente dal database di Kaspersky Security Center in qualsiasi sistema SIEM

  Questo metodo di esportazione degli eventi può essere utilizzato per ricevere gli eventi direttamente da visualizzazioni pubbliche del database tramite query SQL. I risultati di una query vengono salvati in un file XML che può essere utilizzato come input dei dati per un sistema esterno. Solo gli eventi disponibili nelle visualizzazioni pubbliche possono essere esportati direttamente dal database.

Ricezione degli eventi da parte del sistema SIEM

Il sistema SIEM deve ricevere e analizzare correttamente gli eventi ricevuti da Kaspersky Security Center. A tale scopo, è necessario configurare correttamente il sistema SIEM. La configurazione dipende dallo specifico sistema SIEM in uso. Sono comunque previsti diversi passaggi generali per la configurazione di tutti i sistemi SIEM, ad esempio la configurazione del ricevitore e del parser.

Informazioni sulla configurazione dell'esportazione di eventi in un sistema SIEM

Il processo di esportazione degli eventi da Kaspersky Security Center ai sistemi SIEM esterni coinvolge due parti: un mittente degli eventi (Kaspersky Security Center) e il destinatario di un evento (il sistema SIEM). È necessario configurare l'esportazione degli eventi nel sistema SIEM e in Kaspersky Security Center.

Le impostazioni specificate nel sistema SIEM dipendono dal particolare sistema in uso. In genere, per tutti i sistemi SIEM è necessario impostare un ricevitore ed eventualmente un parser dei messaggi per l'analisi degli eventi ricevuti.

Configurazione del ricevitore

Per la ricezione degli eventi inviati da Kaspersky Security Center, è necessario impostare il ricevitore nel sistema SIEM. In generale, le seguenti impostazioni devono essere specificate nel sistema SIEM:

- **Protocollo di esportazione o tipo di input**

  È il protocollo di trasferimento dei messaggi, ad esempio UDP. Il protocollo deve corrispondere al protocollo specificato in Kaspersky Security Center.

- **Porta**

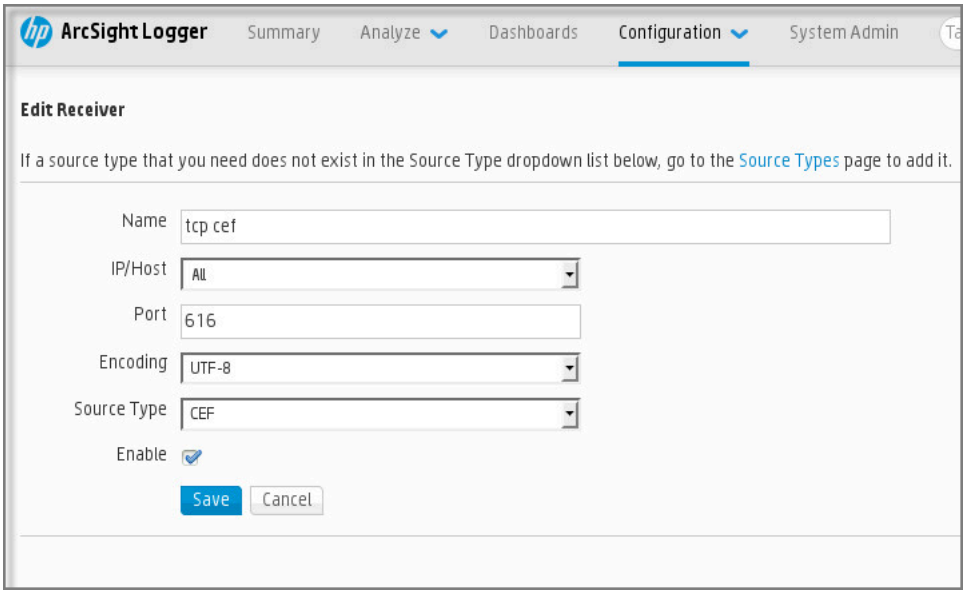
  Numero di porta per la connessione a Kaspersky Security Center. Questa porta deve corrispondere alla porta specificata in Kaspersky Security Center.

- **Protocollo dei messaggi o tipo di origine**

  Protocollo utilizzato per esportare gli eventi nel sistema SIEM. Può essere uno dei protocolli standard: Syslog, CEF o LEEF. Il sistema SIEM seleziona il parser dei messaggi in base al protocollo specificato.

A seconda del sistema SIEM in uso, potrebbe essere necessario specificare alcune impostazioni aggiuntive del ricevitore.

La figura seguente mostra la schermata di configurazione del ricevitore in ArcSight.



Configurazione del ricevitore in ArcSight

Parser dei messaggi

Gli eventi esportati vengono inviati ai sistemi SIEM come messaggi. Questi messaggi devono essere analizzati correttamente per consentire l'utilizzo delle informazioni sugli eventi nel sistema SIEM. I parser dei messaggi fanno parte del sistema SIEM: vengono utilizzati per suddividere il contenuto del messaggio nei campi appropriati, ad esempio l'ID degli eventi, il livello di criticità, la descrizione, i parametri. Questo consente al sistema SIEM di elaborare gli eventi ricevuti da Kaspersky Security Center in modo che possano essere memorizzati nel database del sistema SIEM.

Contrassegno degli eventi per l'esportazione nei sistemi SIEM in formato Syslog

Dopo aver abilitato l'esportazione automatica degli eventi, è necessario selezionare gli eventi da esportare nel sistema SIEM esterno.

È possibile configurare l'esportazione degli eventi in formato Syslog in un sistema esterno in base alle seguenti condizioni:

- Contrassegno di eventi generali. Se si contrassegnano gli eventi da esportare in un criterio, nelle impostazioni di un evento o nelle impostazioni di Administration Server, il sistema SIEM riceverà gli eventi contrassegnati che si sono verificati in tutte le applicazioni gestite dal criterio specifico. Se sono stati selezionati eventi esportati nel criterio, non sarà possibile ridefinirli per una singola applicazione gestita da questo criterio.

- Contrassegno degli eventi per un'applicazione gestita. Se si contrassegnano gli eventi da esportare per un'applicazione gestita installata in un dispositivo gestito, il sistema SIEM riceverà solo gli eventi che si sono verificati nell'applicazione.

Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog

Se si desidera esportare gli eventi che si sono verificati in una singola applicazione gestita installata in un dispositivo gestito, contrassegnare gli eventi per l'esportazione per l'applicazione. Se sono stati contrassegnati eventi esportati in precedenza nel criterio, non sarà possibile ridefinire gli eventi contrassegnati per una singola applicazione gestita da questo criterio.

Per contrassegnare gli eventi per l'esportazione per una singola applicazione gestita:

1. Nella struttura della console di Kaspersky Security Center selezionare il nodo **Dispositivi gestiti** e passare alla scheda **Dispositivi**.

2. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida del dispositivo desiderato, quindi selezionare **Proprietà**.

3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la sezione **Applicazioni**.

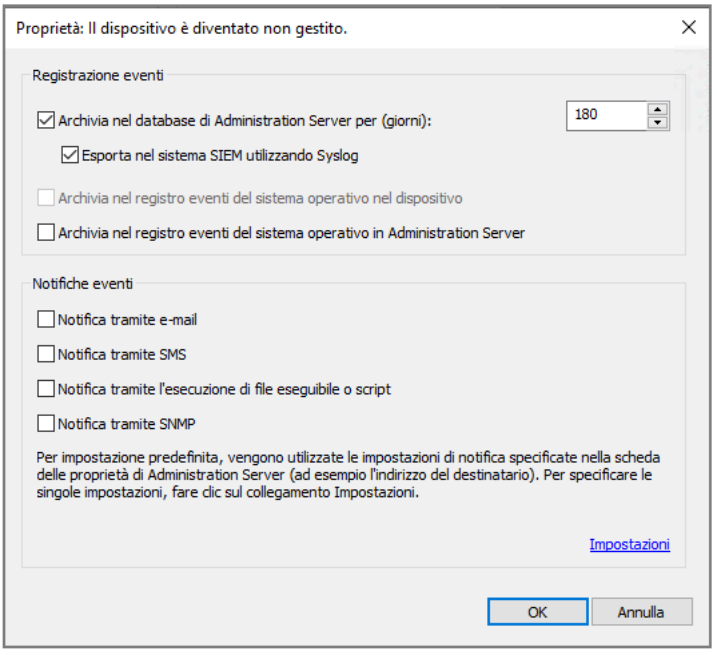
4. Nell'elenco delle applicazioni visualizzato selezionare l'applicazione di cui si desidera esportare gli eventi e fare clic sul pulsante **Proprietà**.

5. Nella finestra delle proprietà dell'applicazione selezionare la sezione **Configurazione eventi**.

6. Nell'elenco degli eventi visualizzato selezionare uno o più eventi che devono essere esportati nel sistema SIEM e fare clic sul pulsante **Proprietà**.

7. Nella finestra delle proprietà dell'evento visualizzata selezionare la casella di controllo **Esporta nel sistema SIEM utilizzando Syslog** per contrassegnare gli eventi selezionati per l'esportazione in formato Syslog. Deselezionare la casella di controllo **Esporta nel sistema SIEM utilizzando Syslog** per rimuovere il contrassegno dagli eventi selezionati per l'esportazione nel formato Syslog.

   Se in un criterio sono definite proprietà degli eventi, i campi di questa finestra non possono essere modificati.



Finestra Proprietà evento

8. Fare clic su **OK** per salvare le modifiche.

9. Fare clic su **OK** nella finestra delle proprietà dell'applicazione e nella finestra delle proprietà del dispositivo.

Gli eventi contrassegnati verranno inviati al sistema SIEM nel formato Syslog. Gli eventi per i quali è stata deselezionata la casella di controllo **Esporta nel sistema SIEM utilizzando Syslog**, non verranno esportati in un sistema SIEM. L'esportazione inizierà non appena si attiva l'esportazione automatica e si selezionano gli eventi da esportare. Configurare il sistema SIEM per fare in modo che riceva gli eventi da Kaspersky Security Center.

Contrassegno di eventi generici per l'esportazione nel formato Syslog

Se si desidera esportare gli eventi che si sono verificati in tutte le applicazioni gestite in base a un criterio specifico, contrassegnare gli eventi da esportare nel criterio. In questo caso, non è possibile contrassegnare gli eventi per una singola applicazione gestita.

Per contrassegnare eventi generici per l'esportazione in un sistema SIEM:

1. Nella struttura della console di Kaspersky Security Center selezionare il nodo **Criteri**.

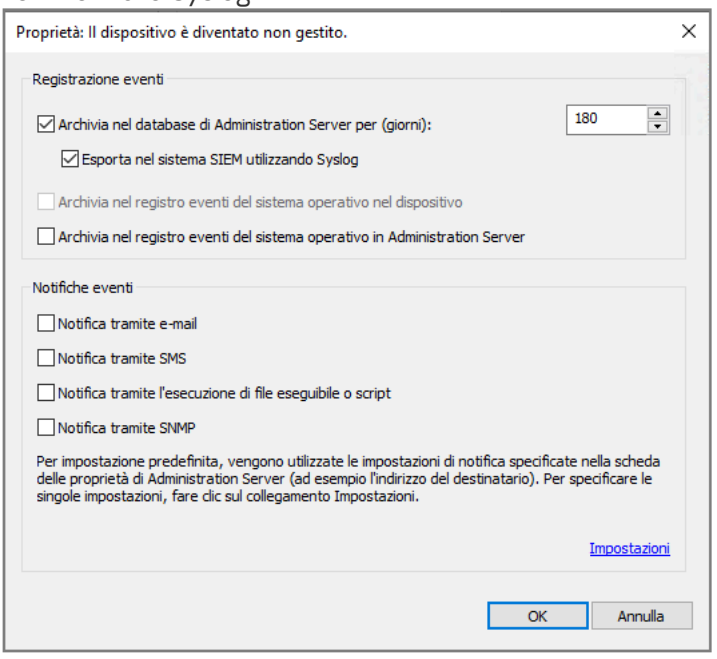
2. Fare clic con il pulsante destro del mouse per aprire il menu di scelta rapida del criterio desiderato, quindi selezionare **Proprietà**.

3. Nella finestra delle proprietà del criterio visualizzata selezionare la sezione **Configurazione eventi**.

4. Nell'elenco degli eventi visualizzato selezionare uno o più eventi che devono essere esportati nel sistema SIEM e fare clic sul pulsante **Proprietà**.

   Se è necessario selezionare tutti gli eventi, fare clic sul pulsante **Seleziona tutto**.

5. Nella finestra delle proprietà dell'evento visualizzata selezionare la casella di controllo **Esporta nel sistema SIEM utilizzando Syslog** per contrassegnare gli eventi selezionati per l'esportazione in formato Syslog. Deselezionare la casella di controllo **Esporta nel sistema SIEM utilizzando Syslog** per rimuovere il contrassegno dagli eventi selezionati per l'esportazione in formato Syslog.



Finestra delle proprietà degli eventi di Administration Server

6. Fare clic su **OK** per salvare le modifiche.

7. Nella finestra delle proprietà del criterio fare clic su **OK**.

Gli eventi contrassegnati verranno inviati al sistema SIEM nel formato Syslog. Gli eventi per i quali è stata deselezionata la casella di controllo **Esporta nel sistema SIEM utilizzando Syslog**, non verranno esportati in un sistema SIEM. L'esportazione inizierà non appena si attiva l'esportazione automatica e si selezionano gli eventi da esportare. Configurare il sistema SIEM per fare in modo che riceva gli eventi da Kaspersky Security Center.

Informazioni sull'esportazione degli eventi utilizzando il formato Syslog

È possibile utilizzare il formato Syslog per esportare nei sistemi SIEM gli eventi che si verificano in Administration Server e in altre applicazioni Kaspersky installate nei dispositivi gestiti.

Syslog è un protocollo standard per la registrazione dei messaggi. Consente una separazione tra il software che genera i messaggi, il sistema che li archivia e il software che li segnala e li analizza. Ogni messaggio dispone di un codice che indica il tipo di software che ha generato il messaggio e di un livello di criticità.

Il formato Syslog è definito dai documenti RFC (Request for Comments) pubblicati da Internet Engineering Task Force (standard Internet). Per l'esportazione degli eventi da Kaspersky Security Center nei sistemi esterni viene utilizzato lo standard RFC 5424.

In Kaspersky Security Center è possibile configurare l'esportazione degli eventi per i sistemi esterni tramite il formato Syslog.

Il processo di esportazione comprende due passaggi:

1. Abilitazione dell'esportazione automatica degli eventi. In questo passaggio Kaspersky Security Center viene configurato in modo da inviare gli eventi al sistema SIEM. Kaspersky Security Center inizia a inviare gli eventi subito dopo l'abilitazione dell'esportazione automatica.

2. Selezione degli eventi da esportare nel sistema esterno. In questo passaggio è possibile selezionare gli eventi da esportare nel sistema SIEM.

Informazioni sull'esportazione degli eventi tramite i formati CEF e LEEF

È possibile utilizzare i formati CEF e LEEF per esportare nei sistemi SIEM gli eventi generali, nonché gli eventi trasferiti dalle applicazioni Kaspersky ad Administration Server. Il set di eventi per l'esportazione è predefinito e non è possibile selezionare gli eventi da esportare. Prima di inviare eventi al sistema SIEM (QRadar, ArcSight o Splunk), è necessario interpretare gli eventi Kaspersky Security Center in eventi in formato CEF e LEEF utilizzando le regole specificate nel file siem_conversion_rules.xml.

Selezionare il formato di esportazione in base al sistema SIEM in uso. Nella tabella seguente sono elencati i sistemi SIEM e i formati di esportazione corrispondenti.

Formati di esportazione degli eventi in un sistema SIEM

Sistema SIEM	Formato di esportazione
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - un formato di eventi personalizzato per IBM Security QRadar SIEM. QRadar può integrare, identificare ed elaborare gli eventi LEEF. Gli eventi LEEF devono utilizzare la codifica dei caratteri UTF-8. Informazioni dettagliate sul protocollo LEEF sono disponibili in IBM Knowledge Center.

- CEF (Common Event Format) è uno standard aperto per la gestione dei registri che migliora l'interoperabilità delle informazioni relative alla sicurezza ottenute da diversi dispositivi e applicazioni di rete e di protezione. CEF consente di utilizzare un formato comune per il registro eventi, permettendo di integrare e aggregare facilmente i dati per l'analisi da un sistema di gestione aziendale. Gli eventi CEF devono utilizzare la codifica dei caratteri UTF-8.

L'esportazione automatica significa che Kaspersky Security Center invii gli eventi generali al sistema SIEM. L'esportazione automatica degli eventi viene avviata subito dopo essere stata abilitata. In questa sezione viene descritto in dettaglio come abilitare l'esportazione automatica degli eventi.

Configurazione di Kaspersky Security Center per l'esportazione degli eventi nel sistema SIEM

È possibile abilitare l'esportazione automatica degli eventi in Kaspersky Security Center.

È possibile esportare solo gli eventi generali dalle applicazioni gestite tramite i formati CEF e LEEF. Le regole di interpretazione utilizzate per convertire gli eventi nei formati CEF e LEEF sono specificate nel file siem_conversion_rules.xml incluso nel kit di distribuzione Kaspersky Security Center. Gli eventi specifici delle applicazioni non possono essere esportati dalle applicazioni gestite tramite i formati CEF e LEEF. Se si desidera esportare gli eventi delle applicazioni gestite o un set di eventi personalizzato che è stato configurato tramite i criteri delle applicazioni gestite, è necessario esportare gli eventi nel formato Syslog.

Per abilitare l'esportazione automatica degli eventi:

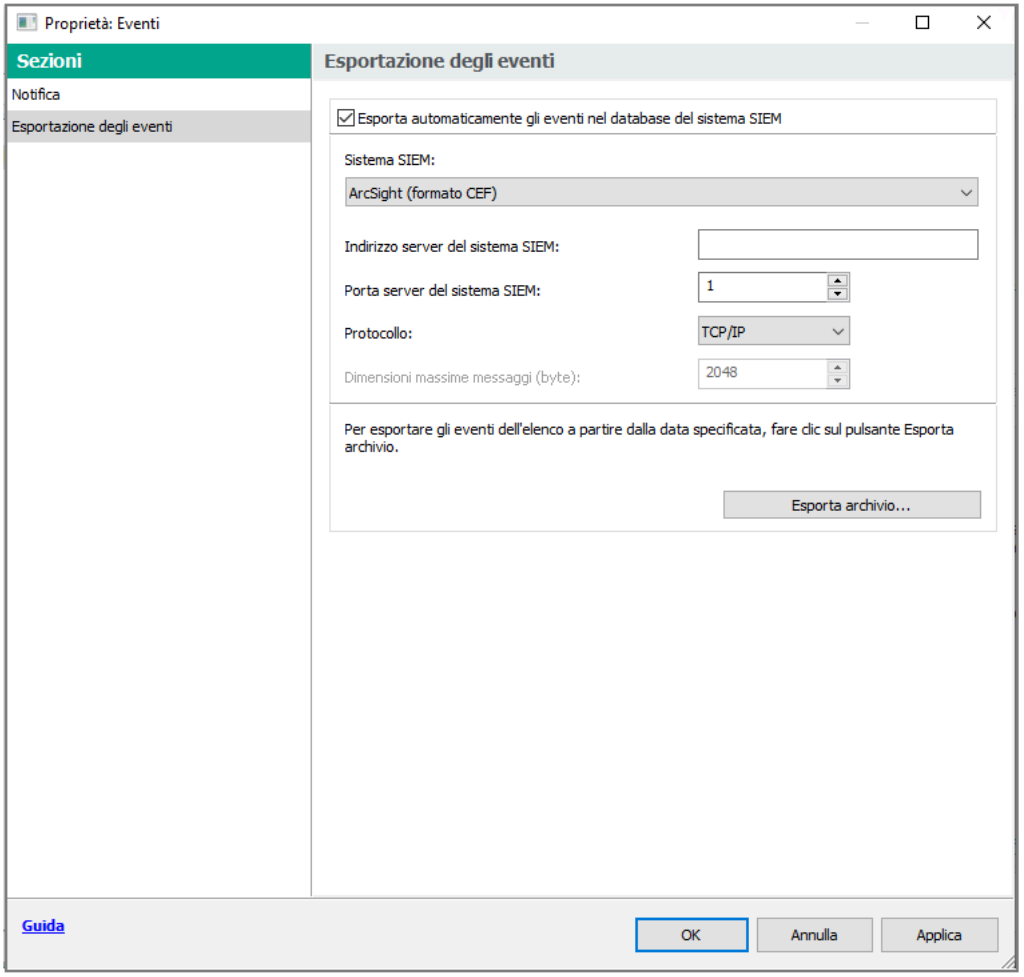
1. Nella struttura della console di Kaspersky Security Center, selezionare l'Administration Server per cui si desidera esportare gli eventi.

2. Nell'area di lavoro dell'Administration Server selezionato, selezionare la scheda **Eventi**.

3. Fare clic sulla freccia a discesa accanto al collegamento **Configura notifiche ed esportazione eventi** e selezionare **Configura esportazione nel sistema SIEM** nell'elenco a discesa.

   Verrà visualizzata la finestra delle proprietà degli eventi, con la sezione **Esportazione degli eventi** visualizzata.

4. Nella sezione **Esportazione degli eventi** specificare le seguenti impostazioni di esportazione:



Sezione di esportazione degli eventi della finestra delle proprietà dell'evento

- **Esporta automaticamente gli eventi nel database del sistema SIEM**

  Selezionare questa casella di controllo per abilitare l'esportazione automatica degli eventi nei sistemi SIEM. Selezionando questa casella di controllo vengono abilitati tutti i campi nella sezione **Esportazione degli eventi**.

- **Sistema SIEM**

  Selezionare il sistema SIEM per l'esportazione degli eventi: QRadar® (formato LEEF), ArcSight (formato CEF), Splunk® (formato CEF) e formato Syslog (RFC 5424).

  Se si seleziona il formato Syslog, è necessario specificare:

  Dimensioni massime messaggi, in byte

  Specificare la dimensione massima (in byte) di un messaggio inviato al sistema SIEM. Ciascun evento viene inviato in un messaggio. Se la durata effettiva di un messaggio è superiore al valore specificato, il messaggio viene troncato e può verificarsi una perdita di dati. Le dimensioni predefinite sono 2048 byte. Questo campo è disponibile solo se stato è selezionato il formato Syslog nel campo **Sistema SIEM**.

- **Indirizzo server del sistema SIEM**

Specificare l'indirizzo server del sistema SIEM. Un indirizzo può essere specificato come nome DNS o NetBIOS o come indirizzo IP.

- **Porta server del sistema SIEM**

  Specificare il numero della porta per la connessione al server del sistema SIEM. Il numero della porta deve essere identico a quello utilizzato dal sistema SIEM per ricevere gli eventi (per informazioni dettagliate vedere la sezione Configurazione di un sistema SIEM).

- **Protocollo**

Selezionare il protocollo da utilizzare per il trasferimento dei messaggi al sistema SIEM. È possibile selezionare il protocollo TCP, UDP o TLS su TCP.

Specificare le seguenti impostazioni TLS se si seleziona il protocollo TLS su TCP:

- **Autenticazione server SIEM**

  Scegliere uno dei seguenti modi per autenticare il server di sistema SIEM:

  - **Utilizzando i certificati dell'autorità di certificazione**. È possibile ricevere un file con un elenco dei certificati da un'autorità di certificazione (CA) attendibile e caricare il file in Kaspersky Security Center. Kaspersky Security Center verifica se anche il certificato del server di sistema SIEM è firmato da un'autorità di certificazione attendibile o meno.

    Per aggiungere un certificato attendibile, fare clic sul pulsante **Sfoglia**, quindi caricare il certificato.

    Se si seleziona l'opzione **Utilizzando i certificati dell'autorità di certificazione**, è possibile specificare i nomi dei soggetti nel campo **Soggetti dei certificati server (facoltativo)**. Il *nome del soggetto* è un nome di dominio per il quale viene ricevuto il certificato. Kaspersky Security Center non può connettersi al server di sistema SIEM se il nome di dominio del server di sistema SIEM non corrisponde al nome del soggetto del certificato del server di sistema SIEM. Tuttavia, il server di sistema SIEM può modificare il proprio nome di dominio se si modifica il nome del soggetto nel certificato. A tale scopo, specificare i nomi dei soggetti nel campo **Soggetti dei certificati server (facoltativo)**. Se uno dei nomi dei soggetti specificati corrisponde al nome del soggetto del certificato di sistema SIEM, Kaspersky Security Center convalida il certificato del server di sistema SIEM.

  - **Utilizzando le identificazioni personali SHA-1 dei certificati server**. È possibile specificare le identificazioni personali SHA-1 dei certificati di sistema SIEM in Kaspersky Security Center Cloud Console. Per aggiungere un'identificazione personale SHA-1, inserirla nel campo sotto l'opzione.

- **Autenticazione client**

  Per l'autenticazione del client, è possibile inserire il certificato o generarlo in Kaspersky Security Center.

  - **Inserire il certificato**. È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. Per inserire un certificato esistente, fare clic sul pulsante **Cerca certificato**. Nella finestra **Certificato** visualizzata, scegliere uno dei seguenti tipi di certificato, quindi specificare il certificato e la relativa chiave privata:

    - **Certificato X.509**. Caricare un file con una chiave privata nel campo **Chiave privata (*.prk, *.pem)** e un file con un certificato nel campo **Certificato (*.cer)**. A tale scopo, fare clic sul pulsante **Sfoglia** a destra del campo corrispondente, quindi aggiungere il file richiesto. Entrambi i file non dipendono l'uno dall'altro e l'ordine di caricamento dei file non è significativo. Dopo aver caricato entrambi i file, specificare la password per la decodifica della chiave privata nel campo **Password**. La password può avere un valore vuoto se la chiave privata non è codificata.

    - **Contenitore PKCS #12**. Caricare un singolo file che contenga un certificato e la relativa chiave privata nel campo **File di certificato**. A tale scopo, fare clic sul pulsante **Sfoglia** a destra del campo, quindi aggiungere il file richiesto. Dopo aver caricato il file, specificare la password per la decodifica della chiave privata nel campo **Password**. La password può avere un valore vuoto se la chiave privata non è codificata.

  - **Generare la chiave**. È possibile generare un certificato autofirmato in Kaspersky Security Center. Fare clic sul pulsante **Genera certificato**, quindi immettere un nome per il soggetto nel campo **Oggetto**. Il certificato client viene generato per questo nome del soggetto e l'identificazione personale SHA-1 di questo certificato viene visualizzata nel campo **Identificazione personale SHA-1 del certificato client**. Di conseguenza, Kaspersky Security Center archivia il certificato

autofirmato generato ed è possibile passare la parte pubblica del certificato o l'identificazione SHA-1 al sistema SIEM.

5. Se si desidera esportare nel database del sistema SIEM gli eventi che si verificavano dopo una data specificata in precedenza, fare clic sul pulsante **Esporta archivio** e specificare la data di avvio dell'esportazione degli eventi. Per impostazione predefinita, l'esportazione degli eventi viene avviata subito dopo l'abilitazione.

6. Per verificare che la connessione al sistema SIEM sia configurata, fare clic sul pulsante **Verifica impostazioni**.

   L'applicazione tenta di stabilire una connessione con il server del sistema SIEM e di inviare un evento di verifica. Se la connessione non viene stabilita, viene visualizzato un messaggio di errore. Se la connessione viene stabilita, non viene visualizzato alcun messaggio. È possibile visualizzare l'evento di test nella scheda **Eventi**, se necessario.

7. Fare clic su **OK**.

L'esportazione automatica degli eventi è abilitata.

Dopo aver abilitato l'esportazione automatica degli eventi, è necessario selezionare gli eventi da esportare nel sistema SIEM.

Esportazione degli eventi direttamente dal database

È possibile recuperare gli eventi direttamente dal database di Kaspersky Security Center senza dover utilizzare l'interfaccia di Kaspersky Security Center. È possibile eseguire direttamente le query sulle visualizzazioni pubbliche e recuperare i dati degli eventi o creare le proprie visualizzazioni sulla base delle visualizzazioni pubbliche esistenti e configurarle in modo che recuperino i dati necessari.

Visualizzazioni pubbliche

Per maggiore praticità, è disponibile un set di visualizzazioni pubbliche nel database di Kaspersky Security Center. È possibile trovare la descrizione di queste visualizzazioni pubbliche nel documento klakdb.chm.

La visualizzazione pubblica v_akpub_ev_event contiene un set di campi che rappresentano i parametri degli eventi nel database. Nel documento klakdb.chm è inoltre possibile trovare informazioni sulle visualizzazioni pubbliche che corrispondono ad altre entità di Kaspersky Security Center, ad esempio dispositivi, applicazioni o utenti. È possibile utilizzare queste informazioni nelle query.

Questa sezione contiene le istruzioni per l'esecuzione di una query SQL tramite l'utilità klsql2 e un esempio di query.

Per creare query SQL o visualizzazioni di database, è anche possibile utilizzare qualsiasi altro programma per l'utilizzo dei database. Le informazioni su come visualizzare i parametri per la connessione al database di Kaspersky Security Center, ad esempio il nome istanza e il nome database, sono indicate nella sezione corrispondente.

Esecuzione di una query SQL tramite l'utilità klsql2

Questo articolo descrive come scaricare e utilizzare l'utilità klsql2 e come eseguire una query SQL utilizzando questa utilità.

Per utilizzare l'utilità klsql2:

1. Individuare l'utilità klsql2 nella cartella di installazione di Kaspersky Security Center. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center. Non utilizzare le versioni dell'utilità klsql2 destinate alle versioni precedenti di Kaspersky Security Center.

2. Creare un file con l'estensione .sql in qualsiasi editor di testo e posizionare il file nella stessa cartella con l'utilità.

3. Nel file .sql creato, digitare la query SQL desiderata e salvare il file.

4. Nel dispositivo in cui è installato Kaspersky Security Center Administration Server digitare nella riga di comando il seguente comando per eseguire la query SQL dal file .sql e salvare i risultati nel file result.xml:
   `klsql2 -i src.sql -u <nome utente> -p <password> -o result.xml`
   dove `<nome utente>` e `<password>` sono le credenziali dell'account utente che ha accesso al database.

5. Se richiesto, inserire account utente e password dell'account utente che ha accesso al database.

6. Aprire i file result.xml creati per visualizzare i risultati della query SQL.

È possibile modificare il file .sql e creare qualsiasi query SQL sulle visualizzazioni pubbliche. Eseguire la query SQL dalla riga di comando e salvare i risultati in un file.

Esempio di una query SQL nell'utilità klsql2

Questa sezione fornisce un esempio di query SQL, eseguita tramite l'utilità klsql2.

I seguenti esempi illustrano il recupero degli eventi che si sono verificati nei dispositivi negli ultimi sette giorni e la visualizzazione degli eventi ordinati in base all'ora in cui si sono verificati. Gli eventi più recenti vengono visualizzati per primi.

Esempio per Microsoft SQL Server:

```
SELECT
  /* identificatore dell'evento */
  e.nId,

  /* ora in cui si è verificato l'evento */
  e.tmRiseTime,

  /* nome interno del tipo di evento */
  e.strEventType,

  /* nome visualizzato dell'evento */
  e.wstrEventTypeDisplayName,

  /* descrizione visualizzata dell'evento */
  e.wstrDescription,

  /* nome del gruppo a cui appartiene il dispositivo */
  e.wstrGroupName,

  /* nome visualizzato del dispositivo in cui si è verificato l'evento */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* indirizzo IP del dispositivo, in cui si è verificato l'evento */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Esempio per PostgreSQL:

```
SELECT
  /* identificatore dell'evento */
  "e"."nId",

  /* ora in cui si è verificato l'evento */
  "e"."tmRiseTime",

  /* nome interno del tipo di eventoe */
  "e"."strEventType",

  /* nome visualizzato dell'evento*/
  "e"."wstrEventTypeDisplayName",

  /* descrizione visualizzata dell'evento */
  "e"."wstrDescription",

  /* descrizione visualizzata dell'evento */
  "e"."wstrGroupName",

  /* nome visualizzato del dispositivo in cui si è verificato l'evento */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* indirizzo IP del dispositivo, in cui si è verificato l'evento */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Esempio per MySQL o MariaDB:

```
SELECT

  /* identificatore dell'evento */
  `e`.`nId`,

  /* ora in cui si è verificato l'evento */
  `e`.`tmRiseTime`,

  /* nome interno del tipo di eventoe */
  `e`.`strEventType`,

  /* nome visualizzato dell'evento */
  `e`.`wstrEventTypeDisplayName`,

  /* descrizione visualizzata dell'evento */
  `e`.`wstrDescription`,

  /* nome del gruppo di dispositivi */
  `e`.`wstrGroupName`,

  /* nome visualizzato del dispositivo in cui si è verificato l'evento */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* indirizzo IP del dispositivo, in cui si è verificato l'evento */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Visualizzazione del nome del database di Kaspersky Security Center

Può essere utile conoscere il nome di un database se è necessario, ad esempio, inviare una query SQL e connettersi al database dall'editor di script SQL.

Per visualizzare il nome del database di Kaspersky Security Center:

1. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server** e selezionare **Proprietà**.

2. Nella finestra delle proprietà di Administration Server, nel riquadro Sezioni selezionare **Avanzate**, quindi **Dettagli del database corrente**.

3. Nella sezione **Dettagli del database corrente** esaminare le seguenti proprietà del database (vedere la figura di seguito):

- **Nome istanza**

  Nome dell'istanza di database di Kaspersky Security Center corrente. Il valore predefinito è *.\KAV_CS_ADMIN_KIT*.

- **Nome database**

  Nome del database SQL Kaspersky Security Center. Il valore predefinito è *KAV*.

- **Spazio allocato per il database di Kaspersky Security Center**

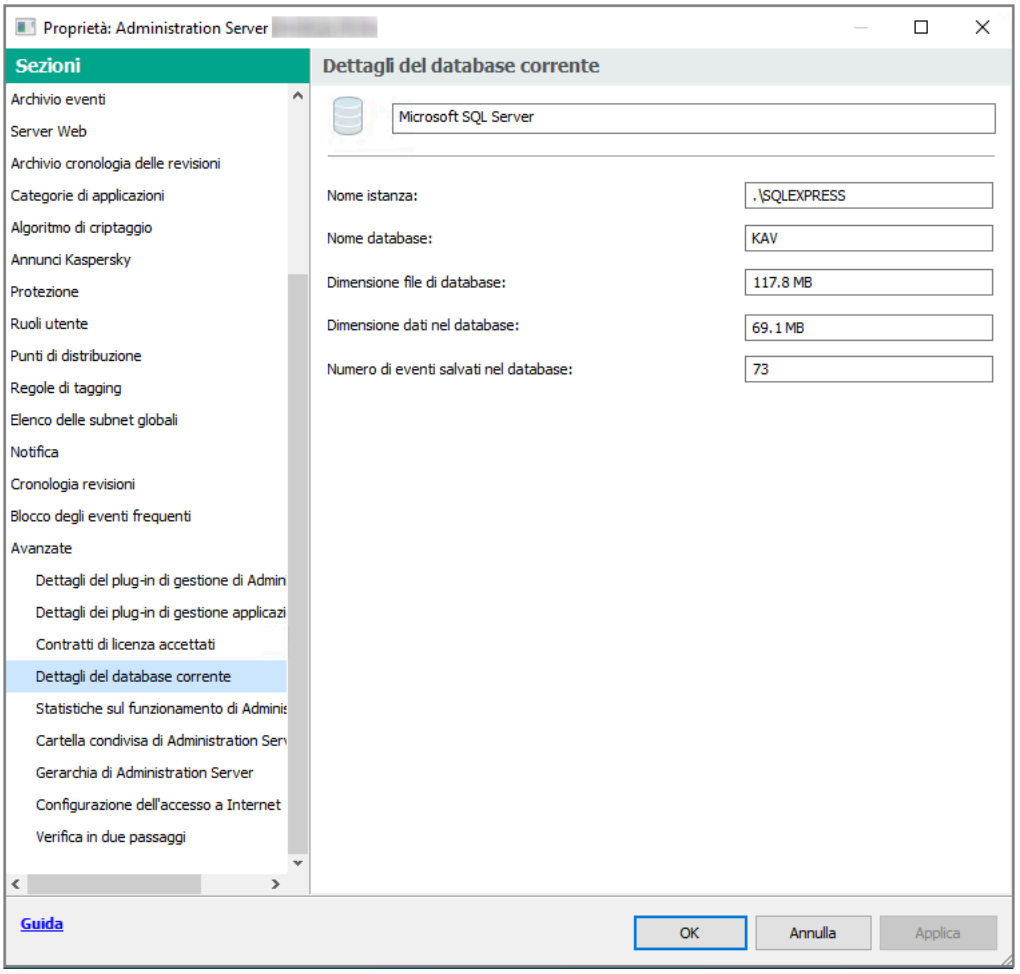
  La dimensione del file del database. Se si desidera ripulire i dati non necessari, configurare la compressione del database tramite l'attività *Manutenzione di Administration Server*.

- **Dimensione dei dati nell'intero database**

  La dimensione effettiva dei dati attualmente utilizzati nel DBMS. Il seguente articolo descrive come diagnosticare il DBMS: La dimensione del database supera il limite.

- **Numero di eventi salvati nel database**

Numero di eventi attualmente archiviati nel DBMS. Per maggiori dettagli, fare riferimento al seguente articolo: Elaborazione e archiviazione degli eventi.



Sezione con le informazioni sul database corrente di Administration Server

4. Fare clic sul pulsante **OK** per chiudere la finestra delle proprietà di Administration Server.

Utilizzare il nome del database per fare riferimento al database nelle query SQL.

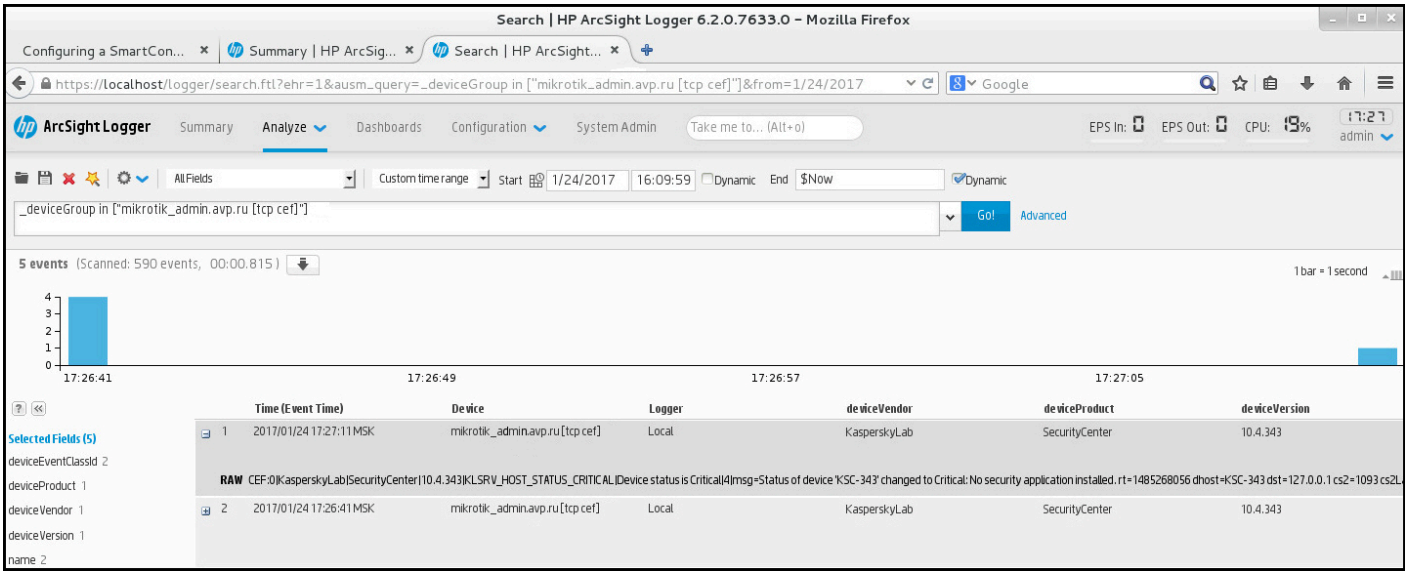
Visualizzazione dei risultati dell'esportazione

È possibile controllare il completamento della procedura di esportazione degli eventi. A tale scopo, controllare se i messaggi con gli eventi esportati vengono ricevuti dal sistema SIEM.

Se gli eventi inviati da Kaspersky Security Center vengono ricevuti e analizzati correttamente dal sistema SIEM, la configurazione su entrambi i lati è stata eseguita correttamente. In caso contrario, controllare le impostazioni specificate in Kaspersky Security Center rispetto alla configurazione del sistema SIEM.

La figura seguente illustra gli eventi esportati in ArcSight. Ad esempio, il primo evento è un evento critico di Administration Server: "*Lo stato del dispositivo è Critico*".

La rappresentazione degli eventi esportati nel sistema SIEM varia in base al sistema SIEM in uso.



Esempio di eventi

Utilizzo di SNMP per l'invio di statistiche ad applicazioni di terze parti

In questa sezione viene descritto come ottenere informazioni da Administration Server utilizzando il protocollo SNMP (Simple Network Management Protocol) in Windows. Kaspersky Security Center contiene l'agente SNMP, che trasferisce le statistiche delle prestazioni di Administration Server alle applicazioni secondarie utilizzando gli OID.

Questa sezione contiene inoltre informazioni sulla risoluzione dei problemi che potrebbero verificarsi durante l'utilizzo del protocollo SNMP per Kaspersky Security Center.

Configurazione del servizio SNMP per l'utilizzo con Kaspersky Security Center

Questa sezione descrive come configurare il servizio SNMP in Windows per ottenere informazioni da Administration Server utilizzando Simple Network Management Protocol (SNMP).

Il supporto SNMP è disabilitato per impostazione predefinita su Windows.

Per abilitare il supporto SNMP in Windows:

1. Accedere al **Pannello di controllo**.
2. Aprire il menu **Disinstalla o modifica programma**.
3. Fare clic su **Attivazione o disattivazione delle funzionalità Windows**.
4. Nell'elenco delle funzionalità Windows accedere alla funzionalità SNMP e fare clic su **OK**.

5. Accedere a **Pannello di controllo** → **Strumenti di amministrazione** → **Servizi**.

6. Scegliere il **servizio SNMP** ed eseguirlo.

7. Verificare se l'ascolto funziona testandolo con `netstat` per una porta UDP standard.

Il supporto SNMP è abilitato in Windows.

Per configurare i servizi SNMP in Windows:

1. Verificare che il componente **Agente SNMP** di Kaspersky Security Center sia stato installato durante l'installazione normale o automatica.

2. Verificare che i servizi **SNMP Service** e **SNMP Trap** di Windows siano in esecuzione.

3. Verificare che ManageEngine MIB Browser sia installato nel sistema.

4. Nelle proprietà del servizio **SNMP Service**, nella scheda **Sicurezza**, aggiungere due community con i seguenti diritti:

Community	Diritti
`kaspersky`	`NOTIFY`
`public`	`READ WRITE`

5. Nel campo **Accetta pacchetti SNMP da questi host**, aggiungere l'indirizzo IP del dispositivo in cui è installato ManageEngine MIB Browser, ad esempio 10.10.10.105.

6. Nella scheda **Trap**, digitare `kaspersky` nel campo **Nome community**.

7. Fare clic su **OK** per salvare le modifiche e chiudere la finestra delle proprietà del servizio.

8. In ManageEngine MIB Browser, caricare il file adminkit.mib dalla cartella di installazione di Kaspersky Security Center. Per impostazione predefinita, il file adminkit.mib si trova nella cartella <Disco>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp.

9. Nel campo **Host** della finestra di MIB ManageEngine Browser, aggiungere l'indirizzo IP del dispositivo in cui è installato Kaspersky Security Center Administration Server.

Il servizio SNMP è configurato per ottenere informazioni da Administration Server utilizzando Simple Network Management Protocol (SNMP).

Agente SNMP e identificatori oggetto

Per Kaspersky Security Center, l'agente SNMP viene implementato come libreria dinamica `klsnmpag.dll`, registrata dal programma di installazione durante l'installazione di Administration Server. L'agente SNMP opera all'interno del processo `snmp.exe` (servizio di Windows). Le applicazioni di terze parti utilizzano SNMP per ricevere statistiche, sotto forma di contatori, sulle prestazioni di Administration Server.

Ogni contatore ha un *identificatore oggetto* univoco (denominato anche OID). Un identificatore oggetto è una sequenza di numeri separati da punti. Gli identificatori oggetto di Administration Server iniziano con il prefisso 1.3.6.1.4.1.23668.1093. L'OID del contatore è una concatenazione di tale prefisso con un suffisso che descrive il contatore. Ad esempio, il contatore con il valore OID 1.3.6.1.4.1.23668.1093.1.1.4 ha il suffisso con il valore 1.1.4.

È possibile utilizzare un client SNMP (come Zabbix) per monitorare lo stato del sistema. Per ottenere le informazioni, è possibile cercare un valore di OID corrispondente alle informazioni e immettere tale valore nel client SNMP. Il client SNMP restituirà quindi un altro valore che caratterizza lo stato del sistema.

L'elenco dei contatori e dei tipi di contatori si trova nel file `adminkit.mib` in Administration Server. *MIB* è l'acronimo di Management Information Base. È possibile importare e analizzare i file `.mib` tramite l'applicazione MIB Viewer, progettata per richiedere e visualizzare i valori del contatore.

Ottenere un nome di contatore di stringhe da un identificatore oggetto

Per utilizzare un identificatore oggetto (OID) per il trasferimento delle informazioni ad applicazioni di terze parti, potrebbe essere necessario ottenere un nome di contatore di stringhe da tale OID.

Per ottenere un nome di contatore di stringhe da un OID:

1. Aprire il file `adminkit.mib`, disponibile in Administration Server, in un editor di testo.
2. Individuare lo spazio dei nomi che descrive il primo valore (da sinistra a destra).

   Ad esempio, per il suffisso OID 1.1.4 sarebbe `"counters" (::= { kladminkit 1 })`.
3. Individuare lo spazio dei nomi che descrive il secondo valore.

   Ad esempio, per il suffisso OID 1.1.4 sarebbe `counters 1`, che sta per `deployment`.
4. Individuare lo spazio dei nomi che descrive il terzo valore.

   Ad esempio, per il suffisso OID 1.1.4 sarebbe `deployment 4`, che sta per `hostsWithAntivirus`.

Il nome del contatore di stringhe è la concatenazione di questi valori, ad esempio `<MIB base namespace>.counters.deployment.hostsWithAntivirus` e corrisponde all'OID con il valore 1.3.6.1.4.1.23668.1093.1.1.4.

Valori degli identificatori oggetto per SNMP

La tabella seguente mostra i valori e le descrizioni degli identificatori oggetto (denominati anche OID), utilizzati per trasferire le informazioni sulle prestazioni di Administration Server ad applicazioni di terze parti.

Valori e descrizioni degli identificatori oggetto per SNMP

Valore dell'identificatore oggetto	Tipo di dati numerici	OID	Descrizione
deploymentStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.1.1	Stato della distribuzione. Lo stato può essere uno dei seguenti: • **Informazioni**. La licenza non è più valida per N dispositivi. • **Avviso**. Uno dei seguenti elementi: Ci sono M dispositivi in cui sono installate applicazioni Kaspersky su un totale di N dispositivi nei gruppi di Administration Server (N > M). La licenza L scadrà in N dispositivi tra M giorni. L'attività T di installazione delle applicazioni è stata completata in N dispositivi. È necessario riavviare per M dispositivi. • **Critico**. Licenza scaduta per N dispositivi. • **OK**. Nessuno dei precedenti.
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	Il motivo deploymentStatus mostra che il gruppo Administration Server contiene troppi dispositivi senza applicazioni gestite. Il valore è uguale a 1 nel caso in cui siano stati rilevati alcuni dispositivi senza applicazioni gestite e 0 in caso contrario.
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	Il motivo deploymentStatus mostra che l'attività di installazione remota non è riuscita in alcuni dispositivi. Il numero di questi dispositivi può essere ottenuto tramite hostsRemoteInstallFailed.
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	Il motivo deploymentStatus mostra che ci sono alcuni dispositivi con una licenza in scadenza nei 7 giorni successivi. Il numero di tali dispositivi può essere ottenuto tramite hostsLicenseExpiring.
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	Il motivo deploymentStatus mostra che ci sono alcuni dispositivi con una licenza scaduta. È possibile ottenere il numero di questi dispositivi tramite hostsLicenseExpired.
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	Numero di dispositivi nei gruppi di Administration Server.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	Numero di dispositivi nei gruppi di Administration Server con applicazioni gestite installate.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	Numero di dispositivi in cui l'attività di installazione remota non è riuscita.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	ID di una chiave di licenza in scadenza (tra meno di 7 giorni).
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	ID della chiave di licenza scaduta.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	Numero di giorni mancanti alla scadenza della licenza. Per questo parametro, il periodo di licenza è considerato scaduto se mancano meno di 7 giorni alla data di scadenza. Se mancano più di 7 giorni alla data di scadenza, il valore è 0.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	Numero di dispositivi con una licenza che scade a breve (tra meno di 7 giorni).
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	Numero di dispositivi con una licenza scaduta.

Valore dell'identificatore oggetto	Tipo di dati numerici	OID	Descrizione
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Stato attuale dell'aggiornamento dei database anti-virus. Lo stato può essere uno dei seguenti: • **Informazioni**. Le basi anti-virus in Administration Server o nei dispositivi non sono state aggiornate da più di 1 giorno ed è trascorso meno di 1 giorno dall'installazione dell'applicazione. • **Avviso**. Le basi anti-virus in Administration Server o nei dispositivi non sono state aggiornate da più di 3 giorni. Questo valore può essere modificato nelle impostazioni del gruppo. • **Critico**. Le basi anti-virus in Administration Server o nei dispositivi non sono state aggiornate da più di 7 giorni. Questo valore può essere modificato nelle impostazioni del gruppo. • **OK**. Nessuno dei precedenti.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	Questo motivo mostra che Administration Server non viene aggiornato da molto tempo. Il periodo di tempo considerato lungo è specificato in updatesStatus.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Questo motivo mostra che alcuni dispositivi non vengono aggiornati da molto tempo (per impostazione predefinita, 7 giorni o più per **Critico** e 3 giorni per **Avviso**). È possibile ottenere il numero di questi dispositivi tramite hostsNotUpdated.
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	L'ultima volta in cui i database anti-virus sono stati aggiornati in Administration Server.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Numero di dispositivi contenenti basi anti-virus che non vengono aggiornate da lungo tempo (per impostazione predefinita, 7 giorni o più per **Critico** e 3 giorni per **Avviso**). Se sono presenti dispositivi con lo stato di aggiornamento **Critico**, vengono conteggiati solo questi dispositivi. È possibile ottenere lo stato dell'aggiornamento tramite updatesStatus.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Stato della protezione in tempo reale. Uno dei seguenti elementi: • **Avviso**. Uno dei seguenti elementi: Viene rilevata una violazione della sicurezza in un dispositivo che appartiene al gruppo di Administration Server. Errori di criptaggio hanno determinato il cambiamento dello stato della protezione da parte di alcuni dispositivi. Scansione completa non eseguita da molto tempo. • **Critico**. La protezione anti-virus non funziona su alcuni dispositivi nei gruppi di Administration Server. • **OK**. Nessuno dei precedenti.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Questo motivo mostra che un'applicazione di protezione non è in esecuzione in alcuni dispositivi. È possibile ottenere il numero di tali dispositivi tramite hostsAntivirusNotRunning.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Questo motivo mostra che la protezione in tempo reale non è in esecuzione in alcuni dispositivi. È possibile ottenere il numero di questi dispositivi tramite hostsRealtimeNotRunning.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Questo motivo mostra che sono presenti dispositivi contenenti oggetti non disinfettati. È possibile ottenere il numero di questi dispositivi tramite hostsNotCuredObject.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Questo motivo mostra che sono state rilevate minacce in alcuni dispositivi. È possibile ottenere il numero di questi dispositivi tramite hostsTooManyThreats.

Valore dell'identificatore oggetto	Tipo di dati numerici	OID	Descrizione
virusOutbreak	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.6	Questo motivo mostra lo stato dell'epidemia di virus del sistema. Il valore è 1 se è stata rilevata una determinata quantità di virus durante un certo periodo di tempo, altrimenti è 0. La quantità di virus e la quantità di tempo vengono specificate in Administration Server, utilizzando le impostazioni `Virus attack`.
hostsAntivirusNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.3	Numero di dispositivi con applicazioni di protezione non in esecuzione.
hostsRealtimeNotRunning	Counter32	.1.3.6.1.4.1.23668.1093.1.3.4	Numero di dispositivi in cui la protezione in tempo reale non è in esecuzione.
hostsRealtimeLevelChanged	Counter32	.1.3.6.1.4.1.23668.1093.1.3.5	Numero di dispositivi con livello di protezione in tempo reale non accettabile.
hostsNotCuredObject	Counter32	.1.3.6.1.4.1.23668.1093.1.3.6	Numero di dispositivi contenenti oggetti non disinfettati.
hostsTooManyThreats	Counter32	.1.3.6.1.4.1.23668.1093.1.3.7	Numero di dispositivi contenenti minacce.
fullscanStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.4.1	Stato della scansione anti-virus completa. Uno dei seguenti elementi: • **Informazioni**. Sono trascorsi meno di 7 giorni dal momento dell'installazione dell'applicazione. • **Avviso**. La scansione anti-virus completa non viene eseguita da più di 7 giorni dal momento dell'installazione dell'applicazione. • **Critico**. La scansione anti-virus completa non viene eseguita da più di 14 giorni dal momento dell'installazione dell'applicazione. • **OK**. Nessuno dei precedenti.
notScannedLately	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.4.2.1	Questo motivo mostra che alcuni dispositivi non vengono esaminati da un determinato periodo di tempo. È possibile ottenere il numero di questi dispositivi tramite `hostsNotScannedLately`. La quantità di tempo è specificata in `fullScanStatus`.
hostsNotScannedLately	Counter32	.1.3.6.1.4.1.23668.1093.1.4.3	Numero di dispositivi che non vengono esaminati da un certo periodo di tempo. La quantità di tempo è specificata in `fullScanStatus`.
logicalNetworkStatus	INTEGER { ok(0), warning(1), critical(2) }	.1.3.6.1.4.1.23668.1093.1.5.1	Stato della rete logica di Administration Server. Uno dei seguenti elementi: • **Avviso**. In presenza di dispositivi con uno stato di avviso ai quali non è possibile accedere o in presenza di dispositivi non appartenenti ad alcun gruppo di Administration Server. • **Critico**. In presenza di dispositivi il cui controllo è stato perso da Administration Server o in presenza di dispositivi con uno stato critico e ai quali non è possibile accedere. • **OK**. Nessuno dei precedenti.
notConnectedLongTime	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.1	Questo motivo mostra che alcuni dispositivi non vengono connessi ad Administration Server da molto tempo (7 giorni o più per un dispositivo con stato **Avviso** e 4 giorni per un dispositivo con lo stato **Critico**). È possibile ottenere il numero di questi dispositivi tramite `hostsNotConnectedLongTime`.
controlLost	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.5.2.2	Questo motivo mostra che sono presenti dispositivi il cui controllo è stato perso da Administration Server. È possibile ottenere il numero di questi dispositivi tramite `hostsControlLost`.
hostsFound	Counter32	.1.3.6.1.4.1.23668.1093.1.5.3	Numero di dispositivi rilevati da Administration Server che non appartengono ad alcun gruppo di Administration Server.
groupsCount	Counter32	.1.3.6.1.4.1.23668.1093.1.5.4	Numero di gruppi in Administration Server.

Valore dell'identificatore oggetto	Tipo di dati numerici	OID	Descrizione
`hostsNotConnectedLongTime`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.5	Numero di dispositivi che non vengono connessi ad Administration Server da molto tempo. Il periodo di tempo considerato lungo è specificato in `notConnectedLongTime`.
`hostsControlLost`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.6	Numero di dispositivi non controllati da Administration Server.
`eventsStatus`	`INTEGER { ok(0), warning(1), critical(2) }`	.1.3.6.1.4.1.23668.1093.1.6.1	Sottosistema Stato degli eventi. Uno dei seguenti elementi: • **Avviso**. Uno dei seguenti elementi: I dispositivi del gruppo di Administration Server non cercano aggiornamenti di Windows da molto tempo. Sono presenti dispositivi con problemi di stato. • **Critico**. Uno dei seguenti elementi: È presente un evento di importanza "Critica" in almeno un dispositivo. È presente un evento di importanza "Errore" in almeno un dispositivo. È presente un evento di mancato completamento di un'attività in almeno un dispositivo. I dispositivi del gruppo di Administration Server non cercano aggiornamenti di Windows da molto tempo. Sono presenti dispositivi con problemi di stato. • **OK**. Nessuno dei precedenti.
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	Il motivo `eventsStatus` mostra che sono presenti alcuni eventi critici in Administration Server. È possibile ottenere il numero di questi eventi tramite `criticalEventsCount`. Il valore è uguale a 1 se è presente almeno un evento critico in qualsiasi dispositivo e 0 in caso contrario.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Numero di eventi critici in Administration Server.

Risoluzione dei problemi

Questa sezione elenca le soluzioni per alcuni problemi tipici che si potrebbero riscontrare durante l'utilizzo del servizio SNMP.

L'applicazione di terze parti non riesce a connettersi al servizio SNMP

Verificare che il servizio SNMP sia installato e configurato come descritto nella sezione Configurazione del servizio SNMP per l'utilizzo con Kaspersky Security Center.

Il servizio SNMP funziona, ma l'applicazione di terze parti non riesce a ottenere alcun valore

Consentire il tracciamento dell'agente SNMP e assicurarsi che venga creato un file non vuoto. Ciò significa che l'agente SNMP è registrato e funziona correttamente. Successivamente, consentire le connessioni dal servizio SNMP nelle impostazioni del servizio secondario. Se un servizio secondario opera nello stesso host dell'agente SNMP, l'elenco di indirizzi IP deve contenere l'indirizzo IP di tale host o `loopback 127.0.0.1`.

In Windows deve essere in esecuzione un servizio SNMP che comunica con gli agenti. È possibile specificare i percorsi degli agenti SNMP nel Registro di sistema di Windows tramite regedit.

- Per Microsoft Windows 10:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Per Windows Vista e Windows Server 2008:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

È possibile consentire il tracciamento dell'agente SNMP tramite regedit.

- Per i sistemi a 32 bit:
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- Per i sistemi a 64 bit:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004
  "TraceDir"="C:\\"

I valori non corrispondono agli stati di Administration Console

Per ridurre il carico per Administration Server, la memorizzazione nella cache dei valori viene implementata per l'agente SNMP. La latenza tra la cache in corso di attualizzazione e i valori modificati in Administration Server potrebbe causare discrepanze tra i valori restituiti dall'agente SNMP e quelli effettivi. Quando si utilizzano applicazioni di terze parti, è necessario tenere in considerazione questa possibile latenza.

Utilizzo di un ambiente cloud

Questa sezione fornisce informazioni sulla distribuzione e la manutenzione di Kaspersky Security Center in ambienti cloud, come Amazon Web Services, Microsoft Azure o Google Cloud.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Informazioni sull'utilizzo di un ambiente cloud

Kaspersky Security Center 15.1 non solo funziona con i dispositivi locali, ma anche fornisce speciali funzionalità per l'utilizzo in un ambiente cloud. Kaspersky Security Center funziona con le seguenti macchine virtuali:

- Istanze Amazon EC2 (di seguito denominate *istanze*). Un'istanza di Amazon EC2 è una macchina virtuale creata in base alla piattaforma Amazon Web Services (AWS). Kaspersky Security Center utilizza l'*API* (Application Programming Interface) AWS.
- Macchine virtuali Microsoft Azure. Kaspersky Security Center utilizza l'API Azure.
- Istanze di macchine virtuali Google Cloud. Kaspersky Security Center utilizza l'API Google.

È possibile distribuire Kaspersky Security Center in un'istanza o una macchina virtuale per la gestione della protezione dei dispositivi nell'ambiente cloud e utilizzare le speciali funzionalità di Kaspersky Security Center per il funzionamento in un ambiente cloud. Tali funzionalità comprendono:

- L'utilizzo degli strumenti API per il polling dei dispositivi in un ambiente cloud
- L'utilizzo degli strumenti API per l'installazione di Network Agent e delle applicazioni di protezione nei dispositivi in un ambiente cloud
- La ricerca di dispositivi in base all'appartenenza a un segmento cloud specifico

È anche possibile utilizzare un'istanza o una macchina virtuale in cui è distribuito Kaspersky Security Center Administration Server per la protezione dei dispositivi locali (ad esempio, quando è preferibile eseguire la manutenzione di un server cloud rispetto a uno fisico). In questo caso, sarà possibile utilizzare l'Administration Server come se fosse installato in un dispositivo locale.

In un sistema Kaspersky Security Center distribuito da un'immagine AMI (Amazon Machine Image) a pagamento (in AWS) o uno SKU con fatturazione mensile basato sull'utilizzo (in Azure), Vulnerability e patch management è attivato automaticamente (inclusa l'integrazione con i sistemi SIEM), mentre Mobile Device Management non può essere attivato.

L'Administration Server viene installato insieme ad Administration Console. Kaspersky Security for Windows Server viene inoltre installato automaticamente nel dispositivo in cui è installato l'Administration Server.

È possibile configurare Kaspersky Security Center con la procedura guidata Configura ambiente cloud, tenendo conto delle specificità del lavoro in un ambiente cloud.

Scenario: Distribuzione per un ambiente cloud

In questa sezione viene descritta la distribuzione di Kaspersky Security Center per l'utilizzo in ambienti cloud come Amazon Web Services, Microsoft Azure e Google Cloud.

Una volta completato lo scenario di distribuzione, Kaspersky Security Center Administration Server e Administration Console vengono avviati e configurati con i parametri predefiniti. La protezione anti-virus gestita da Kaspersky Security Center viene distribuita nelle istanze Amazon EC2 o macchine virtuali Microsoft Azure selezionate. È quindi possibile ottimizzare la configurazione di Kaspersky Security Center, creare una struttura complessa di gruppi di amministrazione e creare vari criteri e attività per i gruppi.

La distribuzione di Kaspersky Security Center per l'utilizzo negli ambienti cloud comprende i seguenti elementi:

1. Operazioni preliminari
2. Distribuzione di Administration Server
3. Installazione delle applicazioni anti-virus di Kaspersky nei dispositivi virtuali che devono essere protetti
4. Configurazione delle impostazioni di download degli aggiornamenti
5. Configurazione delle impostazioni per la gestione dei rapporti sullo stato della protezione dei dispositivi

La procedura guidata Configura ambiente cloud consente di eseguire la configurazione iniziale. Viene avviata automaticamente la prima volta che Kaspersky Security Center viene distribuito da un'immagine pronta all'uso. È possibile avviare manualmente la procedura guidata in qualsiasi momento. È inoltre possibile eseguire manualmente tutte le operazioni che esegue.

È consigliabile pianificare almeno un'ora per la distribuzione di Kaspersky Security Center Administration Server nell'ambiente cloud e almeno un giorno lavorativo per la distribuzione della protezione nell'ambiente cloud.

La distribuzione di Kaspersky Security Center nell'ambiente cloud comprende le seguenti fasi:

1. **Pianificazione della configurazione dei segmenti cloud**

   Informazioni sul funzionamento di Kaspersky Security Center in un ambiente cloud. Pianificare dove distribuire Administration Server (all'interno o all'esterno dell'ambiente cloud) e determinare quanti segmenti cloud si prevede di proteggere. Se si prevede di distribuire Administration Server all'esterno dell'ambiente cloud o se si intende proteggere più di 5000 dispositivi, sarà necessario installare manualmente Administration Server.

   Per l'utilizzo di Google Cloud, è possibile installare Administration Server solo manualmente.

2. **Pianificazione delle risorse**

   Verificare di disporre di tutto il necessario per la distribuzione.

3. **Abbonamento a Kaspersky Security Center come immagine pronta all'uso**

   Selezionare una delle immagini AMI pronte per l'uso in AWS Marketplace o uno SKU con fatturazione mensile basato sull'utilizzo in Azure Marketplace, effettuare il pagamento in base alle regole del marketplace, se necessario (o utilizzare il modello BYOL), quindi utilizzare l'immagine per distribuire un'istanza di Amazon EC2/macchina virtuale Microsoft Azure con Kaspersky Security Center installato.

   Questa fase è necessaria solo se si prevede di distribuire Administration Server in un'istanza/macchina virtuale all'interno di un ambiente cloud e si intende distribuire la protezione per non più di 5000 dispositivi. In caso contrario, questa fase non è necessaria ed è invece necessario installare manualmente Administration Server, Administration Console e il DBMS.

   Questo passaggio non è disponibile per Google Cloud.

4. **Determinazione della posizione del DBMS**

   Determinare dove posizionare il DBMS.

   Se si desidera utilizzare un database all'esterno dell'ambiente cloud, verificare di disporre di un database funzionante.

   Se si prevede di utilizzare Amazon Relational Database Service (RDS), creare un database con RDS nell'ambiente cloud AWS.

   Se si prevede di utilizzare il DBMS SQL Microsoft Azure, creare un database con il servizio Database di Azure nell'ambiente cloud Microsoft Azure.

Se si prevede di utilizzare MySQL Google, creare un database in Google Cloud. Per informazioni dettagliate, fare riferimento a https://cloud.google.com/sql/docs/mysql.

5. **Installazione manuale di Administration Server e Administration Console (Console basata sul Web e/o Microsoft Management Console) nei dispositivi selezionati**

   Installare Administration Server, Administration Console e il DBMS nei dispositivi selezionati, come descritto nello scenario di installazione principale per Kaspersky Security Center.

   Questa fase è necessaria se si prevede di collocare Administration Server all'esterno di un ambiente cloud o si intende distribuire la protezione per più di 5000 dispositivi. Assicurarsi quindi che Administration Server soddisfi i requisiti hardware. In caso contrario, questa fase non è necessaria ed è sufficiente un abbonamento a Kaspersky Security Center come immagine pronta all'uso in AWS Marketplace, Azure Marketplace o Google Cloud.

6. **Verifica delle autorizzazioni di Administration Server per l'utilizzo delle API cloud**

   In AWS accedere alla console di gestione AWS e creare un ruolo IAM o un account utente IAM. Il ruolo IAM (o l'account utente IAM) creato consentirà a Kaspersky Security Center di interagire con l'API AWS: polling dei segmenti cloud e distribuzione della protezione.

   In Azure creare una sottoscrizione e un ID applicazione con una password. Kaspersky Security Center utilizza queste credenziali per l'utilizzo dell'API Azure: polling dei segmenti cloud e distribuzione della protezione.

   In Google Cloud registrare un progetto, ottenere l'ID del progetto e una chiave privata. Kaspersky Security Center utilizza queste credenziali per eseguire il polling dei segmenti cloud utilizzando l'API Google.

7. **Creazione di un ruolo IAM per le istanze protette (solo per AWS)**

   Nella console di gestione AWS creare un ruolo IAM che definisce il set di autorizzazioni per l'esecuzione delle richieste ad AWS. Il ruolo creato verrà successivamente assegnato alle nuove istanze. Il ruolo IAM è necessario per utilizzare Kaspersky Security Center per installare le applicazioni nelle istanze.

8. **Preparazione di un database tramite Amazon Relational Database Service o Microsoft Azure SQL**

   Se si prevede di utilizzare Amazon Relational Database Service (RDS), creare un'istanza di database Amazon RDS e un bucket S3 in cui archiviare il backup del database. È possibile ignorare questa fase se si desidera posizionare un database nella stessa istanza EC2 in cui è installato Administration Server o in un'altra posizione.

   Se si prevede di utilizzare Microsoft Azure SQL, creare un account di archiviazione e un database in Microsoft Azure.

   Se si prevede di utilizzare MySQL Google, configurare il database in Google Cloud. Per informazioni dettagliate, fare riferimento a https://cloud.google.com/sql/docs/mysql.

9. **Licensing di Kaspersky Security Center per l'utilizzo nell'ambiente cloud**

   Verificare di disporre delle licenze di Kaspersky Security Center per l'utilizzo nell'ambiente cloud e specificare un codice di attivazione o un file chiave, che verrà aggiunto all'archivio delle licenze dell'applicazione. Questa fase può essere completata durante la configurazione dell'ambiente cloud.

   Questa fase è necessaria se si utilizza Kaspersky Security Center installato da un'AMI pronta all'uso gratuita in base al modello BYOL o se si desidera installare manualmente Kaspersky Security Center senza l'utilizzo di AMI. In ognuno di questi casi, per attivare Kaspersky Security Center sarà necessaria una licenza per Kaspersky Security for Virtualization o una licenza per Kaspersky Hybrid Cloud Security.

   Se si utilizza Kaspersky Security Center installato da un'immagine pronta all'uso, questa fase non è necessaria e la finestra corrispondente della procedura guidata Configura ambiente cloud non è disponibile.

10. **Autorizzazione nell'ambiente cloud**

    Specificare in Kaspersky Security Center le credenziali AWS, Azure o Google Cloud, in modo che Kaspersky Security Center possa operare con le autorizzazioni necessarie. Questa fase può essere completata durante l'autorizzazione nell'ambiente cloud.

11. **Polling di un segmento cloud per consentire ad Administration Server di ricevere le informazioni sui dispositivi nel segmento cloud**

    Avviare il polling dei segmenti cloud. Nell'ambiente AWS Kaspersky Security Center riceverà gli indirizzi e i nomi di tutte le istanze accessibili in base alle autorizzazioni del ruolo IAM o dell'utente IAM. Nell'ambiente Microsoft Azure Kaspersky Security Center riceverà gli indirizzi e i nomi di tutte le macchine virtuali accessibili in base alle autorizzazioni del ruolo Lettore.

    È quindi possibile utilizzare Kaspersky Security Center per installare le applicazioni Kaspersky e software di altri produttori nelle istanze rilevate o nelle macchine virtuali.

    Kaspersky Security Center avvia periodicamente un polling, che consente di rilevare automaticamente le nuove istanze o macchine virtuali.

12. **Combinazione di tutti i dispositivi in rete nel gruppo di amministrazione Cloud**

    Spostare le istanze individuate o le macchine virtuali nel gruppo di amministrazione **Dispositivi gestiti\Cloud**, in modo da renderle disponibili per la gestione centralizzata. Se si desidera assegnare i dispositivi a sottogruppi, ad esempio a seconda del sistema operativo installato, è possibile creare diversi gruppi di amministrazione all'interno del gruppo **Dispositivi gestiti\Cloud**. È possibile abilitare lo spostamento automatico di tutti i dispositivi che verranno rilevati durante il polling di routine nel gruppo **Dispositivi gestiti\Cloud**.

13. **Utilizzo di Network Agent per la connessione dei dispositivi in rete ad Administration Server**

    Installare Network Agent nei dispositivi nell'ambiente cloud. Network Agent è il componente di Kaspersky Security Center che consente la comunicazione tra i dispositivi e Administration Server. Le impostazioni di Network Agent vengono configurate automaticamente per impostazione predefinita.

    È possibile installare Network Agent in ciascun dispositivo in locale. È anche possibile installare Network Agent nei dispositivi in remoto tramite Kaspersky Security Center. In alternativa, è possibile saltare questa fase e installare Network Agent insieme alle versioni più recenti delle applicazioni di protezione.

14. **Installazione delle versioni più recenti delle applicazioni di protezione nei dispositivi in rete**

    Selezionare i dispositivi in cui si desidera installare le applicazioni di protezione, quindi installare le versioni più recenti delle applicazioni di protezione in tali dispositivi. È possibile eseguire l'installazione in remoto tramite Kaspersky Security Center in Administration Server oppure in locale.

    Potrebbe essere necessario creare manualmente i pacchetti di installazione per questi programmi.

    Kaspersky Endpoint Security for Linux è destinato alle istanze e macchine virtuali che eseguono Linux.

    Kaspersky Security for Windows Server è destinato alle istanze e macchine virtuali che eseguono Windows.

15. **Configurazione delle impostazioni di aggiornamento**

L'attività **Trova vulnerabilità e aggiornamenti richiesti** viene creata automaticamente quando viene avviata la configurazione dell'ambiente cloud. È inoltre possibile creare l'attività manualmente. Questa attività trova e scarica automaticamente gli aggiornamenti richiesti dell'applicazione per la successiva installazione nei dispositivi di rete tramite gli strumenti di Kaspersky Security Center.

È consigliabile eseguire questa fase al termine della configurazione dell'ambiente cloud:

1. **Configurazione della gestione dei rapporti**

    È possibile visualizzare i rapporti nella scheda **Monitoraggio** nell'area di lavoro del nodo **Administration Server**. È inoltre possibile ricevere rapporti via e-mail. I rapporti nella scheda **Monitoraggio** sono disponibili per impostazione predefinita. Per configurare la ricezione dei rapporti tramite e-mail, specificare gli indirizzi e-mail a cui inviare i rapporti, quindi configurare il formato dei rapporti.

Risultati

Al termine dello scenario è consigliabile assicurarsi che la configurazione iniziale sia andata a buon fine:

- È possibile connettersi ad Administration Server tramite Administration Console o Kaspersky Security Center Web Console.
- Le versioni più recenti delle applicazioni di protezione di Kaspersky sono installate e vengono eseguite nei dispositivi gestiti.
- Kaspersky Security Center ha creato le attività e i criteri predefiniti per tutti i dispositivi gestiti.

Prerequisiti per la distribuzione di Kaspersky Security Center in un ambiente cloud

Prima di avviare la distribuzione di Kaspersky Security Center nell'ambiente cloud Amazon Web Services o Microsoft Azure, verificare di disporre dei seguenti elementi:

- Accesso a Internet
- Uno dei seguenti account:
  - Account Amazon Web Services (per l'utilizzo con AWS)
  - Account Microsoft (per l'utilizzo con Azure)
  - Account Google (per l'utilizzo con Google Cloud)
- Uno dei seguenti elementi:
  - Licenza per Kaspersky Security for Virtualization
  - Licenza per Kaspersky Hybrid Cloud Security
  - Disponibilità economica per l'acquisto di tale licenza (Kaspersky Security for Virtualization o Kaspersky Hybrid Cloud Security)
  - Disponibilità economica per pagare un'immagine pronta all'uso in Azure Marketplace
- Guide per le ultime versioni di Kaspersky Endpoint Security for Linux e Kaspersky Security for Windows Server

Requisiti hardware per Administration Server in un ambiente cloud

Per la distribuzione in ambienti cloud, i requisiti per Administration Server e il server database sono gli stessi di quelli per Administration Server fisico (a seconda del numero di dispositivi che si desidera gestire). Fare riferimento alla documentazione dell'ambiente cloud per informazioni dettagliate.

Opzioni di licenza in un ambiente cloud

Il funzionamento in un ambiente cloud va oltre le funzionalità di base di Kaspersky Security Center, quindi è richiesta una licenza dedicata.

Sono disponibili due opzioni di licensing di Kaspersky Security Center per l'utilizzo in un ambiente cloud:

- immagine AMI a pagamento (in Amazon Web Services) o SKU con fatturazione mensile basato sull'utilizzo (in Microsoft Azure).

  In tal modo, vengono concesse una licenza per Kaspersky Security Center e le licenze per Kaspersky Endpoint Security for Linux e Kaspersky Security for Windows Server. Il pagamento varia in base alle regole dell'ambiente cloud in uso.

  Questo modello consente di avere un massimo di 200 dispositivi client per un Administration Server.

- Immagine gratuita pronta per l'uso con una licenza proprietaria, in base al modello Bring Your Own License (BYOL).

  Per la gestione delle licenze di Kaspersky Security Center in AWS o Azure, è necessario disporre di una licenza per le seguenti applicazioni:

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  Il modello BYOL consente di avere un massimo di 100.000 dispositivi client per un Administration Server. Questo modello consente inoltre di gestire i dispositivi all'esterno dell'ambiente AWS, Azure o Google.

  È possibile scegliere il modello BYOL in uno dei seguenti casi:

  - Si dispone già di una licenza valida per Kaspersky Security for Virtualization.
  - Si dispone già di una licenza valida per Kaspersky Hybrid Cloud Security.
  - Si desidera acquistare una licenza subito prima della distribuzione di Kaspersky Security Center.

  Durante la configurazione iniziale, Kaspersky Security Center richiede un codice di attivazione o un file chiave.

  Se si seleziona BYOL, non sarà necessario pagare per Kaspersky Security Center tramite Azure Marketplace o AWS Marketplace.

In entrambi casi, Vulnerability e patch management viene attivato automaticamente, mentre Mobile Device Management non può essere attivato.

Se si verifica un errore durante il tentativo di attivare la funzionalità Supporto dell'ambiente cloud utilizzando la licenza per Kaspersky Hybrid Cloud Security, utilizzare il file chiave.

Con l'abbonamento a Kaspersky Security Center, si ottiene un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o una macchina virtuale Microsoft Azure con Kaspersky Security Center Administration Server. I pacchetti di installazione per Kaspersky Security for Windows Server e Kaspersky Endpoint Security for Linux sono disponibili nell'Administration Server. È possibile installare tali applicazioni nei dispositivi nell'ambiente cloud. Non è necessario concedere in licenza queste applicazioni.

Se un dispositivo gestito non risulta visibile per l'Administration Server per più di una settimana, l'applicazione (Kaspersky Security for Windows Server o Kaspersky Endpoint Security for Linux) nel dispositivo passerà alla modalità con funzionalità limitate. Per riattivare l'applicazione, è necessario rendere il dispositivo in cui è installata l'applicazione nuovamente visibile per l'Administration Server.

Opzioni del database per l'utilizzo in un ambiente cloud

È necessario disporre di un database per l'utilizzo di Kaspersky Security Center. Durante la distribuzione di Kaspersky Security Center in AWS, in Microsoft Azure o Google Cloud, sono disponibili tre opzioni:

- Creare un database locale nello stesso dispositivo dell'Administration Server. Kaspersky Security Center include un database SQL Server Express in grado di supportare fino a 5.000 dispositivi gestiti. Selezionare questa opzione se SQL Server Express Edition è sufficiente per le proprie esigenze.

- Creare un database con Relational Database Service (RDS) nell'ambiente cloud AWS o con il servizio Database di Azure nell'ambiente cloud Microsoft Azure. Scegliere questa opzione se si desidera un sistema DBMS diverso da SQL Express. I dati verranno trasferiti nell'ambiente cloud, dove resteranno archiviati, senza costi aggiuntivi. Se si utilizza già Kaspersky Security Center in locale e il database contiene alcuni dati, è possibile trasferirli nel nuovo database.

  Per l'utilizzo in Google Cloud Platform, è possibile utilizzare solo Cloud SQL per MySQL.

- Utilizzare un server di database esistente. Selezionare questa opzione se si dispone già di un server di database e si desidera utilizzarlo per Kaspersky Security Center. Se il server è esterno all'ambiente cloud, i dati verranno trasferiti via Internet. Tale operazione può comportare costi aggiuntivi.

La procedura di distribuzione di Kaspersky Security Center nell'ambiente cloud include uno speciale passaggio per la creazione (scelta) di un database.

Utilizzo dell'ambiente cloud Amazon Web Services

In questa sezione viene descritto come eseguire la preparazione per l'utilizzo di Kaspersky Security Center in Amazon Web Services.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Informazioni sull'utilizzo dell'ambiente cloud Amazon Web Services

È possibile acquistare Kaspersky Security Center in AWS Marketplace sotto forma di Amazon Machine Image (AMI), un'immagine pronta all'uso di una macchina virtuale preconfigurata. È possibile abbonarsi a un'immagine AMI a pagamento o BYOL e, in base a tale immagine, creare un'istanza di Amazon EC2 con Kaspersky Security Center Administration Server installato.

Per utilizzare la piattaforma AWS e, in particolare, per acquistare le app in AWS Marketplace e creare istanze, è necessario un account Amazon Web Services. È possibile creare un account gratuito all'indirizzo https://aws.amazon.com/it. È anche possibile utilizzare un account Amazon esistente.

Se è stato scelto un abbonamento per un'immagine AMI disponibile in AWS Marketplace, si riceverà un'istanza con Kaspersky Security Center pronto all'uso. Non è necessario installare l'applicazione manualmente. In questo caso, Kaspersky Security Center Administration Server è installato nell'istanza senza l'intervento dell'utente. Dopo l'installazione, è possibile avviare Administration Console e connettersi ad Administration Server per iniziare a utilizzare Kaspersky Security Center.

Per ulteriori informazioni su un'AMI e sul funzionamento di AWS Marketplace, visitare la pagina della Guida di AWS Marketplace. Per ulteriori informazioni sull'utilizzo della piattaforma AWS, l'utilizzo delle istanze e i relativi concetti, fare riferimento alla documentazione di Amazon Web Services.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Creazione di ruoli IAM e account utente IAM per le istanze Amazon EC2

In questa sezione sono descritte le azioni da eseguire per garantire il corretto funzionamento dell'Administration Server. Queste azioni includono l'utilizzo dei ruoli e degli account utente IAM (Identity and Access Management) AWS. Sono inoltre descritte le azioni che devono essere eseguite nei dispositivi client per installare Network Agent in tali dispositivi e quindi installare Kaspersky Security for Windows Server e Kaspersky Endpoint Security for Linux.

Verifica delle autorizzazioni di Kaspersky Security Center Administration Server per l'utilizzo di AWS

Gli standard per l'esecuzione nell'ambiente cloud Amazon Web Services prevedono l'assegnazione di un ruolo IAM speciale all'istanza di Administration Server per l'utilizzo con i servizi AWS. Un ruolo IAM è un'entità IAM che definisce il set di autorizzazioni per l'esecuzione delle richieste ai servizi AWS. Il ruolo IAM fornisce le autorizzazioni per il polling dei segmenti cloud e l'installazione delle applicazioni nelle istanze.

Dopo aver creato un ruolo IAM e averlo assegnato all'Administration Server, sarà possibile distribuire la protezione delle istanze utilizzando questo ruolo, senza fornire informazioni aggiuntive a Kaspersky Security Center.

Tuttavia, potrebbe essere consigliabile non creare un ruolo IAM per l'Administration Server nei seguenti casi:

- I dispositivi di cui si prevede di gestire la protezione sono istanze EC2 all'interno di ambiente cloud Amazon Web Services, ma l'Administration Server è all'esterno dell'ambiente.

- Si prevede di gestire la protezione di istanze non solo all'interno del proprio segmento cloud, ma anche in altri segmenti cloud che sono stati creati con un altro account in AWS. In questo caso, sarà necessario un ruolo IAM solo per la protezione del proprio segmento cloud. Non sarà richiesto un ruolo IAM per proteggere un altro segmento cloud.

In questi casi, invece di creare un ruolo IAM, sarà necessario creare un *account utente IAM*, che verrà usato da parte di Kaspersky Security Center per l'utilizzo dei servizi AWS. Prima di iniziare a utilizzare Administration Server, creare un account utente IAM con una *chiave di accesso AWS IAM* (di seguito denominata anche *chiave di accesso IAM*).

La creazione di un ruolo IAM o di un account utente IAM richiede la console di gestione AWS. Per utilizzare la console di gestione AWS, saranno necessari il nome utente e la password di un account AWS.

Creazione di un ruolo IAM per l'Administration Server

Prima di distribuire Administration Server, nella console di gestione AWS creare un ruolo IAM con le autorizzazioni richieste per l'installazione delle applicazioni nelle istanze. Per ulteriori dettagli, vedere le sezioni della Guida AWS sui ruoli IAM.

Per creare un ruolo IAM per l'Administration Server:

1. Aprire la console di gestione AWS e accedere con il proprio account AWS.

2. Nella sezione **Ruoli** creare un ruolo con le seguenti autorizzazioni:

   - **AmazonEC2ReadOnlyAccess**, se si prevede di eseguire solo il polling dei segmenti cloud e non si intende installare applicazioni nelle istanze EC2 tramite API AWS.

   - **AmazonEC2ReadOnlyAccess** e **AmazonSSMFullAccess**, se si intende eseguire il polling dei segmenti cloud e installare le applicazioni nelle istanze EC2 utilizzando API AWS. In questo caso sarà necessario assegnare anche un ruolo IAM con l'autorizzazione AmazonEC2RoleforSSM alle istanze EC2 protette.

È necessario assegnare questo ruolo all'istanza EC2 che verrà utilizzata come Administration Server.

Il nuovo ruolo creato è disponibile per tutte le applicazioni nell'Administration Server. Di conseguenza, qualsiasi applicazione in esecuzione nell'Administration Server è in grado di eseguire il polling dei segmenti cloud o di installare applicazioni nelle istanze EC2 all'interno di un segmento cloud.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Creazione di un account utente IAM per l'utilizzo di Kaspersky Security Center

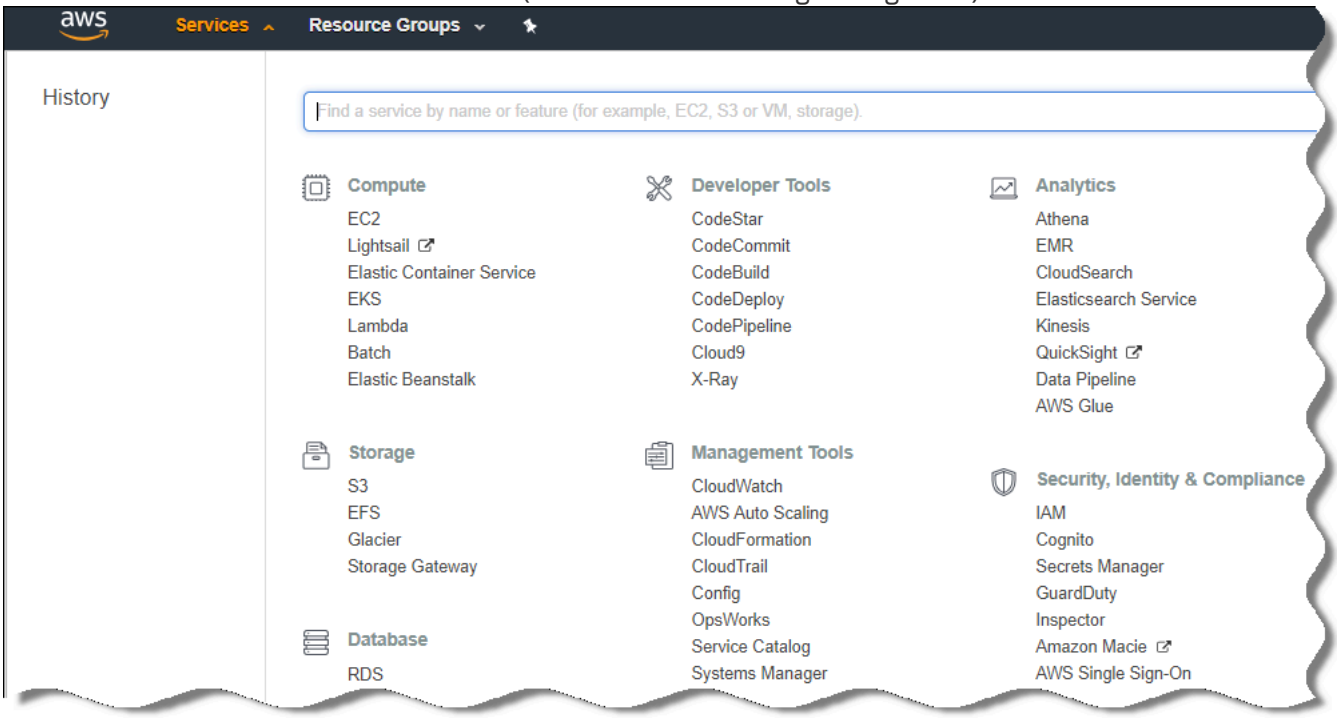
È necessario un account utente IAM per l'utilizzo di Kaspersky Security Center se all'Administration Server non è stato assegnato un ruolo IAM con le autorizzazioni per la device discovery e l'installazione delle applicazioni nelle istanze. Se si utilizza un bucket S3, è inoltre necessario lo stesso account, o un account differente, per l'attività di backup dei dati di Administration Server. È possibile creare un solo account utente IAM con tutte le autorizzazioni necessarie oppure due account utente distinti.

Per l'utente IAM viene creata automaticamente una *chiave di accesso IAM* che sarà necessario fornire a Kaspersky Security Center durante la configurazione iniziale. Una chiave di accesso IAM è costituita da un ID chiave di accesso e da una chiave segreta. Per ulteriori informazioni sul servizio IAM, consultare le seguenti pagine di riferimento su AWS:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- http://docs.aws.amazon.com/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Per creare un account utente IAM con le autorizzazioni richieste:

1. Aprire la console di gestione AWS e accedere con il proprio account.
2. Nell'elenco dei servizi AWS selezionare **IAM** (come illustrato nella figura seguente).



Elenco di servizi nella console di gestione AWS

Verrà visualizzata una finestra che contiene un elenco di nomi utente e un menu che consente di utilizzare lo strumento.

3. Spostarsi tra le aree della console per gestire gli account utente e aggiungere uno o più nomi utente.

4. Per gli utenti aggiunti, specificare le seguenti proprietà AWS:

   - Tipo di accesso: **Programmatic Access**.
   - Limite per le autorizzazioni non impostato.
   - Autorizzazioni:
     - **ReadOnlyAccess** - Se si prevede di eseguire solo il polling dei segmenti cloud e non si intende installare applicazioni nelle istanze EC2 tramite API AWS.
     - **ReadOnlyAccess** e **AmazonSSMFullAccess** - Se si intende eseguire il polling dei segmenti cloud e installare le applicazioni nelle istanze EC2 utilizzando API AWS. In questo caso, è necessario assegnare un ruolo IAM con l'autorizzazione AmazonEC2RoleforSSM alle istanze EC2 protette.

   Dopo aver aggiunto le autorizzazioni, verificare che siano corrette. Se la selezione è errata, tornare alla finestra precedente e ripetere la selezione.

5. Dopo la creazione dell'account utente, verrà visualizzata una tabella contenente la chiave di accesso IAM del nuovo utente IAM. L'ID chiave di accesso sarà visualizzato nella colonna **Access key ID**. La chiave segreta sarà visualizzata tramite asterischi nella colonna **Secret access key**. Per visualizzare la chiave segreta, fare clic su **Show**.

Il nuovo account creato verrà visualizzato nell'elenco degli account utente IAM corrispondente all'account in AWS.

Durante la distribuzione di Kaspersky Security Center in un segmento cloud, è necessario specificare un account utente IAM e fornire l'ID chiave di accesso e la chiave segreta a Kaspersky Security Center.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Creazione di un ruolo IAM per l'installazione delle applicazioni nelle istanze Amazon EC2

Prima di avviare la distribuzione della protezione nelle istanze EC2 utilizzando Kaspersky Security Center, creare nella console di gestione AWS un ruolo IAM con le autorizzazioni richieste per l'installazione delle applicazioni nelle istanze. Per ulteriori dettagli, vedere le sezioni della Guida AWS sui ruoli IAM.

Il ruolo IAM è necessario in modo da poterlo assegnare a tutte le istanze EC2 in cui si intende installare applicazioni di protezione utilizzando Kaspersky Security Center. Se non si assegna a un'istanza il ruolo IAM con le autorizzazioni necessarie, l'installazione delle applicazioni in questa istanza utilizzando gli strumenti API AWS genererà un errore.

Per utilizzare la console di gestione AWS, saranno necessari il nome utente e la password di un account AWS.

Per creare un ruolo IAM per l'installazione delle applicazioni nelle istanze:

1. Aprire la console di gestione AWS e accedere con il proprio account AWS.
2. Nel menu a sinistra selezionare **Roles**.
3. Fare clic sul pulsante **Create Role**.

4. Nell'elenco dei servizi visualizzato selezionare **EC2** e quindi, nell'elenco **Select Your Use Case**, selezionare nuovamente **EC2**.

5. Fare clic sul pulsante **Next: Permissions**.

6. Nell'elenco visualizzato selezionare la casella di controllo accanto a **AmazonEC2RoleforSSM**.

7. Fare clic sul pulsante **Next: Review**.

8. Immettere un nome e una descrizione per il ruolo IAM e fare clic sul pulsante **Create role**.

   Il ruolo creato viene visualizzato nell'elenco dei ruoli con il nome e la descrizione immessi.

Da questo momento in poi è possibile utilizzare il nuovo ruolo IAM creato per creare nuove istanze EC2 da proteggere tramite Kaspersky Security Center, nonché associarlo alle istanze esistenti.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Utilizzo di Amazon RDS

In questa sezione vengono descritte le azioni da eseguire per preparare un database di Amazon Relational Database Service (RDS) per Kaspersky Security Center, inserirlo in un gruppo di opzioni, creare un ruolo IAM per l'utilizzo di un database RDS, preparare un bucket S3 per l'archiviazione ed eseguire la migrazione di un database esistente a RDS.

Amazon RDS è un servizio Web che consente agli utenti AWS di impostare, eseguire e scalare un database relazionale nell'ambiente cloud AWS. Se si desidera, è possibile utilizzare un database Amazon RDS per l'utilizzo con Kaspersky Security Center.

È possibile utilizzare i seguenti database:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Creazione di un'istanza Amazon RDS

Se si desidera utilizzare Amazon RDS come sistema DBMS, è necessario creare un'istanza di database Amazon RDS. Questa sezione descrive come selezionare SQL Express Edition; se si desidera utilizzare Aurora MySQL o Standard MySQL (versioni 5.7, 8.0), è necessario selezionare uno di questi motori.

Per creare un'istanza di database Amazon RDS:

1. Aprire la console di gestione AWS all'indirizzo https://console.aws.amazon.com e accedere con il proprio account.

2. Utilizzando l'interfaccia AWS, creare un database con le seguenti impostazioni:

   - Motore: Microsoft SQL Server, SQL Express Edition
   - Versione del motore di database: SQL Server 2014 12.00.5546.0v1
   - Classe dell'istanza database: db.t2.medium
   - Tipo di archiviazione: generale
   - Archiviazione allocata: almeno 50 GiB
   - Gruppo di protezione: lo stesso gruppo a cui apparterrà l'istanza EC2 con Kaspersky Security Center Administration Server

   Creare un identificatore, un nome utente e una password per l'istanza RDS.

   È possibile mantenere le impostazioni predefinite in tutti gli altri campi. In alternativa, modificare le impostazioni predefinite se si desidera personalizzare l'istanza Amazon RDS. Per assistenza, fare riferimento alla pagine delle informazioni su AWS.

3. Durante l'ultimo passaggio, AWS visualizza i risultati del processo. Per visualizzare i dettagli dell'istanza Amazon RDS, fare clic su **View DB instance details**. Per passare all'azione successiva, avviare la creazione di un gruppo di opzioni per l'istanza Amazon RDS.

La creazione di una nuova istanza di Amazon RDS può richiedere diversi minuti. Dopo la creazione dell'istanza, è possibile utilizzarla per lavorare con i dati di Kaspersky Security Center.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Creazione di gruppo di opzioni per l'istanza Amazon RDS

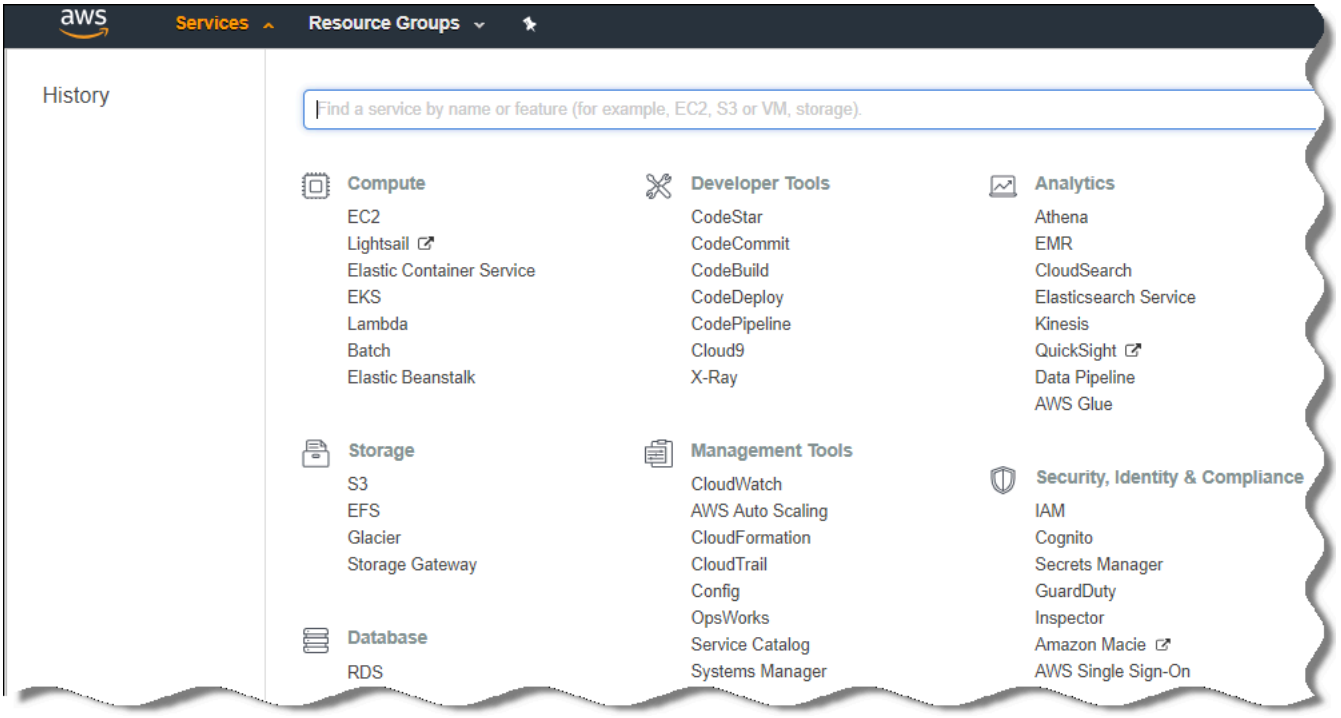
È necessario inserire l'istanza Amazon RDS in un gruppo di opzioni.

Per creare un gruppo di opzioni per l'istanza Amazon RDS:

1. Verificare di aver aperto la console di gestione AWS (https://console.aws.amazon.com) e di aver effettuato l'accesso con il proprio account.

2. Nella riga del menu fare clic su **Services**.

   Verrà visualizzato l'elenco dei servizi disponibili (vedere la figura seguente).



Elenco di servizi nella console di gestione AWS

3. Nell'elenco fare clic su **RDS**.

4. Nel riquadro sinistro fare clic su **Option groups**.

5. Fare clic sul pulsante **Create group**.

6. Creare un gruppo di opzioni con le seguenti impostazioni, se è stato selezionato SQL Server durante la creazione dell'istanza Amazon RDS:

   - Motore: SQLserver-ex
   - Versione principale del motore: 12.00

   Se è stato selezionato un database SQL diverso durante la creazione dell'istanza Amazon RDS, scegliere un motore corrispondente.

Il gruppo verrà creato e visualizzato nell'elenco dei gruppi.

Dopo la creazione del gruppo di opzioni, posizionare l'istanza Amazon RDS in questo gruppo di opzioni.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Modifica del gruppo di opzioni

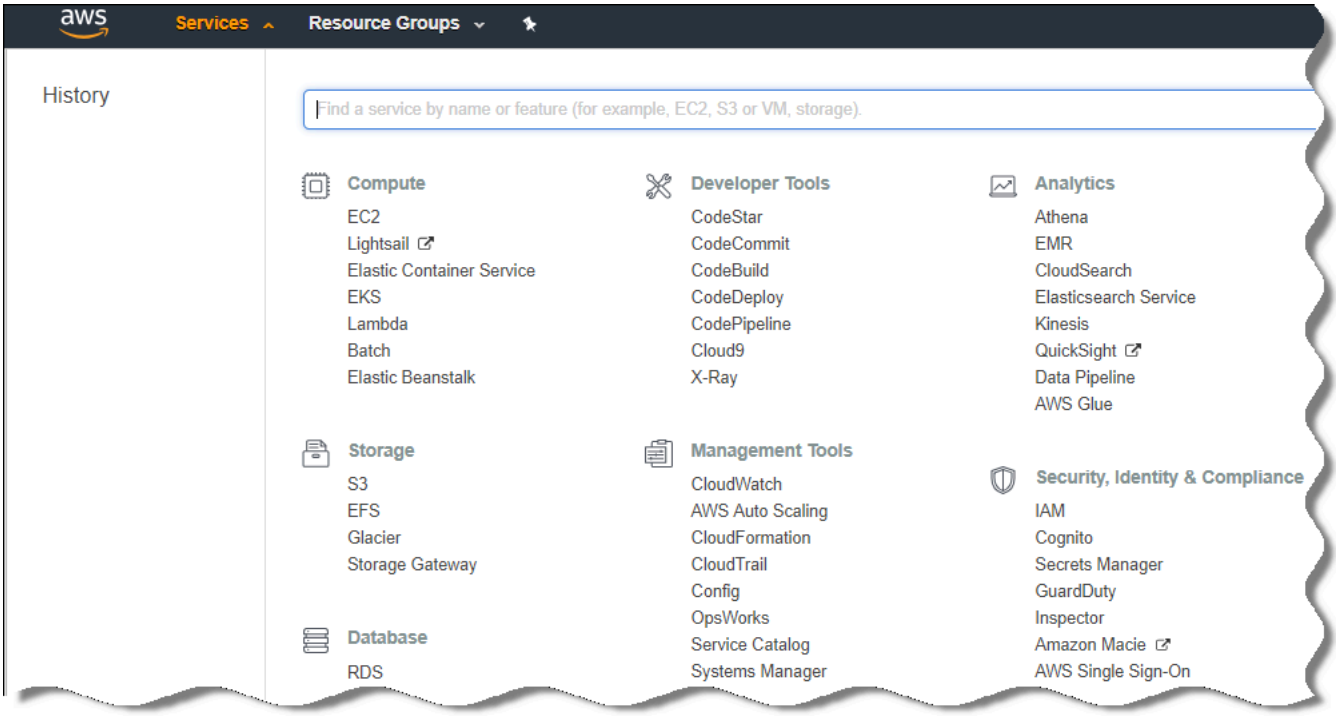
La configurazione predefinita del gruppo di opzioni in cui è stata posizionata l'istanza di Amazon RDS non è sufficiente per l'utilizzo del database di Kaspersky Security Center. È necessario aggiungere opzioni al gruppo di opzioni e creare un nuovo ruolo IAM per l'utilizzo del database.

Per modificare il gruppo di opzioni e creare un nuovo ruolo IAM:

1. Verificare di aver aperto la console di gestione AWS (https://console.aws.amazon.com) e di aver effettuato l'accesso con il proprio account.

2. Nella riga del menu fare clic su **Services**.

   Verrà visualizzato l'elenco dei servizi disponibili (vedere la figura seguente).



Elenco di servizi nella console di gestione AWS

3. Nell'elenco selezionare RDS.

4. Nel riquadro sinistro fare clic su **Option groups**.

   Verrà visualizzato l'elenco dei gruppi di opzioni.

5. Selezionare il gruppo di opzioni in cui è posizionata l'istanza Amazon RDS, quindi fare clic sul pulsante **Add option**.

   Verrà visualizzata la finestra **Add option**.

6. Nella sezione IAM role selezionare l'opzione **Create a new role** / **Yes** e immettere un nome per il nuovo ruolo IAM.

   Il ruolo verrà creato con un set predefinito di autorizzazioni. Successivamente, sarà necessario modificarne le autorizzazioni.

7. Nella sezione S3 bucket eseguire una delle seguenti operazioni:

   - Se non è stata creata un'istanza bucket Amazon S3 per il backup dei dati, selezionare il collegamento **Create a new S3 bucket** e creare un nuovo bucket S3 tramite l'interfaccia AWS.
   - Se è già stata creata un'istanza bucket Amazon S3 per l'attività di backup dei dati di Administration Server, selezionare il bucket S3 nell'elenco a discesa.

8. Completare l'aggiunta delle opzioni facendo clic sul pulsante **Add option** nella parte inferiore della pagina.

È stato modificato il gruppo di opzioni e creato un nuovo ruolo IAM per l'utilizzo del database RDS.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Modifica delle autorizzazioni per il ruolo IAM per l'istanza di database Amazon RDS

Dopo aver aggiunto le opzioni al gruppo di opzioni, è necessario assegnare al ruolo IAM che è stato creato le autorizzazioni richieste per l'utilizzo dell'istanza di database Amazon RDS.

Per assegnare al ruolo IAM che è stato creato le autorizzazioni richieste per l'utilizzo dell'istanza di database Amazon RDS:

1. Verificare di aver aperto la console di gestione AWS (https://console.aws.amazon.com) e di aver effettuato l'accesso con il proprio account.
2. Nell'elenco dei servizi selezionare **IAM**.

   Verrà visualizzata una finestra che contiene un elenco di nomi utente e un menu che consente di utilizzare lo strumento.

3. Nel menu selezionare **Ruoli**.
4. Nell'elenco dei ruoli IAM visualizzato nell'area di lavoro selezionare il ruolo che è stato creato durante l'aggiunta dell'opzione al gruppo di opzioni.
5. Utilizzando l'interfaccia AWS, eliminare il criterio **sqlNativeBackup-<data>**.
6. Utilizzando l'interfaccia AWS, associare il criterio **AmazonS3FullAccess** al ruolo.

Al ruolo IAM verranno assegnate le autorizzazioni richieste per l'utilizzo di Amazon RDS.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Preparazione del bucket Amazon S3 per il database

Se si prevede di utilizzare il database Amazon Relational Database System (Amazon RDS), è necessario creare un'istanza bucket Amazon Simple Storage Service (Amazon S3) in cui archiviare il backup periodico del database. Per informazioni su Amazon S3 e i bucket S3, fare riferimento alle pagine della Guida di Amazon. Per ulteriori informazioni sulla creazione di un'istanza Amazon S3, fare riferimento alla pagina della Guida di Amazon S3.

Per creare un bucket Amazon S3:

1. Verificare che la console di gestione AWS sia aperta e di avere effettuato l'accesso con il proprio account.
2. Nell'elenco dei servizi AWS selezionare S3.
3. Spostarsi nella console per creare un bucket, seguendo le istruzioni della procedura guidata.
4. Selezionare la stessa regione in cui si trova (o sarà posizionato) l'Administration Server.
5. Al termine della procedura guidata, verificare che il nuovo bucket sia visualizzato nell'elenco dei bucket.

   Un nuovo bucket S3 verrà creato e sarà visualizzato nell'elenco dei bucket. È necessario specificare questo bucket durante l'aggiunta di opzioni al gruppo di opzioni. È inoltre necessario specificare l'indirizzo del bucket S3 in Kaspersky Security Center quando Kaspersky Security Center crea l'attività *Backup dei dati di Administration Server*.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Migrazione del database ad Amazon RDS

È possibile eseguire la migrazione del database di Kaspersky Security Center da un dispositivo locale a un'istanza di Amazon S3 che supporta Amazon RDS. A tale scopo, è necessario un bucket S3 per un database RDS e un account utente IAM con l'autorizzazione AmazonS3FullAccess per questo bucket S3.

Per eseguire la migrazione del database:

1. Verificare di aver creato un'istanza RDS (per ulteriori informazioni, vedere le pagine di riferimento su Amazon RDS).
2. Nell'Administration Server fisico (locale) eseguire l'utilità di backup di Kaspersky per eseguire il backup dei dati di Administration Server.

   È necessario assicurarsi che il file si chiami backup.zip.
3. Copiare il file backup.zip nell'istanza EC2 in cui è installato Administration Server.

   Verificare che lo spazio su disco sia sufficiente nell'istanza EC2 in cui è installato Administration Server. Nell'ambiente AWS è possibile aggiungere spazio su disco all'istanza in base ai requisiti del processo di migrazione del database.

4. Nell'Administration Server AWS avviare nuovamente l'utilità di backup di Kaspersky in modalità interattiva.

   Verrà avviata la Procedura guidata di backup e ripristino.

5. Nel passaggio **Seleziona azione** selezionare **Ripristina dati di Administration Server** e fare clic su **Avanti**.

6. Nel passaggio **Ripristinare le impostazioni** fare clic sul pulsante **Sfoglia** accanto a **Cartella per l'archiviazione delle copie di backup**.

7. Nella finestra **Accedere all'archivio online** visualizzata compilare i seguenti campi e fare clic su **OK**:

   - **Nome del bucket S3**

     Nome del bucket S3.

   - **Cartella di backup**

     Specificare il percorso della cartella di archiviazione da utilizzare per il backup.

   - **ID chiave di accesso**

     ID chiave di accesso AWS IAM appartenente all'utente IAM che dispone delle autorizzazioni per l'utilizzo del bucket S3 (autorizzazione AmazonS3FullAccess).

   - **Chiave segreta**

     Chiave segreta AWS IAM appartenente all'utente IAM che dispone delle autorizzazioni per l'utilizzo del bucket S3 (autorizzazione AmazonS3FullAccess).

8. Selezionare l'opzione **Esegui la migrazione dal backup locale**. Il pulsante **Sfoglia** diventa disponibile.

9. Fare clic sul pulsante **Sfoglia** per scegliere la cartella nell'Administration Server AWS in cui è stato copiato il file backup.zip.

10. Fare clic su **Avanti** e completare la procedura.

    I dati verranno ripristinati nel database RDS tramite il bucket S3. È possibile utilizzare questo database per ulteriori operazioni con Kaspersky Security Center nell'ambiente AWS.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Utilizzo dell'ambiente cloud Microsoft Azure

Questa sezione fornisce le informazioni sulla distribuzione e sulla manutenzione di Kaspersky Security Center in un ambiente cloud fornito da Microsoft Azure, nonché i dettagli sulla distribuzione della protezione nelle macchine virtuali in questo ambiente cloud.

In un sistema Kaspersky Security Center che è stato distribuito da uno SKU con fatturazione mensile basato sull'utilizzo, Vulnerability e patch management è attivato automaticamente, mentre Mobile Device Management non può essere attivato.

Informazioni sull'utilizzo di Microsoft Azure

Per utilizzare la piattaforma Microsoft Azure e, in particolare, per acquistare app in Azure Marketplace e creare macchine virtuali, è necessaria una sottoscrizione Azure. Prima di distribuire l'Administration Server, creare un ID applicazione Azure con le autorizzazioni richieste per l'installazione delle applicazioni nelle macchine virtuali.

Se si acquista un'immagine di Kaspersky Security Center in Azure Marketplace, è possibile distribuire una macchina virtuale con Kaspersky Security Center Administration Server pronto per l'uso. È necessario selezionare le impostazioni della macchina virtuale, ma non è necessario installare manualmente l'applicazione. Dopo l'installazione, è possibile avviare Administration Console e connettersi ad Administration Server per iniziare a utilizzare Kaspersky Security Center.

È anche possibile utilizzare una macchina virtuale di Azure in cui è distribuito Kaspersky Security Center Administration Server per la protezione dei dispositivi locali (ad esempio, quando è preferibile eseguire la manutenzione di un server cloud rispetto a uno fisico). In questo caso, sarà possibile utilizzare l'Administration Server come se fosse installato in un dispositivo locale. Se non si prevede di utilizzare gli strumenti dell'API Azure, non è necessario un ID applicazione Azure. In questo caso, una sottoscrizione Azure è sufficiente.

Creazione di una sottoscrizione, un ID applicazione e una password

Per utilizzare Kaspersky Security Center nell'ambiente Microsoft Azure, sono necessari una sottoscrizione Azure, l'ID applicazione Azure e la password dell'applicazione Azure. È possibile utilizzare una sottoscrizione esistente, se si dispone già di una sottoscrizione.

Una sottoscrizione Azure consente al proprietario di accedere al portale di gestione della piattaforma Microsoft Azure e ai servizi Microsoft Azure. Il proprietario può utilizzare la piattaforma Microsoft Azure per gestire servizi come Azure SQL e Archiviazione Azure.

Per creare una sottoscrizione Microsoft Azure:

Visitare l'indirizzo https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription e seguire le istruzioni.

Ulteriori informazioni sulla creazione di una sottoscrizione sono disponibili nel sito Web di Microsoft. Verrà creato un ID sottoscrizione, che in un secondo momento sarà necessario specificare in Kaspersky Security Center insieme con l'ID applicazione e la password.

Per creare e salvare l'ID applicazione Azure e la password:

1. Visitare https://portal.azure.com e verificare di aver eseguito l'accesso.
2. Creare l'ID applicazione, seguendo le istruzioni nella pagina di riferimento.
3. Passare alla sezione **Chiavi** delle impostazioni dell'applicazione.
4. Nella sezione **Chiavi** compilare i campi **Descrizione** e **Scadenza** e lasciare vuoto il campo **Valore**.

5. Fare clic su **Salva**.

   Facendo clic su **Salva**, il sistema inserisce automaticamente nel campo **Valore** una lunga sequenza di caratteri. La sequenza è la password dell'applicazione Azure (ad esempio yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). La descrizione è visualizzata così come viene immessa.

6. Copiare la password e salvarla in modo da poter specificare in un secondo momento l'ID applicazione e la password in Kaspersky Security Center.

   È possibile copiare la password solo al momento della creazione. Successivamente, la password non verrà più visualizzata e non potrà essere ripristinata.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Assegnazione di un ruolo all'ID applicazione Azure

Se si desidera rilevare le macchine virtuali solo tramite la device discovery, l'ID applicazione Azure deve disporre del ruolo Lettura. Se si desidera non solo rilevare le macchine virtuali, ma anche distribuire la protezione nelle macchine virtuali, l'ID applicazione Azure deve disporre del ruolo Collaboratore macchina virtuale.

Seguire le istruzioni nel sito Web di Microsoft per assegnare un ruolo all'ID applicazione Azure.

Distribuzione di Administration Server in Microsoft Azure e selezione del database

Per distribuire Administration Server nell'ambiente Microsoft Azure:

1. Accedere a Microsoft Azure utilizzando il proprio account.
2. Accedere al portale di Azure.
3. Nel riquadro sinistro fare clic sul segno più verde.
4. Digitare "Kaspersky Hybrid Cloud Security" nel campo di ricerca del menu.

   Kaspersky Hybrid Cloud Security è una combinazione di Kaspersky Security Center e di due applicazioni di protezione per la protezione delle istanze: Kaspersky Endpoint Security for Linux e Kaspersky Security for Windows Server.

5. Nell'elenco dei risultati selezionare Kaspersky Hybrid Cloud Security o Kaspersky Hybrid Cloud Security (BYOL).

   Nella parte destra dello schermo verrà visualizzata una finestra di informazioni.

6. Leggere le informazioni e fare clic sul pulsante Crea nella parte inferiore della finestra delle informazioni.
7. Compilare tutti i campi necessari. Utilizzare le descrizioni comandi per ottenere informazioni e assistenza.
8. Quando si seleziona la dimensione, selezionare una delle opzioni con tre stelle.

   Nella maggior parte dei casi, 8 gigabyte (GB) di RAM sono sufficienti. Tuttavia, in Azure, è possibile aumentare le dimensioni della RAM e altre risorse della macchina virtuale in qualsiasi momento.

9. Quando si seleziona un database, selezionare una delle opzioni seguenti, a seconda del piano in uso:

   - Locale - Se si desidera un database nella stessa macchina virtuale in cui sarà distribuito l'Administration Server. Kaspersky Security Center include un database SQL Server Express. Selezionare questa opzione se SQL Server Express è sufficiente per le proprie esigenze.

   - Nuovo - Se si desidera un nuovo database RDS nell'ambiente Azure. Scegliere questa opzione se si desidera un sistema DBMS diverso da SQL Server Express. I dati verranno trasferiti nell'ambiente cloud, dove resteranno archiviati, senza costi aggiuntivi.

   - Esistente - Se si desidera utilizzare un server di database esistente. In questo caso, sarà necessario specificare la posizione. Se il server è esterno all'ambiente Azure, i dati verranno trasferiti via Internet. Tale operazione può comportare costi aggiuntivi.

10. Quando si immette l'ID della sottoscrizione, utilizzare la sottoscrizione che è stata creata in precedenza.

    Dopo la distribuzione, è possibile connettersi all'Administration Server tramite RDP. È possibile utilizzare Administration Console per lavorare con l'Administration Server.

Utilizzo di Azure SQL

In questa sezione vengono descritte le azioni da eseguire per preparare un database Microsoft Azure per Kaspersky Security Center, preparare un account di archiviazione Azure ed eseguire la migrazione di un database esistente ad Azure SQL.

SQL Database è un servizio gestito di database relazionale generico in Microsoft Azure.

> Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Creazione dell'account di archiviazione Azure

È necessario creare un account di archiviazione in Microsoft Azure per l'utilizzo del database Azure SQL e degli script di distribuzione.

Per creare un account di archiviazione:

1. Accedere al portale di Azure.

2. Nel riquadro sinistro selezionare **Account di archiviazione** per aprire la finestra **Account di archiviazione**.

3. Nella finestra **Account di archiviazione** fare clic sul pulsante **Aggiungi** per passare alla finestra **Crea account di archiviazione**.

4. Compilare tutti i campi necessari per creare un account di archiviazione:

   - Posizione: deve corrispondere alla posizione di Administration Server.
   - Altri campi: è possibile mantenere i valori predefiniti.

   Utilizzare le descrizioni comandi per ottenere informazioni su ogni campo.

   Dopo aver creato l'account di archiviazione, viene visualizzato l'elenco degli account di archiviazione.

5. Nell'elenco degli account di archiviazione fare clic sul nome dell'account creato per visualizzare le informazioni su tale account.

6. Assicurarsi di conoscere il nome dell'account, il gruppo di risorse e le chiavi di accesso per questo account di archiviazione. Queste informazioni sono necessarie per l'utilizzo di Kaspersky Security Center.

Per assistenza, è possibile fare riferimento al sito Web di Azure.

Se si dispone già di un account di archiviazione, è possibile utilizzarlo con Kaspersky Security Center.

Creazione del database SQL Azure e del server SQL

Sono necessari un database SQL e un server SQL nell'ambiente Azure.

Per creare un database SQL Azure e un server SQL:

1. Seguire le istruzioni sul sito Web di Azure.

   È possibile creare un nuovo server quando richiesto da Microsoft Azure. Se si dispone già di un server SQL Azure, è possibile utilizzarlo per Kaspersky Security Center anziché crearne uno nuovo.

2. Dopo aver creato il database SQL e il server SQL, assicurarsi di conoscere il nome della risorsa e il gruppo di risorse:

   a. Visitare https://portal.azure.com e verificare di aver eseguito l'accesso.

   b. Nel riquadro sinistro selezionare i **database SQL**.

   c. Fare clic sul nome di un database nell'elenco dei database.

      Verrà visualizzata la finestra delle proprietà.

   d. Il nome del database è il nome della risorsa. Il nome del gruppo di risorse viene visualizzato nella sezione **Panoramica** della finestra delle proprietà.

Sono necessari il nome della risorsa e il gruppo di risorse del database per la migrazione al database SQL di Azure.

Migrazione del database ad Azure SQL

Dopo la distribuzione di Administration Server nell'ambiente Azure, è possibile eseguire la migrazione del database di Kaspersky Security Center da un dispositivo locale ad Azure SQL. È necessario un account di archiviazione Azure per un database Azure SQL. È inoltre necessario disporre di Microsoft SQL Server Data-Tier Application Framework (DacFx) e SQLSysCLRTypes nell'Administration Server.

Per eseguire la migrazione del database:

1. Verificare di avere creato un account di archiviazione Azure.
2. Verificare di disporre di SQLSysCLRTypes e DacFx in Administration Server.

   È possibile scaricare Microsoft SQL Server Data-Tier Application Framework (17.0.1 DacFx) e SQLSysCLRTypes (scegliere la versione corrispondente alla propria versione di SQL Server) dal sito Web ufficiale di Microsoft.
3. Nell'Administration Server fisico (locale) eseguire l'utilità di backup di Kaspersky per eseguire il backup dei dati di Administration Server con l'opzione **Esegui la migrazione al formato Azure** abilitata.
4. Copiare il file di backup nell'Administration Server Azure.

   Verificare che lo spazio su disco sia sufficiente nella macchina virtuale di Azure in cui è installato Administration Server. Nell'ambiente Azure è possibile aggiungere spazio su disco alle macchine virtuali in base ai requisiti del processo di migrazione del database.
5. In Administration Server nell'ambiente Microsoft Azure avviare nuovamente l'utilità di backup di Kaspersky in modalità interattiva.

   Verrà avviata la Procedura guidata di backup e ripristino.
6. Nel passaggio **Seleziona azione** selezionare **Ripristina dati di Administration Server** e fare clic su **Avanti**.
7. Nel passaggio **Ripristinare le impostazioni** fare clic sul pulsante **Sfoglia** accanto a **Cartella per l'archiviazione delle copie di backup**.

8. Nella finestra **Accedere all'archivio online** visualizzata compilare i seguenti campi e fare clic su **OK**:

   - **Nome dell'account di archiviazione Azure**

     È stato creato il nome dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

   - **Cartella di backup**

     Specificare il percorso della cartella di archiviazione da utilizzare per il backup.

   - **ID sottoscrizione Azure**

     La sottoscrizione è stata creata dall'utente nel portale di Azure.

   - **Password dell'applicazione Azure**

     La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

     I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

   - **Chiave di accesso all'archivio Azure**

     Disponibile nelle proprietà dell'account di archiviazione, nella sezione Chiavi di accesso. È possibile utilizzare qualsiasi chiave (chiave1 o chiave2).

   - **Nome del server SQL Azure**

     Disponibile nelle proprietà del server SQL Azure.

   - **Gruppo di risorse del server SQL Azure**

     Disponibile nelle proprietà del server SQL Azure.

   - **ID applicazione Azure**

     L'ID applicazione è stato creato dall'utente nel portale di Azure.

     È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

9. Selezionare l'opzione **Esegui la migrazione dal backup locale**.

   Il pulsante **Sfoglia** diventa disponibile.

10. Fare clic sul pulsante **Sfoglia** per scegliere la cartella nell'Administration Server Azure in cui è stato copiato il file di backup.

11. Fare clic su **Avanti** e completare la procedura.

I dati verranno ripristinati nel database Azure SQL utilizzando l'archivio Azure. È possibile utilizzare questo database per ulteriori operazioni con Kaspersky Security Center nell'ambiente Azure.

Gli indirizzi delle pagine Web citate in questo documento sono corretti alla data di rilascio di Kaspersky Security Center.

Utilizzo in Google Cloud

Questa sezione contiene informazioni sull'utilizzo di Kaspersky Security Center in un ambiente cloud fornito da Google.

Creazione di e-mail client, ID progetto e chiave privata

È possibile avvalersi dell'API di Google per utilizzare Kaspersky Security Center in Google Cloud Platform. È richiesto un account Google. Per ulteriori informazioni, fare riferimento alla documentazione di Google all'indirizzo https://cloud.google.com.

Sarà necessario creare e fornire a Kaspersky Security Center le seguenti credenziali:

- **E-mail client**

  L'e-mail client è l'indirizzo e-mail utilizzato per la registrazione del progetto in Google Cloud.

- **ID progetto**

  L'ID progetto è l'ID ricevuto durante la registrazione del progetto in Google Cloud.

- **Chiave privata**

  La chiave privata è la sequenza di caratteri ricevuta come chiave privata durante la registrazione del progetto in Google Cloud. È consigliabile copiare e incollare questa sequenza per evitare errori.

Utilizzo di Google Cloud SQL per l'istanza MySQL

È possibile creare un database in Google Cloud e utilizzare questo database per Kaspersky Security Center.

Kaspersky Security Center funziona con MySQL 5.7 e 5.6. Altre versioni di MySQL non sono state testate.

Per creare e configurare un database MySQL:

Nel browser accedere a https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen e seguire le istruzioni fornite.

Quando si configura un database MySQL, utilizzare i seguenti flag:

- **sort_buffer_size** 10000000
- **join_buffer_size** 20000000
- **innodb_lock_wait_timeout** 300
- **max_allowed_packet** 32000000
- **innodb_thread_concurrency** 20
- **max_connections** 151
- **tmp_table_size** 67108864
- **max_heap_table_size** 67108864
- **lower_case_table_names** 1

Prerequisiti dei dispositivi client in un ambiente cloud per l'utilizzo di Kaspersky Security Center

I dispositivi in cui si intende installare Administration Server, Network Agent e le applicazioni di protezione Kaspersky devono essere soddisfare le seguenti condizioni:

- La configurazione dei gruppi di protezione rende disponibili le seguenti porte in Administration Server (set minimo di porte richieste per la distribuzione):
  - 8060 HTTP—Per il trasferimento dei pacchetti di installazione di Network Agent e dei pacchetti di installazione delle applicazioni di protezione da Administration Server alle istanze protette
  - 8061 HTTPS—Per il trasferimento dei pacchetti di installazione di Network Agent e dei pacchetti di installazione delle applicazioni di protezione da Administration Server alle istanze protette
  - 13000 TCP—Per i trasferimenti dalle istanze protette e dagli Administration Server secondari all'Administration Server primario tramite SSL
  - 13000 UDP—Per il trasferimento delle informazioni sull'arresto delle istanze all'Administration Server
  - 14000 TCP—Per i trasferimenti dalle istanze protette e dagli Administration Server secondari all'Administration Server primario senza utilizzare SSL
  - 13291—Per la connessione di Administration Console all'Administration Server
  - 40080—Per l'esecuzione degli script di distribuzione

  È possibile configurare i gruppi di protezione nella console di gestione AWS o nel portale di Azure. Se si intende utilizzare Kaspersky Security Center in una configurazione non predefinita, fare riferimento alla Knowledge Base. Esempi di configurazioni non predefinite includono l'installazione di Administration Console nella propria workstation anziché nel dispositivo di Administration Server o l'utilizzo di un server proxy KSN.
- La porta 15000 UDP è disponibile nei dispositivi client (per la ricezione delle richieste di comunicazione con Administration Server).

- Nell'ambiente cloud AWS:
  - Se si prevede di utilizzare l'API AWS, è impostato il ruolo IAM con cui le applicazioni verranno installate nelle istanze.
  - In ogni istanza Amazon EC2, l'agente SSM (Systems Manager Agent) è installato e in esecuzione.
  - L'agente SSM consente a Kaspersky Security Center di installare automaticamente le applicazioni nei dispositivi e nei gruppi di dispositivi senza richiedere conferma ogni volta all'amministratore.
  - Nelle istanze in cui è in esecuzione un sistema operativo Windows e che sono state distribuite da AMI dopo novembre 2016 l'agente SSM è installato e in esecuzione. È necessario installare manualmente l'agente SSM in tutti gli altri dispositivi. Per informazioni dettagliate sull'installazione dell'agente SSM nei dispositivi che eseguono sistemi operativi Windows e Linux, consultare la pagina della Guida AWS.
- Nell'ambiente cloud Microsoft Azure:
  - In ogni macchina virtuale di Azure, l'agente di macchine virtuali di Azure è installato e in esecuzione.

    Per impostazione predefinita, una nuova macchina virtuale viene creata con l'agente di macchine virtuali di Azure e non è necessario installarlo o abilitarlo manualmente. Fare riferimento alle pagine della Guida di Microsoft per informazioni dettagliate sull'agente di macchine virtuali di Azure nei dispositivi Windows e nei dispositivi Linux.
  - L'ID applicazione Azure dispone dei seguenti ruoli:
    - Lettore (per individuare le macchine virtuali utilizzando il polling)
    - Collaboratore Macchina virtuale (per distribuire la protezione nelle macchine virtuali)
    - Collaboratore SQL Server (per utilizzare un database SQL nell'ambiente Microsoft Azure)

    Se si desidera eseguire tutte queste operazioni, assegnare tutti e tre i ruoli all'ID applicazione Azure.

Creazione dei pacchetti di installazione necessari per la configurazione dell'ambiente cloud

La procedura guidata Configura ambiente cloud in Kaspersky Security Center è disponibile se si dispone dei pacchetti di installazione e dei plug-in di gestione per i seguenti programmi:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

  La distribuzione di Kaspersky Endpoint Security for Windows in un ambiente cloud sarà disponibile dopo l'imminente rilascio di Kaspersky Endpoint Security 12.0 for Windows.
- Kaspersky Security for Windows Server

Questi pacchetti di installazione sono necessari per l'installazione delle applicazioni nelle istanze o nelle macchine virtuali che si desidera proteggere. Se non si dispone di questi pacchetti di installazione, è necessario crearli. In caso contrario, la procedura guidata Configura ambiente cloud non può funzionare.

Per creare i pacchetti di installazione:

1. Scaricare le versioni più recenti delle applicazioni e dei plug-in dal sito Web di Kaspersky:
   - Il programma di installazione e il plug-in di gestione per Kaspersky Security for Windows Server.
   - Il programma di installazione, i file per l'installazione remota tramite Kaspersky Security Center e il plug-in di gestione per Kaspersky Endpoint Security for Linux.
2. Salvare tutti i file nell'istanza (o macchina virtuale) in cui è installato Administration Server.
3. Estrarre i file da tutti i pacchetti.
4. Avviare Kaspersky Security Center.
5. Nella struttura della console accedere a **Avanzate** → **Installazione remota** → **Pacchetti di installazione** e fare clic su **Crea pacchetto di installazione**.
6. Selezionare **Crea pacchetto di installazione di Kaspersky**.
7. Specificare il nome del pacchetto e il percorso del programma di installazione dell'applicazione:<cartella> \ <nome file>.kud, quindi fare clic su **Avanti**.
8. Leggere il Contratto di licenza con l'utente finale e selezionare la casella di controllo per confermare che si accettano i termini, quindi fare clic su **Avanti**.

Il pacchetto di installazione verrà caricato in Administration Server e sarà disponibile nell'elenco dei pacchetti di installazione.

La configurazione di un ambiente cloud diventa disponibile non appena si creano i pacchetti di installazione e si installano i plug-in di gestione in Administration Server.

Configurazione dell'ambiente cloud

Per configurare Kaspersky Security Center con la procedura guidata Configura ambiente cloud, sono necessari i seguenti prerequisiti:

- Credenziali specifiche per un ambiente cloud:
  - Un ruolo IAM che dispone dei diritti per il polling del segmento cloud o un account utente IAM che dispone dei diritti per il polling del segmento cloud (per l'utilizzo con Amazon Web Services)
  - ID applicazione Azure, password e sottoscrizione (per l'utilizzo con Microsoft Azure)
  - E-mail client Google, ID progetto e chiave privata (per l'utilizzo con Google Cloud)
- Pacchetti di installazione:
  - Network Agent per Windows
  - Network Agent per Linux
  - Kaspersky Endpoint Security for Linux

- Plug-in Web per Kaspersky Endpoint Security for Linux
- Almeno uno dei seguenti componenti:
  - Pacchetto di installazione e plug-in Web per Kaspersky Endpoint Security for Windows (consigliato)
  - Pacchetto di installazione e plug-in Web per Kaspersky Security for Windows Server

Se non si desidera utilizzare le funzionalità per l'ambiente cloud (ad esempio, se si intende gestire solo la protezione dei dispositivi client fisici), è possibile chiudere la procedura guidata Configura ambiente cloud ed eseguire manualmente l'Avvio rapido guidato di Administration Server.

L'operazione Configura ambiente cloud viene avviato automaticamente la prima volta che ci si connette ad Administration Server tramite Administration Console se si sta distribuendo Kaspersky Security Center da un'immagine pronta all'uso. È anche possibile avviare la procedura guidata Configura ambiente cloud manualmente in qualsiasi momento.

Per avviare manualmente la procedura guidata Configura ambiente cloud:

1. Nella struttura della console selezionare il nodo **Administration Server**.
2. Nel menu di scelta rapida del nodo selezionare **Tutte le attività** → **Configura ambiente cloud**.

La sessione di lavoro media ha una durata di circa 15 minuti.

Informazioni sulla procedura guidata Configura ambiente cloud

La procedura guidata Configura ambiente cloud consente di configurare Kaspersky Security Center in considerazione delle specifiche di utilizzo in un ambiente cloud.

La procedura guidata crea i seguenti oggetti:

- Criterio di Network Agent con le impostazioni predefinite
- Criteri per Kaspersky Endpoint Security for Linux
- Criteri per Kaspersky Security for Windows Server
- Gruppo di amministrazione per le istanze e una regola per lo spostamento automatico delle istanze in questo gruppo di amministrazione
- Attività di backup dei dati di Administration Server
- Attività per l'installazione della protezione nei dispositivi che eseguono Windows e Linux
- Attività per ogni dispositivo gestito:
  - Scansione malware rapida
  - Download degli aggiornamenti

Se è stata selezionata l'opzione di licenza BYOL, la configurazione dell'ambiente cloud attiva anche Kaspersky Security Center con un file chiave o un codice di attivazione e inserisce il file chiave o il codice di attivazione nell'archivio delle licenze.

Passaggio 1. Selezione del metodo di attivazione dell'applicazione

Questo passaggio non viene visualizzato se è stata eseguita la registrazione a una delle AMI pronte all'uso (in AWS Marketplace) o a uno SKU con fatturazione mensile basato sull'utilizzo (in Azure Marketplace). In questo caso, la procedura guidata procede immediatamente al passaggio successivo. Tuttavia, non è possibile acquistare un'AMI pronta all'uso per Google Cloud.

Se è stata selezionata l'opzione di licenza BYOL per Kaspersky Security Center, la procedura guidata richiede di selezionare il metodo di attivazione dell'applicazione.

Attivare l'applicazione con un codice di attivazione (o un file chiave) per Kaspersky Security for Virtualization o per Kaspersky Hybrid Cloud Security.

È possibile attivare l'applicazione in uno dei seguenti modi:

- Immettendo un codice di attivazione.

  Verrà avviata l'attivazione online. Nel corso del processo vengono eseguite la verifica del codice di attivazione specificato, nonché l'emissione e l'attivazione di un file chiave.

- Specificando un file chiave.

  L'applicazione controllerà il file chiave e lo attiverà se contiene le informazioni corrette o richiederà di specificare un altro file chiave.

Kaspersky Security Center inserisce la chiave di licenza nell'archivio delle licenze e la contrassegna come distribuita automaticamente nei dispositivi gestiti.

Se ci si connette a un'istanza utilizzando il componente standard di Microsoft Windows Connessione Desktop remoto o un'applicazione simile, nelle proprietà della connessione remota è necessario specificare l'unità del dispositivo fisico utilizzato per la connessione. Questo garantisce l'accesso dall'istanza ai file nel dispositivo fisico e consente di selezionare e specificare il file chiave.

Se si utilizza Kaspersky Security Center distribuito da un'AMI a pagamento o per uno SKU con fatturazione mensile basato sull'utilizzo, non è possibile aggiungere file chiave o codici di attivazione all'archivio delle licenze.

Passaggio 2. Selezione dell'ambiente cloud

Selezionare l'ambiente cloud in cui distribuire Kaspersky Security Center: AWS, Azure o Google Cloud.

Passaggio 3. Autorizzazione nell'ambiente cloud

AWS

Se è stato selezionato AWS, specificare che si dispone di un ruolo IAM con i diritti richiesti o fornire a Kaspersky Security Center una chiave di accesso AWS IAM. Non è possibile eseguire il polling dei segmenti cloud senza un ruolo IAM o una chiave di accesso AWS IAM.

Specificare le seguenti impostazioni per la connessione da utilizzare per il polling dei segmenti cloud:

- **Nome della connessione**

  Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

  Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

  Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

- **Usa ruolo IAM AWS**

  Selezionare questa opzione se è stato già creato un ruolo IAM per l'utilizzo dei servizi AWS da parte di Administration Server.

- **Usa account utente IAM AWS**

  Selezionare questa opzione se si dispone di un account utente IAM con le autorizzazioni richieste ed è possibile immettere un ID chiave e una chiave segreta.

  - **ID chiave di accesso**

    L'ID chiave di accesso IAM è una sequenza di caratteri alfanumerici. L'ID chiave è stato ricevuto al momento della creazione dell'account utente IAM.

    Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

  - **Chiave segreta**

    Chiave segreta ricevuta con l'ID chiave di accesso al momento della creazione dell'account utente IAM.

    I caratteri della chiave segreta sono visualizzati come asterischi. Quando si inizia a immettere la chiave segreta, viene visualizzato il pulsante **Mostra**. Tenere premuto questo pulsante per visualizzare i caratteri immessi.

    Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

La connessione viene salvata nelle impostazioni dell'applicazione. È possibile creare una sola chiave di accesso AWS IAM con Configura ambiente cloud. Successivamente è possibile specificare più connessioni per gestire altri segmenti cloud.

Se si desidera installare le applicazioni nelle istanze tramite Kaspersky Security Center, è necessario verificare che il ruolo IAM (o l'utente IAM il cui account è associato alla chiave immessa) disponga di tutte le autorizzazioni richieste.

Azure

Se è stato selezionato Azure, specificare le seguenti impostazioni per la connessione da utilizzare per il polling del segmento cloud:

- **Nome della connessione**

  Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

  Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

  Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

- **ID applicazione Azure**

  L'ID applicazione è stato creato dall'utente nel portale di Azure.

  È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

- **ID sottoscrizione Azure**

  La sottoscrizione è stata creata dall'utente nel portale di Azure.

- **Password dell'applicazione Azure**

  La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

  I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

- **Nome dell'account di archiviazione Azure**

  È stato creato il nome dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

- **Chiave di accesso all'archivio Azure**

  È stata ricevuta una password (chiave) durante la creazione dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

  La chiave è disponibile nella sezione "Panoramica dell'account di archiviazione Azure", nella sottosezione "Chiavi".

La connessione viene salvata nelle impostazioni dell'applicazione.

Google Cloud

Se è stato selezionato Google Cloud, specificare le seguenti impostazioni per la connessione da utilizzare per il polling del segmento cloud:

- **Nome della connessione**

  Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

  Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

  Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

- **E-mail client**

  L'e-mail client è l'indirizzo e-mail utilizzato per la registrazione del progetto in Google Cloud.

- **ID progetto**

  L'ID progetto è l'ID ricevuto durante la registrazione del progetto in Google Cloud.

- **Chiave privata**

  La chiave privata è la sequenza di caratteri ricevuta come chiave privata durante la registrazione del progetto in Google Cloud. È consigliabile copiare e incollare questa sequenza per evitare errori.

La connessione viene salvata nelle impostazioni dell'applicazione.

Passaggio 4. Configurazione della sincronizzazione con Cloud e selezione delle azioni successive

In questo passaggio viene avviato il polling dei segmenti cloud e viene creato uno speciale gruppo di amministrazione per le istanze. Le istanze rilevate durante il polling vengono inserite in questo gruppo. Viene configurata la pianificazione del polling dei segmenti cloud (per impostazione predefinita, ogni 5 minuti).

Viene inoltre creata una regola di spostamento automatico **Sincronizza con il cloud**. Per ogni successiva scansione della rete cloud, i dispositivi virtuali rilevati verranno spostati nel sottogruppo corrispondente all'interno del gruppo **Dispositivi gestiti\Cloud**.

Nella pagina **Sincronizzazione con il segmento cloud** è possibile definire le seguenti impostazioni:

- **Sincronizza struttura di gruppi di amministrazione con il segmento cloud**

  Se questa opzione è abilitata, viene creato automaticamente il gruppo **Cloud** all'interno del gruppo **Dispositivi gestiti** e viene avviata una device discovery cloud. Le istanze e le macchine virtuali rilevate durante ciascuna scansione della rete cloud sono inserite nel gruppo Cloud. La struttura dei sottogruppi di amministrazione all'interno di questo gruppo corrisponde alla struttura del segmento cloud (in AWS, le zone di disponibilità e i gruppi di collocazione non sono rappresentati nella struttura; in Azure, le subnet non sono rappresentate nella struttura). I dispositivi che non sono stati identificati come istanze nell'ambiente cloud si trovano nel gruppo **Dispositivi non assegnati**. La struttura di questo gruppo consente di utilizzare le attività di installazione di gruppo per installare le applicazioni anti-virus nelle istanze, nonché di configurare diversi criteri per diversi gruppi.

  Se questa opzione è disabilitata, viene creato il gruppo **Cloud** e viene avviata una device discovery cloud, tuttavia all'interno del gruppo non vengono creati i sottogruppi che corrispondono alla struttura del segmento cloud. Tutte le istanze rilevate si trovano nel gruppo di amministrazione **Cloud**, pertanto vengono visualizzate in un unico elenco. Se l'utilizzo di Kaspersky Security Center richiede la sincronizzazione, è possibile modificare le proprietà della regola **Sincronizza con il cloud** e quindi applicarla. Applicando la regola viene modificata la struttura dei sottogruppi nel gruppo Cloud in modo da creare la corrispondenza con la struttura del segmento cloud.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Distribuisci protezione**

  Se questa opzione è selezionata, la procedura guidata crea un'attività per l'installazione delle applicazioni di protezione nelle istanze. Al termine della procedura guidata, verrà avviata automaticamente la Distribuzione guidata della protezione nei dispositivi nei segmenti cloud e sarà possibile installare Network Agent e le applicazioni di protezione in tali dispositivi.

  Kaspersky Security Center può eseguire la distribuzione tramite i propri strumenti nativi. Se non si dispone delle autorizzazioni per installare le applicazioni in istanze EC2 o nelle macchine virtuali Azure, è possibile configurare l'attività **Installazione remota** manualmente e specificare un account con le autorizzazioni richieste. In questo caso l'attività di installazione remota non funzionerà per i dispositivi rilevati utilizzando API AWS o Azure. Questa attività funzionerà solo per i dispositivi rilevati tramite il polling di Active Directory, dei domini Windows o dell'intervallo IP.

  Se questa opzione è deselezionata, la Distribuzione guidata della protezione non viene avviata e non vengono create attività per l'installazione delle applicazioni di protezione nelle istanze. È possibile eseguire manualmente entrambe le operazioni in un secondo momento.

Per Google Cloud, è possibile eseguire la distribuzione solo con gli strumenti nativi di Kaspersky Security Center. Se è stato selezionato Google Cloud, l'opzione **Distribuisci protezione** non è disponibile.

Passaggio 5. Configurazione di Kaspersky Security Network nell'ambiente cloud

Specificare le impostazioni per la trasmissione delle informazioni sulle operazioni di Kaspersky Security Center alla Knowledge Base di Kaspersky Security Network. Selezionare una delle seguenti opzioni:

- **Accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center e le applicazioni gestite installate nei dispositivi client trasferiranno automaticamente i dettagli sull'esecuzione a Kaspersky Security Network. La partecipazione a Kaspersky Security Network garantisce aggiornamenti più rapidi dei database contenenti le informazioni sui virus e sulle altre minacce, assicurando una risposta più rapida alle minacce per la sicurezza emergenti.

- **Non accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center e le applicazioni gestite non forniranno informazioni a Kaspersky Security Network.

  Se si seleziona questa opzione, l'utilizzo di Kaspersky Security Network sarà disabilitato.

Kaspersky consiglia la partecipazione a Kaspersky Security Network.

Passaggio 6. Configurazione delle notifiche e-mail nell'ambiente cloud

Configurare l'invio di notifiche relative agli eventi registrati durante l'esecuzione delle applicazioni Kaspersky nei dispositivi client virtuali. Queste impostazioni verranno utilizzate come impostazioni predefinite per i criteri dell'applicazione.

Per configurare l'invio di notifiche relative agli eventi che si verificano nelle applicazioni Kaspersky, utilizzare le seguenti impostazioni:

- **Destinatari (indirizzi e-mail)**

  Gli indirizzi e-mail degli utenti a cui l'applicazione invierà le notifiche. È possibile immettere uno o più indirizzi; se si immette più di un indirizzo, separarli con un punto e virgola.

- **Server SMTP**

  L'indirizzo o gli indirizzi dei server di posta dell'organizzazione.

  Se si immette più di un indirizzo, separarli con un punto e virgola. È possibile utilizzare i seguenti valori:

  - Indirizzo IPv4 o IPv6
  - Nome di rete Windows (nome NetBIOS) del dispositivo
  - Nome DNS del server SMTP

- **Porta server SMTP**

  Numero di porta di comunicazione del server SMTP. Se si utilizzano più server SMTP, la connessione a questi viene stabilita tramite la porta di comunicazione specificata. Il numero di porta predefinito è 25.

- **Usa autenticazione ESMTP**

  Abilita il supporto dell'autenticazione ESMTP. Quando la casella di controllo è selezionata, nei campi **Nome utente** e **Password** è possibile specificare le impostazioni per l'autenticazione ESMTP. Per impostazione predefinita, questa casella di controllo è deselezionata.

È possibile verificare le nuove impostazioni di notifica e-mail facendo clic sul pulsante **Invia messaggio di prova**. Se è stato ricevuto il messaggio di prova all'indirizzo specificato nel campo **Destinatari (indirizzi e-mail)**, le impostazioni sono state configurate correttamente.

Passaggio 7. Creazione di una configurazione iniziale della protezione dell'ambiente cloud

In questo passaggio Kaspersky Security Center crea automaticamente criteri e attività. La finestra **Configura protezione iniziale** visualizza un elenco dei criteri e delle attività creati dall'applicazione.

Se si utilizza un database RDS nell'ambiente cloud AWS, è necessario specificare la coppia di chiavi di accesso IAM in Kaspersky Security Center durante la creazione dell'attività di backup di Administration Server. In questo caso, compilare i seguenti campi:

- **Nome del bucket S3**

  Nome del bucket S3 che è stato creato per il backup.

- **ID chiave di accesso**

  L'ID chiave (sequenza di caratteri alfanumerici) è stato ricevuto al momento della creazione dell'account utente IAM per l'utilizzo dell'istanza di archiviazione del bucket S3.

  Il campo è disponibile se è stato selezionato il database RDS in un bucket S3.

- **Chiave segreta**

  Chiave segreta ricevuta con l'ID chiave di accesso al momento della creazione dell'account utente IAM.

  I caratteri della chiave segreta sono visualizzati come asterischi. Quando si inizia a immettere la chiave segreta, viene visualizzato il pulsante **Mostra**. Tenere premuto questo pulsante per visualizzare i caratteri immessi.

  Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

Se si utilizza un database SQL Azure nell'ambiente cloud Azure, è necessario specificare le informazioni sul server SQL Azure in Kaspersky Security Center durante la creazione dell'attività di backup di Administration Server. In questo caso, compilare i seguenti campi:

- **Nome dell'account di archiviazione Azure**

  È stato creato il nome dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

- **ID sottoscrizione Azure**

  La sottoscrizione è stata creata dall'utente nel portale di Azure.

- **Password dell'applicazione Azure**

  La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

  I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

- **ID applicazione Azure**

  L'ID applicazione è stato creato dall'utente nel portale di Azure.

  È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

- **Nome del server SQL Azure**

  Il nome e il gruppo di risorse sono disponibili nelle proprietà del server SQL Azure.

- **Gruppo di risorse del server SQL Azure**

  Il nome e il gruppo di risorse sono disponibili nelle proprietà del server SQL Azure.

- **Chiave di accesso all'archivio Azure**

  Disponibile nelle proprietà dell'account di archiviazione, nella sezione Chiavi di accesso. È possibile utilizzare qualsiasi chiave (chiave1 o chiave2).

Se è in corso la distribuzione di Administration Server in Google Cloud, è necessario selezionare una cartella in cui verranno archiviate le copie di backup. Selezionare una cartella nel dispositivo locale o una cartella nell'istanza di una macchina virtuale.

Il pulsante **Avanti** diventa disponibile dopo la creazione di tutti i criteri e le attività che sono necessari per la configurazione minima della protezione.

Se un dispositivo in cui devono essere eseguite le attività non è visibile per l'Administration Server, le attività vengono avviate solo quando il dispositivo diventa visibile. Se si crea una nuova istanza EC2 o una nuova macchina virtuale di Azure, potrebbe essere necessario un certo tempo prima che risulti visibile per l'Administration Server. Se si desidera che Network Agent e le applicazioni di protezione vengano installati appena possibile in tutti i nuovi dispositivi creati, verificare che l'opzione **Esegui attività non effettuate** sia abilitata per l'attività **Installa l'applicazione in remoto**. In caso contrario, Network Agent e le applicazioni di protezione non verranno installati in una nuova istanza o macchina virtuale creata finché l'attività non viene avviata in base alla relativa pianificazione.

Passaggio 8. Selezione dell'azione nel momento in cui deve essere riavviato il sistema operativo durante l'installazione (per l'ambiente cloud)

Se precedentemente è stata selezionata l'opzione **Distribuisci protezione**, è necessario scegliere quale operazione eseguire quando il sistema operativo di un dispositivo di destinazione deve essere riavviato. Se non è stata selezionata l'opzione **Distribuisci protezione**, questo passaggio viene ignorato.

Scegliere se riavviare le istanze qualora il sistema operativo del dispositivo debba essere riavviato durante l'installazione delle applicazioni:

- **Non riavviare il dispositivo**

  Se questa opzione è selezionata, il dispositivo non verrà riavviato dopo l'installazione dell'applicazione di protezione.

- **Riavvia il dispositivo**

  Se questa opzione è selezionata, il dispositivo verrà riavviato dopo l'installazione dell'applicazione di protezione.

Se si desidera forzare la chiusura delle applicazioni nelle sessioni bloccate nelle istanze prima del riavvio, selezionare la casella di controllo **Forza chiusura delle applicazioni nelle sessioni bloccate**. Se questa casella di controllo è deselezionata, sarà necessario chiudere manualmente tutte le applicazioni in esecuzione nelle istanze bloccate.

Passaggio 9. Ricezione degli aggiornamenti da parte di Administration Server

In questo passaggio è possibile visualizzare lo stato di avanzamento del download degli aggiornamenti per il corretto funzionamento di Administration Server. È possibile fare clic sul pulsante **Avanti** senza attendere il completamento del download per passare alla pagina finale della procedura guidata.

La procedura guidata verrà completata.

Controllo della configurazione

Per verificare se Kaspersky Security Center 15.1 è stato configurato per l'utilizzo in un ambiente cloud:

1. Avviare Kaspersky Security Center e verificare che sia possibile connettersi all'Administration Server tramite Administration Console.
2. Nella struttura della console selezionare **Dispositivi gestiti\Cloud**.
3. Durante la visualizzazione dei sottogruppi nel gruppo **Dispositivi gestiti\Cloud** verificare che la scheda **Dispositivi** visualizzi tutti i dispositivi di tale sottogruppo.

   Se i dispositivi non vengono visualizzati, è possibile eseguire manualmente il polling dei segmenti cloud corrispondenti per trovarli.
4. Verificare che la scheda **Criteri** disponga di criteri attivi per le seguenti applicazioni:
   - Kaspersky Security Center Network Agent
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   Se non sono presenti nell'elenco, è possibile crearli manualmente.
5. Verificare che la scheda **Attività** elenchi le seguenti attività:
   - **Backup dei dati di Administration Server**
   - **Attività di aggiornamento per Windows Server**
   - **Manutenzione di Administration Server**
   - **Scarica aggiornamenti nell'archivio dell'Administration Server**
   - **Trova vulnerabilità e aggiornamenti richiesti**
   - **Installa la protezione per Windows**
   - **Installa la protezione per Linux**
   - **Attività di scansione rapida per Windows Server**
   - **Scansione rapida**
   - **Installa gli aggiornamenti per Linux**

   Se non sono presenti nell'elenco, è possibile crearli manualmente.

Kaspersky Security Center 15.1 è stato configurato per l'utilizzo in un ambiente cloud.

Gruppo di dispositivi Cloud

È possibile gestire i dispositivi cloud organizzandoli in gruppi. Durante la configurazione iniziale di Kaspersky Security Center, il gruppo di amministrazione **Dispositivi gestiti\Cloud** viene creato per impostazione predefinita e i dispositivi cloud rilevati durante il polling vengono inseriti in questo gruppo.

Se è stata selezionata l'opzione **Sincronizza struttura di gruppi di amministrazione con il segmento cloud** quando è stata configurata la sincronizzazione, la struttura dei sottogruppi in questo gruppo di amministrazione è identica alla struttura dei segmenti cloud. Tuttavia, in AWS, le zone di disponibilità e i gruppi di collocazione non sono rappresentati nella struttura; in Microsoft Azure, le subnet non sono rappresentate nella struttura. I sottogruppi vuoti all'interno del gruppo rilevati durante il polling vengono eliminati automaticamente.

È inoltre possibile creare manualmente i gruppi di amministrazione, combinando tutti dispositivi o dispositivi specifici.

Per impostazione predefinita, il gruppo **Dispositivi gestiti\Cloud** eredita criteri e attività dal gruppo **Dispositivi gestiti**. È possibile modificare le impostazioni se le caselle di controllo **Modifica consentita** sono selezionate nelle proprietà delle impostazioni dei criteri e delle attività corrispondenti.

Polling dei segmenti di rete

Le informazioni sulla struttura e sui dispositivi della rete vengono ricevute dall'Administration Server tramite il polling periodico dei segmenti cloud mediante gli strumenti API AWS, API Azure o API Google. Kaspersky Security Center utilizza queste informazioni per aggiornare il contenuto delle cartelle **Dispositivi non assegnati** e **Dispositivi gestiti**. Se i dispositivi sono stati configurati in modo da essere spostati automaticamente nei gruppi di amministrazione, i dispositivi rilevati sono inclusi nei gruppi di amministrazione.

Per consentire ad Administration Server di eseguire il polling dei segmenti cloud, è necessario disporre dei diritti forniti con un ruolo IAM o un account utente IAM (in AWS) o con un ID applicazione e una password (in Azure) o con l'e-mail client di Google, l'ID progetto di Google e una chiave privata.

È possibile aggiungere ed eliminare le connessioni, nonché configurare la pianificazione di polling per ogni segmento cloud.

Aggiunta di connessioni per il polling dei segmenti cloud

Per aggiungere una connessione per il polling dei segmenti cloud all'elenco delle connessioni disponibili:

1. Nella struttura della console selezionare il nodo **Device discovery** → **Cloud**.
2. Nell'area di lavoro della finestra fare clic su **Configura polling**.

   Verrà visualizzata una finestra contenente un elenco delle connessioni disponibili per il polling dei segmenti cloud.
3. Fare clic sul pulsante **Aggiungi**.

   Verrà aperta la finestra **Connessione**.

4. Specificare il nome dell'ambiente cloud per la connessione da utilizzare per il successivo polling del segmento cloud:

Ambiente cloud

L'ambiente in cui si trovano le istanze EC2 o (macchine virtuali) può essere Amazon Web Services (AWS), Microsoft Azure o Google Cloud.

Se è stato selezionato AWS, specificare le seguenti impostazioni:

- **Nome della connessione**

  Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

  Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

  Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

- **Usa ruolo IAM AWS**

  Selezionare questa opzione se è stato già creato un ruolo IAM per l'utilizzo dei servizi AWS da parte di Administration Server.

- **Usa account utente IAM AWS**

  Selezionare questa opzione se si dispone di un account utente IAM con le autorizzazioni richieste ed è possibile immettere un ID chiave e una chiave segreta.

  - **ID chiave di accesso**

    L'ID chiave di accesso IAM è una sequenza di caratteri alfanumerici. L'ID chiave è stato ricevuto al momento della creazione dell'account utente IAM.

    Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

  - **Chiave segreta**

    Chiave segreta ricevuta con l'ID chiave di accesso al momento della creazione dell'account utente IAM.

    I caratteri della chiave segreta sono visualizzati come asterischi. Quando si inizia a immettere la chiave segreta, viene visualizzato il pulsante **Mostra**. Tenere premuto questo pulsante per visualizzare i caratteri immessi.

    Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

La procedura guidata Configura ambiente cloud consente di specificare solo una chiave di accesso AWS IAM. Successivamente è possibile specificare più connessioni per gestire altri segmenti cloud.

Se è stato selezionato Azure, specificare le seguenti impostazioni:

- **Nome della connessione**

  Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

  Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

  Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

- **ID applicazione Azure**

  L'ID applicazione è stato creato dall'utente nel portale di Azure.

  È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

- **ID sottoscrizione Azure**

  La sottoscrizione è stata creata dall'utente nel portale di Azure.

- **Password dell'applicazione Azure**

  La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

  I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

- **Nome dell'account di archiviazione Azure**

  È stato creato il nome dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

- **Chiave di accesso all'archivio Azure**

  È stata ricevuta una password (chiave) durante la creazione dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

  La chiave è disponibile nella sezione "Panoramica dell'account di archiviazione Azure", nella sottosezione "Chiavi".

Se è stato selezionato Google Cloud, specificare le seguenti impostazioni:

- **Nome della connessione**

  Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

  Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

  Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

- **E-mail client**

L'e-mail client è l'indirizzo e-mail utilizzato per la registrazione del progetto in Google Cloud.

- **ID progetto**

  L'ID progetto è l'ID ricevuto durante la registrazione del progetto in Google Cloud.

- **Chiave privata**

  La chiave privata è la sequenza di caratteri ricevuta come chiave privata durante la registrazione del progetto in Google Cloud. È consigliabile copiare e incollare questa sequenza per evitare errori.

5. Se si desidera, selezionare **Imposta pianificazione di polling** e modificare le impostazioni predefinite.

   La connessione viene salvata nelle impostazioni dell'applicazione.

Dopo la prima esecuzione del polling del nuovo segmento cloud, il sottogruppo corrispondente a tale segmento viene visualizzato nel gruppo di amministrazione **Dispositivi gestiti\Cloud**.

Se si specificano credenziali errate, non verranno individuate istanze durante il polling del segmento cloud e non verrà visualizzato un nuovo sottogruppo nel gruppo di amministrazione **Dispositivi gestiti\Cloud**.

Eliminazione di connessioni per il polling dei segmenti cloud

Se non è più necessario eseguire il polling di uno specifico segmento cloud, è possibile eliminare la connessione corrispondente al segmento dall'elenco delle connessioni disponibili. È anche possibile eliminare una connessione se, ad esempio, le autorizzazioni per il polling di un segmento cloud sono state trasferite a un altro utente IAM AWS con una chiave diversa.

Per eliminare una connessione:

1. Nella struttura della console selezionare il nodo **Device discovery** → **Cloud**.
2. Nell'area di lavoro della finestra selezionare **Configura polling**.

   Verrà visualizzata una finestra contenente un elenco delle connessioni disponibili per il polling dei segmenti cloud.
3. Selezionare la connessione che si desidera eliminare e fare clic sul pulsante **Elimina** nella parte destra della finestra.
4. Nella finestra visualizzata fare clic sul pulsante **OK** per confermare la selezione.

Se si eliminano connessioni dall'elenco delle connessioni disponibili, i dispositivi all'interno dei segmenti corrispondenti vengono automaticamente eliminati dai gruppi di amministrazione corrispondenti.

Configurazione della pianificazione di polling

Il polling dei segmenti cloud viene eseguito in base a una pianificazione. È possibile impostare la frequenza di polling.

La frequenza di polling è impostata automaticamente su 5 minuti nelle impostazioni di Configura ambiente cloud. È possibile modificare il valore in qualsiasi momento e impostare una pianificazione diversa. Non è tuttavia consigliabile configurare il polling per l'esecuzione con una frequenza inferiore a 5 minuti perché potrebbero verificarsi errori nel funzionamento dell'API.

Per configurare la pianificazione del polling dei segmenti cloud:

1. Nella struttura della console selezionare il nodo **Device discovery** → **Cloud**.
2. Nell'area di lavoro fare clic su **Configura polling**.

   Verrà visualizzata la finestra delle proprietà del cloud.
3. Nell'elenco selezionare la connessione desiderata e fare clic sul pulsante **Proprietà**.

   Verrà visualizzata la finestra delle proprietà di connessione.
4. Nella finestra delle proprietà fare clic sul collegamento **Imposta pianificazione di polling**.

   Verrà aperta la finestra **Pianificazione**.

5. Definire le seguenti impostazioni:

- **Avvio pianificato**

  Opzioni per la pianificazione di polling:

  - Ogni N giorni

    Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - Ogni N minuti

    Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

    Per impostazione predefinita, il polling viene eseguito ogni 5 minuti, a partire dall'ora di sistema corrente.

  - In base ai giorni della settimana

    Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

    Per impostazione predefinita, il polling viene eseguito ogni venerdì alle 18:00:00.

  - Ogni mese nei giorni specificati delle settimane selezionate

    Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

    Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è 18:00:00.

- Esegui attività non effettuate

  Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

  Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

  Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

  Per impostazione predefinita, questa opzione è abilitata.

6. Fare clic su **OK** per salvare le modifiche.

La pianificazione del polling verrà configurata e salvata.

Installazione di applicazioni nei dispositivi in un ambiente cloud

È possibile installare le seguenti applicazioni Kaspersky nei dispositivi in un ambiente cloud: Kaspersky Security for Windows Server (per i dispositivi Windows) e Kaspersky Endpoint Security for Linux (per i dispositivi Linux).

I dispositivi client in cui si desidera installare la protezione devono soddisfare i requisiti per il funzionamento di Kaspersky Security Center in un ambiente cloud. È necessario disporre di una licenza valida per installare le applicazioni nelle istanze AWS, nelle macchine virtuali di Microsoft Azure o nelle istanze di macchine virtuali Google Cloud.

Kaspersky Security Center 15.1 supporta i seguenti scenari:

- Un dispositivo client viene rilevato tramite un'API; anche l'installazione viene eseguita tramite un'API. Per ambienti cloud AWS e Azure, questo scenario è supportato.
- Un dispositivo client viene rilevato tramite il polling di Active Directory, dei domini Windows o dell'intervallo IP; l'installazione viene eseguita tramite Kaspersky Security Center.
- Un dispositivo client viene rilevato tramite l'API Google; l'installazione viene eseguita tramite Kaspersky Security Center. Per Google Cloud, è supportato solo questo scenario.

Non sono supportati altri metodi per l'installazione delle applicazioni.

Per installare le applicazioni nei dispositivi virtuali, utilizzare i pacchetti di installazione.

Per creare un'attività per l'installazione remota dell'applicazione nelle istanze utilizzando l'API AWS o l'API Azure:

1. Nella struttura della console selezionare la cartella **Attività**.
2. Fare clic sul pulsante **Nuova attività**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Nella pagina **Selezionare il tipo di attività** selezionare **Installa l'applicazione in remoto** come tipo di attività.

4. Nella pagina **Seleziona dispositivi** selezionare i dispositivi desiderati dal gruppo **Dispositivi gestiti\Cloud**.

5. Se Network Agent non è ancora stato installato nei dispositivi in cui si intende installare l'applicazione, nella pagina **Selezione di un account per l'esecuzione dell'attività** selezionare **Account richiesto (Network Agent non utilizzato)** e fare clic sul pulsante **Aggiungi** nella parte destra della finestra. Nel menu visualizzato selezionare uno dei seguenti elementi:

   - **Account cloud**

     Selezionare questa opzione se si desidera installare le applicazioni in istanze AWS e si dispone di una chiave di accesso AWS IAM con le autorizzazioni necessarie, ma non si dispone di un ruolo IAM. Selezionare questa opzione anche se si desidera installare le applicazioni in dispositivi nell'ambiente Azure.

     Nella finestra visualizzata specificare in Kaspersky Security Center le credenziali che concedono i diritti per l'installazione delle applicazioni nei dispositivi.

     Selezionare l'ambiente cloud: AWS o Azure.

     Nel campo **Nome account** immettere un nome per tali credenziali. Questo nome verrà visualizzato nell'elenco degli account per l'esecuzione dell'attività.

     Se è stato selezionato AWS, nei campi **ID chiave di accesso** e **Chiave segreta** immettere le credenziali per l'account utente IAM che dispone dei diritti per l'installazione delle applicazioni nei dispositivi specificati.

     Se è stato selezionato Azure, nei campi **ID sottoscrizione Azure** e **Password dell'applicazione Azure** immettere le credenziali per l'account Azure che dispone dei diritti per l'installazione delle applicazioni nei dispositivi specificati.

     Se si specificano credenziali errate, l'attività di installazione remota verrà terminata con un errore nei dispositivi per cui è pianificata.

   - **Account**

     Per le istanze che eseguono Windows, selezionare questa opzione se non si desidera installare l'applicazione tramite gli strumenti dell'API AWS o Azure. In questo caso, verificare che i dispositivi nel segmento cloud soddisfino le condizioni richieste. Kaspersky Security Center installa le applicazioni autonomamente, senza utilizzare l'API AWS o l'API Azure.

     Se si specificano dati errati, l'attività di installazione remota verrà terminata con un errore nei dispositivi per cui è pianificata.

   - **Ruolo IAM**

     Selezionare questa opzione se si desidera installare le applicazioni in istanze nell'ambiente AWS e si dispone di un ruolo IAM con i diritti richiesti.

     Se si seleziona questa opzione ma non si dispone di un ruolo IAM con i diritti richiesti, l'attività di installazione remota verrà terminata con un errore nei dispositivi per cui è pianificata.

   - **Certificato SSH**

Per le istanze che eseguono Linux, selezionare questa opzione se non si desidera installare l'applicazione tramite gli strumenti dell'API AWS o dell'API Azure. In questo caso, verificare che i dispositivi nel segmento cloud soddisfino le condizioni richieste. Kaspersky Security Center installa le applicazioni autonomamente, senza utilizzare l'API AWS o l'API Azure.

Per specificare la chiave privata del certificato SSH, è possibile generarla utilizzando l'utilità ssh-keygen. Si noti che Kaspersky Security Center supporta il formato PEM delle chiavi private, ma l'utilità ssh-keygen genera chiavi SSH nel formato OPENSSH per impostazione predefinita. Il formato OPENSSH non è supportato da Kaspersky Security Center. Per creare una chiave privata nel formato PEM supportato, aggiungere l'opzione `-m PEM` nel comando ssh-keygen. Ad esempio:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail dell'utente>"
```

È possibile specificare più credenziali facendo clic sul pulsante **Aggiungi** per ogni nuova chiave. Se diversi segmenti cloud richiedono credenziali differenti, specificare le credenziali per tutti i segmenti.

Al termine della procedura guidata, l'attività di installazione remota dell'applicazione viene visualizzata nell'elenco delle attività nell'area di lavoro della cartella **Attività**.

In Microsoft Azure l'installazione remota delle applicazioni di protezione in una macchina virtuale può dare origine all'eliminazione dell'estensione per lo script personalizzata installata nella macchina virtuale.

Visualizzazione delle proprietà dei dispositivi cloud

Per visualizzare le proprietà di un dispositivo cloud:

1. Nella struttura della console, nel nodo **Device discovery** → **Cloud**, selezionare il sottonodo che corrisponde al gruppo in cui si trova l'istanza desiderata.

   Se non si è conoscenza del gruppo in cui si trova il dispositivo virtuale desiderato, utilizzare la funzione di ricerca:

   a. Fare clic con il pulsante destro del mouse sul nome del nodo **Dispositivi gestiti** → **Cloud**, quindi selezionare **Cerca** nel menu di scelta rapida.

   b. Nella finestra visualizzata eseguire una ricerca.

      Se un dispositivo soddisfa i criteri impostati dall'utente, il nome e i dettagli verranno visualizzati nella parte inferiore della finestra.

2. Fare clic con il pulsante destro del mouse sul nome del nodo desiderato. Nel menu di scelta rapida selezionare **Proprietà**.

   Nella finestra visualizzata vengono mostrate le proprietà dell'oggetto.

   La sezione **Informazioni sul sistema** → Informazioni generali di sistema contiene le proprietà specifiche per i dispositivi nell'ambiente cloud:

   - **Dispositivo rilevato tramite API** (**AWS**, **Azure** o **Google Cloud**; se il dispositivo non può essere rilevato utilizzando gli strumenti API, viene visualizzato il valore **No**).
   - **Regione cloud**.
   - **VPC cloud** (solo per dispositivi AWS e Google Cloud).
   - **Zona di disponibilità cloud** (solo per dispositivi AWS e Google Cloud).
   - **Sottorete cloud**.
   - **Gruppo di collocazione Cloud** (questa unità viene visualizzata solo se l'istanza appartiene a un gruppo di collocazione; in caso contrario, non viene visualizzata).

È possibile fare clic sul pulsante **Esporta in un file** per esportare queste informazioni in un file .csv o .txt.

Sincronizzazione con il cloud

Durante l'esecuzione di Configura ambiente cloud, viene automaticamente creata la regola Sincronizza con il cloud. La regola consente di spostare automaticamente le istanze rilevate in ogni polling dal gruppo **Dispositivi non assegnati** al gruppo **Dispositivi gestiti\Cloud** per rendere disponibili le istanze per la gestione centralizzata. Per impostazione predefinita, la regola è attiva dopo la creazione. È possibile disabilitare, modificare o applicare la regola in qualsiasi momento.

Per modificare le proprietà della regola Sincronizza con il cloud e/o applicare la regola:

1. Nella struttura della console fare clic con il pulsante destro del mouse sul nodo **Device discovery**.
2. Nel menu di scelta rapida selezionare **Proprietà**.
3. Nella finestra **Proprietà** visualizzata, nel riquadro **Sezioni**, selezionare **Sposta dispositivi**.
4. Nell'elenco delle regole di spostamento dei dispositivi nell'area di lavoro selezionare la regola **Sincronizza con il cloud**, quindi fare clic sul pulsante **Proprietà** nella parte inferiore della finestra.

   Verrà visualizzata la finestra delle proprietà della regola.

5. Se necessario, specificare le seguenti impostazioni nel gruppo di impostazioni **Segmenti cloud**:

- Il dispositivo si trova in un segmento cloud

  La regola viene applicata solo ai dispositivi inclusi nel segmento cloud selezionato. In caso contrario, la regola viene applicata a tutti i dispositivi individuati.

  Per impostazione predefinita, questa opzione è selezionata.

  - Includi gli oggetti figlio

    La regola viene applicata a tutti i dispositivi nel segmento selezionato e in tutte le sottosezioni cloud nidificate. In caso contrario, la regola viene applicata solo ai dispositivi inclusi nel segmento radice.

    Per impostazione predefinita, questa opzione è selezionata.

  - Sposta i dispositivi dagli oggetti nidificati nei sottogruppi corrispondenti

    Se questa opzione è abilitata, i dispositivi vengono spostati automaticamente dagli oggetti nidificati ai sottogruppi corrispondenti alla relativa struttura.

    Se questa opzione è disabilitata, i dispositivi vengono spostati automaticamente dagli oggetti nidificati alla radice del sottogruppo Cloud senza ulteriori ramificazioni.

    Per impostazione predefinita, questa opzione è abilitata.

    - Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati

      Se questa opzione è abilitata, quando la struttura del gruppo **Dispositivi gestiti\Cloud** non ha sottogruppi corrispondenti alla sezione che contiene il dispositivo, Kaspersky Security Center crea tali sottogruppi. Ad esempio, se viene rilevata una nuova subnet durante la device discovery, verrà creato un nuovo gruppo con lo stesso nome nel gruppo **Dispositivi gestiti\Cloud**.

      Se questa opzione è disabilitata, Kaspersky Security Center non crea nuovi sottogruppi. Ad esempio, se viene rilevata una nuova subnet durante il polling della rete, non verrà creato un nuovo gruppo con lo stesso nome nel gruppo **Dispositivi gestiti\Cloud** e i dispositivi presenti nella subnet verranno spostati nel gruppo **Dispositivi gestiti\Cloud**.

      Per impostazione predefinita, questa opzione è abilitata.

    - Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud

      Se questa opzione è abilitata, l'applicazione elimina dal gruppo Cloud tutti i sottogruppi a cui non corrisponde alcun oggetto cloud esistente.

      Se questa opzione è disabilitata, vengono mantenuti i sottogruppi a cui non corrisponde alcun oggetto cloud esistente.

      Per impostazione predefinita, questa opzione è abilitata.

  Se è stata abilitata l'opzione **Sincronizza con il cloud** durante l'esecuzione di Configura ambiente cloud, la regola Sincronizza con il cloud viene creata con le caselle di controllo **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati** ed **Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud** selezionate.

Se non è stata abilitata l'opzione **Sincronizza con il cloud**, la regola Sincronizza con il cloud viene creata con queste opzioni disabilitate (deselezionate). Se l'utilizzo di Kaspersky Security Center richiede che la struttura dei sottogruppi nel sottogruppo di **Dispositivi gestiti\Cloud** corrisponda alla struttura dei segmenti cloud, selezionare le caselle di controllo **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati** ed **Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud** nelle proprietà della regola e quindi applicare la regola.

6. Nell'elenco a discesa **Dispositivo rilevato tramite API** selezionare uno dei seguenti valori:
   - **AWS**. Il dispositivo viene rilevato tramite l'API AWS, quindi si trova senz'altro nell'ambiente cloud AWS.
   - **Azure**. Il dispositivo viene rilevato tramite l'API Azure, quindi si trova senz'altro nell'ambiente cloud Azure.
   - **Google Cloud.** Il dispositivo viene rilevato tramite l'API Google, quindi si trova senz'altro nell'ambiente cloud Google.
   - **No**. Il dispositivo non può essere rilevato tramite l'API AWS, Azure o Google, ad esempio perché si trova all'esterno dell'ambiente cloud oppure si trova nell'ambiente cloud ma non può essere rilevato tramite un'API.
7. **Nessun valore**. Questa condizione non viene applicata. Se necessario, configurare le proprietà delle altre regole nelle altre sezioni.
8. Se necessario, applicare la regola facendo clic sul pulsante **Forza** nella parte inferiore della finestra.

   Verrà avviata l'Aggiunta guidata regola di esecuzione. Seguire le istruzioni della procedura guidata. Al termine della procedura guidata, la regola verrà eseguita e la struttura dei sottogruppi nel sottogruppo **Dispositivi gestiti\Cloud** corrisponderà alla struttura dei segmenti cloud.
9. Fare clic sul pulsante **OK**.

Le proprietà verranno impostate e salvate.

Per disabilitare la regola Sincronizza con il cloud:

1. Nella struttura della console fare clic con il pulsante destro del mouse sul nodo **Device discovery**.
2. Nel menu di scelta rapida selezionare **Proprietà**.
3. Nella finestra **Proprietà** visualizzata, nel riquadro **Sezioni**, selezionare **Sposta dispositivi**.
4. Nell'elenco delle regole di spostamento dei dispositivi nell'area di lavoro disabilitare (deselezionare) l'opzione **Sincronizza con il cloud**, quindi fare clic su **OK**.

La regola verrà disabilitata e non sarà più applicata.

Distribuzione di Kaspersky Security Center in Yandex.Cloud

È possibile distribuire Kaspersky Security Center in Yandex.Cloud. È disponibile solo la modalità a consumo; i database cloud non sono supportati.

In Yandex.Cloud sono disponibili i seguenti metodi di distribuzione per le applicazioni di protezione:

- Mediante i metodi offerti da Kaspersky Security Center, ovvero tramite l'attività *Installazione remota* (la distribuzione dei programmi di protezione è possibile solo se Administration Server e le macchine virtuali da proteggere si trovano sullo stesso segmento di rete)
- Tramite script di distribuzione

Per la distribuzione di Kaspersky Security Center in Yandex.Cloud, è necessario disporre di un account di servizio in Yandex.Cloud. È necessario fornire a questo account l'autorizzazione marketplace.meteringAgent e associare l'account alla macchina virtuale (fare riferimento a https://cloud.yandex.com/en per informazioni dettagliate).

Appendici

Questa sezione fornisce informazioni di riferimento e dati aggiuntivi per l'utilizzo di Kaspersky Security Center.

Funzioni avanzate

In questa sezione vengono descritte numerose opzioni avanzate di Kaspersky Security Center, che consentono di espandere le funzionalità di gestione centralizzata delle applicazioni nei dispositivi.

Automazione delle operazioni di Kaspersky Security Center. utilità klakaut

È possibile automatizzare le operazioni di Kaspersky Security Center tramite l'utilità klakaut. L'utilità klakaut e la relativa Guida sono disponibili nella cartella di installazione di Kaspersky Security Center.

Strumenti personalizzati

Kaspersky Security Center consente di creare un elenco di *strumenti personalizzati* (di seguito denominati anche semplicemente *strumenti*), ovvero applicazioni attivate per un dispositivo client in Administration Console utilizzando il gruppo **Strumenti personalizzati** del menu di scelta rapida. Ogni strumento dell'elenco sarà associato a un comando di menu, che verrà utilizzato da Administration Console per avviare l'applicazione corrispondente a tale strumento.

Le applicazioni vengono avviate nella workstation dell'amministratore. L'applicazione può accettare gli attributi di un dispositivo client remoto come argomenti della riga di comando (nome NetBIOS, nome DNS o indirizzo IP). La connessione al dispositivo remoto può essere stabilita tramite tunneling.

Per impostazione predefinita, l'elenco degli strumenti personalizzati contiene i seguenti programmi di servizio per ogni dispositivo client:

- **Diagnostica remota** è un'utilità per la diagnostica remota di Kaspersky Security Center.
- **Desktop remoto** è un componente standard di Microsoft Windows denominato Connessione Desktop remoto.
- **Gestione computer** è un componente standard di Microsoft Windows.

Per aggiungere o rimuovere strumenti personalizzati o modificare le relative impostazioni:

Nel menu di scelta rapida del dispositivo client selezionare **Strumenti personalizzati** → **Configura strumenti personalizzati**.

Viene aperta la finestra **Strumenti personalizzati**. In questa finestra è possibile aggiungere strumenti personalizzati o modificarne le impostazioni utilizzando i pulsanti **Aggiungi** e **Modifica**. Per rimuovere uno strumento personalizzato, fare clic sul pulsante Rimuovi con l'icona della croce rossa ( ).

Modalità di clonazione del disco di Network Agent

La clonazione del disco rigido di un dispositivo di riferimento è un popolare metodo di installazione del software nei nuovi dispositivi. Se Network Agent viene eseguito in modalità standard nel disco rigido del dispositivo di riferimento, si verifica il seguente problema:

Dopo la distribuzione dell'immagine del disco di riferimento con Network Agent nei nuovi dispositivi, questi vengono visualizzati in Administration Console con una singola icona. Questo problema si verifica perché la procedura di clonazione comporta il mantenimento nei nuovi dispositivi di dati interni identici, utilizzati da Administration Server per associare un dispositivo a un'icona in Administration Console.

Una specifica *modalità di clonazione del disco di Network Agent* consente di evitare i problemi associati a una visualizzazione errata dei nuovi dispositivi in Administration Console dopo la clonazione. Utilizzare questa modalità durante la distribuzione del software (con Network Agent) nei nuovi dispositivi tramite la clonazione del disco.

Nella modalità di clonazione del disco, Network Agent continua a funzionare, ma non si connette ad Administration Server. Quando si esce dalla modalità di clonazione, Network Agent elimina i dati interni, in base ai quali Administration Server associa più dispositivi a una singola icona in Administration Console. Al termine della clonazione dell'immagine del dispositivo di riferimento, i nuovi dispositivi sono visualizzati correttamente in Administration Console (con singole icone).

Scenario di utilizzo della modalità di clonazione del disco di Network Agent

1. L'amministratore installa Network Agent in un dispositivo di riferimento.
2. L'amministratore verifica la connessione di Network Agent ad Administration Server utilizzando l'utilità klnagchk.
3. L'amministratore abilita la modalità di clonazione del disco di Network Agent.
4. L'amministratore installa il software e le patch nel dispositivo e lo riavvia tutte le volte che risulta necessario.
5. L'amministratore clona il disco rigido del dispositivo di riferimento in qualsiasi numero di dispositivi.
6. Ogni copia clonata deve soddisfare le seguenti condizioni:
    a. Il nome del dispositivo deve essere modificato.
    b. Il dispositivo deve essere riavviato.
    c. La modalità di clonazione del disco deve essere disabilitata.

Abilitazione e disabilitazione della modalità di clonazione del disco utilizzando l'utilità klmover

Per abilitare o disabilitare la modalità di clonazione del disco di Network Agent:

1. Eseguire l'utilità klmover nel dispositivo in cui è installato Network Agent da clonare.

   L'utilità klmover si trova nella cartella di installazione di Network Agent.

2. Per abilitare la modalità di clonazione del disco, immettere il seguente comando nel prompt dei comandi di Windows:

   ```
   klmover -cloningmode 1
   ```

   Network Agent passa alla modalità di clonazione del disco.

3. Per richiedere lo stato corrente della modalità di clonazione del disco, immettere il seguente comando nel prompt dei comandi:

   ```
   klmover -cloningmode
   ```

   La finestra dell'utilità indicherà se la modalità di clonazione del disco è abilitata o disabilitata.

4. Per disabilitare la modalità di clonazione del disco, immettere il seguente comando nella riga di comando dell'utilità:

   ```
   klmover -cloningmode 0
   ```

Preparazione di un dispositivo di riferimento in cui è installato Network Agent per la creazione di un'immagine del sistema operativo

È consigliabile creare un'immagine del sistema operativo di un dispositivo di riferimento in cui è installato Network Agent e distribuire l'immagine nei dispositivi della rete. In questo caso, si crea un'immagine del sistema operativo di un dispositivo di riferimento in cui Network Agent non è ancora stato avviato. Se si avvia Network Agent in un dispositivo di riferimento prima della creazione di un'immagine del sistema operativo, l'identificazione di Administration Server dei dispositivi distribuiti da un'immagine del sistema operativo del dispositivo di riferimento presenterà diversi problemi.

Per preparare il dispositivo di riferimento per la creazione di un'immagine del sistema operativo:

1. Assicurarsi che il sistema operativo Windows sia installato nel dispositivo di riferimento e installare l'altro software desiderato in tale dispositivo.

2. Nel dispositivo di riferimento, nelle impostazioni delle connessioni di rete Windows disconnettere il dispositivo di riferimento dalla rete in cui è installato Kaspersky Security Center.

3. Nel dispositivo di riferimento avviare l'installazione locale di Network Agent utilizzando il file setup.exe.

   Viene avviata l'Installazione guidata di Kaspersky Security Center Network Agent. Seguire le istruzioni della procedura guidata.

4. Nella pagina **Administration Server** della procedura guidata, specificare l'indirizzo IP dell'Administration Server.

   Se non si conosce l'indirizzo esatto di Administration Server, immettere localhost. È possibile modificare l'indirizzo IP in un secondo momento utilizzando l'utilità klmover con la chiave `-address`.

5. Nella pagina **Avvia applicazione** della procedura guidata disabilitare l'opzione **Avvia l'applicazione durante l'installazione**.

6. Al termine dell'installazione di Network Agent, non riavviare il dispositivo prima di creare un'immagine del sistema operativo.

   Se si riavvia il dispositivo, sarà necessario ripetere l'intero processo di preparazione di un dispositivo di riferimento per la creazione di un'immagine del sistema operativo.

7. Nel dispositivo di riferimento, nella riga di comando avviare l'utilità sysprep ed eseguire il seguente comando: `sysprep.exe /generalize /oobe /shutdown`.

Il dispositivo di riferimento è pronto per la creazione di un'immagine del sistema operativo.

Configurazione della ricezione dei messaggi da File Integrity Monitor

Le applicazioni gestite, ad esempio Kaspersky Security for Windows Server o Kaspersky Security for Virtualization Light Agent, inviano messaggi da File Integrity Monitor a Kaspersky Security Center. Kaspersky Security Center consente anche di monitorare qualsiasi variazione dei componenti critici dei sistemi (ad esempio server Web e sportelli bancomat) e rispondere tempestivamente alle violazioni dell'integrità di tali sistemi. A tale scopo, è possibile ricevere messaggi dal componente File Integrity Monitor. Il componente File Integrity Monitor consente di monitorare non solo il file system di un dispositivo, ma anche gli hive del registro, lo stato del firewall e lo stato dell'hardware connesso.

È necessario configurare Kaspersky Security Center per la ricezione dei messaggi dal componente File Integrity Monitor senza utilizzare Kaspersky Security for Windows Server o Kaspersky Security for Virtualization Light Agent.

Per configurare la ricezione dei messaggi da File Integrity Monitor:

1. Aprire il Registro di sistema del dispositivo in cui è installato Administration Server (ad esempio, in locale, utilizzando il comando regedit dal menu **Start** → **Esegui**).

2. Passare al seguente hive:

   - Per i sistemi a 32 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - Per i sistemi a 64 bit:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Creare le chiavi:

   - Creare la chiave KLSRV_EVP_FIM_PERIOD_SEC per specificare il periodo di tempo per il conteggio del numero di eventi elaborati. Specificare le seguenti impostazioni:

     a. Specificare KLSRV_EVP_FIM_PERIOD_SEC come nome della chiave.

     b. Specificare DWORD come tipo di chiave.

     c. Specificare un intervallo di valori per il periodo di tempo da 43 200 a 172 800 secondi. Per impostazione predefinita, l'intervallo di tempo è di 86 400 secondi.

   - Creare la chiave KLSRV_EVP_FIM_LIMIT per limitare il numero di eventi ricevuti per l'intervallo di tempo specificato. Specificare le seguenti impostazioni:

     a. Specificare KLSRV_EVP_FIM_LIMIT come nome della chiave.

     b. Specificare DWORD come tipo di chiave.

     c. Specificare un intervallo di valori per gli eventi ricevuti da 2.000 a 50.000. Il numero predefinito di eventi è 20.000.

   - Creare la chiave KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC per il conteggio degli eventi con una precisione fino a uno specifico intervallo di tempo. Specificare le seguenti impostazioni:

     a. Specificare KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC come nome della chiave.

     b. Specificare DWORD come tipo di chiave.

     c. Specificare un intervallo di valori da 120 a 600 secondi. L'intervallo di tempo predefinito è 300 secondi.

   - Creare la chiave KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC in modo che, al termine del periodo di tempo specificato, l'applicazione possa verificare se il numero di eventi elaborati nell'intervallo di tempo risulta inferiore il limite specificato. Questa verifica viene eseguita al raggiungimento del limite per la ricezione degli eventi. Se questa condizione risulta soddisfatta, l'applicazione riprende il salvataggio degli eventi nel database. Specificare le seguenti impostazioni:

     a. Specificare KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC come nome della chiave.

     b. Specificare DWORD come tipo di chiave.

     c. Specificare un intervallo di valori da 600 a 3600 secondi. L'intervallo di tempo predefinito è 1800 secondi.

   Se le chiavi non vengono create, vengono utilizzati i valori predefiniti.

4. Riavviare il servizio Administration Server.

Verranno configurati i limiti per la ricezione degli eventi dal componente File Integrity Monitor. È possibile visualizzare i risultati del componente File Integrity Monitor nei rapporti denominati **Le 10 regole di Monitoraggio integrità file/Monitoraggio integrità di sistema che sono state attivate più frequentemente nei dispositivi** e **I 10 dispositivi in cui sono state attivate più frequentemente le regole di Monitoraggio integrità file/Monitoraggio integrità di sistema**.

Manutenzione di Administration Server

La manutenzione di Administration Server consente di liberare spazio nella cartella di Administration Server e ridurre il volume del database eliminando gli oggetti non più necessari. Ciò consente di migliorare le prestazioni e l'affidabilità operativa dell'applicazione. Si consiglia di eseguire la manutenzione di Administration Server almeno una volta alla settimana.

La manutenzione di Administration Server viene eseguita tramite un'attività specializzata. Durante la manutenzione di Administration Server, l'applicazione esegue le azioni seguenti:

- Elimina le cartelle e i file non necessari dalla cartella di archiviazione.
- Elimina i record non necessari dalle tabelle (noti anche come "puntatori pendenti").
- Cancella la cache.
- Esegue la manutenzione del database (se si utilizza SQL Server o PostgreSQL come DBMS):
  - Verifica la presenza di errori nel database (disponibile solo per SQL Server).
  - Riorganizza gli indici del database.
  - Aggiorna le statistiche del database.
  - Riduce le dimensioni del database (se necessario).

Per creare l'attività di Manutenzione di Administration Server:

1. Nella struttura della console selezionare il nodo di Administration Server per cui si desidera creare l'attività di *Manutenzione di Administration Server*.
2. Selezionare la cartella **Attività**.
3. Nell'area di lavoro della cartella **Attività** fare clic sul pulsante **Nuova attività**.

   Verrà avviata la Creazione guidata nuova attività.
4. Nella finestra **Selezionare il tipo di attività** della procedura guidata selezionare **Manutenzione di Administration Server** come tipo di attività, quindi fare clic su **Avanti**.
5. Se è necessario ridurre le dimensioni del database di Administration Server durante la manutenzione, nella finestra **Impostazioni** della procedura guidata selezionare la casella di controllo **Comprimi database**.
6. Seguire le rimanenti istruzioni della procedura guidata.

L'attività creata viene visualizzata nell'elenco di attività nell'area di lavoro della cartella **Attività**. Una sola attività di *Manutenzione di Administration Server* può essere in esecuzione per un singolo Administration Server. Se è stata già creata l'attività di *Manutenzione di Administration Server* per un Administration Server, non può essere creata alcuna nuova attività di *Manutenzione di Administration Server*.

Accesso ai server DNS pubblici

Se non è possibile accedere ai server Kaspersky utilizzando il DNS di sistema, Kaspersky Security Center può utilizzare i seguenti server DNS pubblici, nel seguente ordine:

1. Google Public DNS (8.8.8.8)
2. Cloudflare DNS (1.1.1.1)
3. Alibaba Cloud DNS (223.6.6.6)
4. Quad9 DNS (9.9.9.9)
5. CleanBrowsing (185.228.168.168)

Le richieste a questi server DNS possono contenere indirizzi di dominio e l'indirizzo IP pubblico di Administration Server, poiché l'applicazione stabilisce una connessione TCP/UDP al server DNS. Se Kaspersky Security Center utilizza un server DNS pubblico, il trattamento dei dati è disciplinato dall'informativa sulla privacy del servizio pertinente.

Per configurare l'uso del DNS pubblico tramite l'utilità klscflag:

1. Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.
2. Per disabilitare l'uso del DNS pubblico, eseguire il seguente comando:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Per abilitare l'uso del DNS pubblico, eseguire il seguente comando:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Finestra Metodo di notifica all'utente

Nella finestra **Metodo di notifica all'utente** è possibile configurare la notifica utente in merito all'installazione del certificato nel dispositivo mobile:

- **Mostra codice QR nella procedura guidata**. Se si seleziona questa opzione, verrà visualizzato un collegamento al pacchetto di installazione nel passaggio finale della Connessione guidata nuovo dispositivo.
- **Invia codice QR all'utente**. Se si seleziona questa opzione, è possibile specificare le impostazioni per l'invio di una notifica all'utente sulla connessione di un dispositivo.

Nel gruppo di impostazioni **Tramite e-mail** è possibile configurare la notifica all'utente dell'installazione di un nuovo certificato nel dispositivo mobile tramite messaggi e-mail. Questo metodo di notifica è disponibile solo se l'opzione Server SMTP è abilitata.

Nel gruppo di impostazioni **Tramite SMS** è possibile configurare la notifica all'utente dell'installazione di un certificato nel dispositivo mobile tramite SMS. Questo metodo di notifica è disponibile solo se l'opzione Notifica tramite SMS è abilitata.

Fare clic sul collegamento **Modifica messaggio** nei gruppi di impostazioni **Tramite e-mail** e **Tramite SMS** per visualizzare e modificare il messaggio di notifica, se necessario.

Finestra Selezione dispositivi

Scegliere una selezione dall'elenco **Selezione dispositivi**. L'elenco contiene le selezioni predefinite e le selezioni create dall'utente.

È possibile visualizzare i dettagli delle selezioni dispositivi nell'area di lavoro della sezione **Selezioni dispositivi**.

Finestra Definire il nome del nuovo oggetto

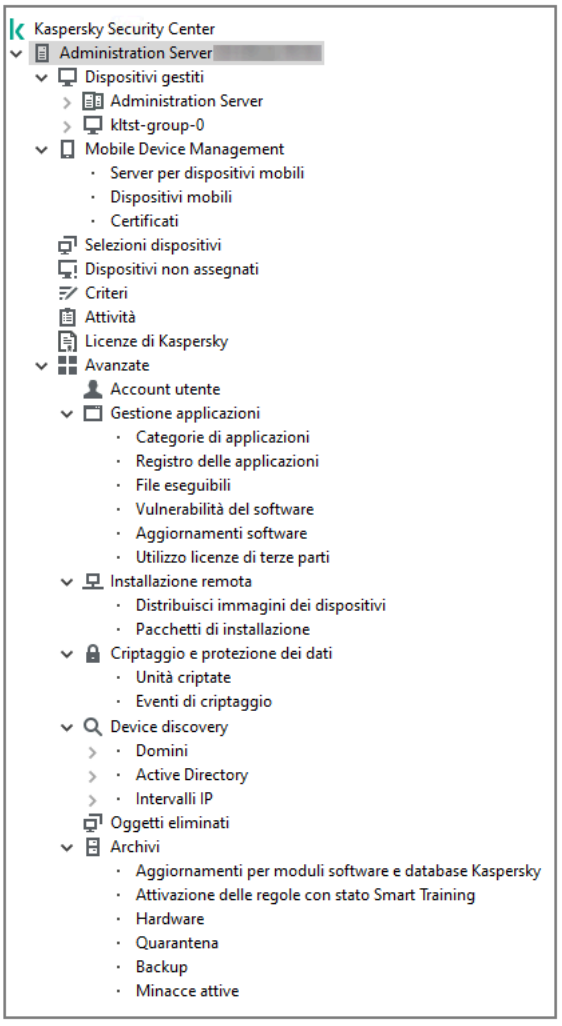
Nella finestra specificare il nome del nuovo oggetto creato. Il nome non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

Funzionalità per l'utilizzo dell'interfaccia di gestione

In questa sezione vengono descritte le azioni che è possibile eseguire nella finestra principale di Kaspersky Security Center.

Struttura della console

La struttura della console (vedere la figura seguente) è progettata per visualizzare la gerarchia degli Administration Server nella rete aziendale, la struttura dei relativi gruppi di amministrazione e altri oggetti dell'applicazione come le cartelle **Archivi** o **Gestione applicazioni**. Lo spazio dei nomi di Kaspersky Security Center può contenere numerosi nodi, tra cui i nomi dei server corrispondenti agli Administration Server installati inclusi nella gerarchia.



Struttura della console

Nodo Administration Server

Il nodo **Administration Server – <Nome dispositivo>** è un contenitore che mostra la struttura organizzativa dell'Administration Server selezionato.

L'area di lavoro del nodo **Administration Server** contiene informazioni riepilogative sullo stato corrente dell'applicazione e dei dispositivi gestiti tramite Administration Server. Le informazioni nell'area di lavoro sono distribuite in varie schede:

- **Monitoraggio**. Visualizza informazioni sul funzionamento dell'applicazione e sullo stato corrente dei dispositivi client in tempo reale. I messaggi importanti per l'amministratore (ad esempio, i messaggi su vulnerabilità, errori o virus rilevati) sono evidenziati in un colore specifico. È possibile utilizzare i collegamenti nella scheda **Monitoraggio** per eseguire le attività di amministrazione standard (ad esempio, installare e configurare l'applicazione di protezione nei dispositivi client) e accedere ad altre cartelle della struttura della console.

- **Statistiche**. Contiene un set di grafici raggruppati per argomenti (stato della protezione, statistiche di Anti-virus, aggiornamenti e così via). Questi grafici visualizzano informazioni aggiornate sull'esecuzione dell'applicazione e sullo stato dei dispositivi client.

- **Rapporti**. Contiene modelli per i rapporti generati dall'applicazione. In questa scheda è possibile creare rapporti utilizzando modelli preimpostati, nonché creare modelli di rapporto personalizzati.

- Finestra **Eventi**. Contiene record sugli eventi che sono stati registrati durante il funzionamento dell'applicazione. Tali record sono distribuiti fra gli argomenti per agevolare la lettura e il filtro. In questa scheda è possibile visualizzare selezioni eventi generate automaticamente e creare selezioni personalizzate.

Cartelle nel nodo Administration Server

Il nodo **Administration Server - <Nome dispositivo>** include le seguenti cartelle:

- **Dispositivi gestiti**. La cartella viene utilizzata per memorizzare, visualizzare, configurare e modificare la struttura di gruppi di amministrazione, criteri di gruppo e attività di gruppo.

- **Mobile Device Management**. Questa cartella è destinata alla gestione dei dispositivi mobili. La cartella **Mobile Device Management** contiene le seguenti sottocartelle:

  - **Server per dispositivi mobili**. Destinato alla gestione degli iOS MDM Server.

  - **Dispositivi mobili**. Destinata alla gestione di dispositivi mobili, KES e MDM iOS.

  - **Certificati**. Destinata alla gestione dei certificati dei dispositivi mobili.

- **Selezioni dispositivi**. Questa cartella è destinata alla selezione rapida dei dispositivi che soddisfano i criteri specificati (una selezione dispositivi) fra tutti i dispositivi gestiti. Ad esempio, è possibile selezionare in modo rapido i dispositivi in cui non è installata alcuna applicazione di protezione e passare a questi dispositivi (vedere l'elenco). È possibile eseguire specifiche azioni su questi dispositivi selezionati, ad esempio assegnare attività. È possibile utilizzare selezioni preimpostate o creare selezioni personalizzate.

- **Dispositivi non assegnati**. Questa cartella contiene un elenco di dispositivi che non sono stati inclusi in nessun gruppo di amministrazione. È possibile eseguire alcune azioni sui dispositivi non assegnati, ad esempio spostarli nei gruppi di amministrazione o installarvi applicazioni.

- **Criteri**. Questa cartella è destinata alla visualizzazione e alla creazione dei criteri.

- **Attività**. Questa cartella è destinata alla visualizzazione e alla creazione delle attività.

- **Licenze di Kaspersky**. Contiene un elenco delle chiavi di licenza disponibili per le applicazioni Kaspersky. Nell'area di lavoro di questa cartella è possibile aggiungere nuove chiavi di licenza per l'archivio delle chiavi di licenza, distribuire chiavi di licenza nei dispositivi gestiti e visualizzare il rapporto sull'utilizzo delle chiavi di licenza.

- **Avanzate**. Questa cartella contiene un set di sottocartelle che corrispondono a vari gruppi di funzionalità dell'applicazione.

Cartella Avanzate. Spostamento delle cartelle nella struttura della console

La cartella **Avanzate** include le seguenti sottocartelle:

- **Account utente**. Contiene un elenco degli account utente di rete.

- **Gestione applicazioni**. Consente di gestire le applicazioni installate nei dispositivi della rete. La cartella **Gestione applicazioni** contiene le seguenti sottocartelle:

  - **Categorie di applicazioni**. Consente di gestire categorie di applicazioni personalizzate.

  - **Registro delle applicazioni**. Contiene un elenco delle applicazioni nei dispositivi in cui è installato Network Agent.

  - **File eseguibili**. Contiene un elenco di file eseguibili archiviati nei dispositivi client in cui è installato Network Agent.

  - **Vulnerabilità del software**. Contiene un elenco delle vulnerabilità delle applicazioni nei dispositivi in cui è installato Network Agent.

  - **Aggiornamenti software**. Contiene un elenco di aggiornamenti delle applicazioni ricevuti da Administration Server che possono essere distribuiti nei dispositivi.

  - **Utilizzo licenze di terze parti**. Contiene un elenco di gruppi di applicazioni concesse in licenza. È possibile utilizzare gruppi di applicazioni concesse in licenza per monitorare l'utilizzo di licenze per software di terzi (applicazioni non Kaspersky) e le possibili violazioni delle limitazioni di licenza.

- **Installazione remota**. La cartella consente di gestire l'installazione remota di sistemi operativi e applicazioni. La cartella **Installazione remota** contiene le seguenti sottocartelle:

  - **Distribuisci immagini dei dispositivi** Consente di distribuire le immagini dei sistemi operativi nei dispositivi.

  - **Pacchetti di installazione**. Contiene un elenco di pacchetti di installazione utilizzabili per l'installazione remota delle applicazioni nei dispositivi.

- **Criptaggio e protezione dei dati**. Questa cartella consente di gestire il processo di criptaggio dei dati nei dischi rigidi e nelle unità rimovibili.

- **Polling della rete**. Questa cartella visualizza la rete in cui è installato Administration Server. Administration Server riceve informazioni sulla struttura della rete e dei relativi dispositivi attraverso il polling periodico della rete Windows, delle subnet IP e di Active Directory® nella rete aziendale. I risultati del polling vengono visualizzati nelle aree di lavoro delle cartelle corrispondenti: **Domini**, **Intervalli IP** e **Active Directory**.

- **Archivi**. La cartella consente di eseguire operazioni con gli oggetti utilizzati per monitorare lo stato dei dispositivi ed effettuarne la manutenzione. La cartella **Archivi** contiene i seguenti sottocartelle:

  - **Rilevamento adattativo delle anomalie**. Contiene un elenco dei rilevamenti eseguiti dalle regole di Kaspersky Endpoint Security funzionanti in modalità SMART Training nei dispositivi client.

  - **Patch e aggiornamenti software Kaspersky**. Contiene un elenco di aggiornamenti ricevuti da Administration Server che possono essere distribuiti ai dispositivi.

  - **Hardware**. Contiene un elenco dell'hardware connesso alla rete dell'organizzazione.

  - **Quarantena**. Contiene un elenco di oggetti spostati in Quarantena dalle applicazioni anti-virus nei dispositivi.

  - **Backup**. Contiene un elenco delle copie di backup dei file che sono stati eliminati o modificati durante la disinfezione nei dispositivi.

  - **File non elaborati**. Contiene un elenco dei file assegnati dalle applicazioni anti-virus per la scansione in un secondo momento.

È possibile modificare il set di sottocartelle incluse nella cartella **Avanzate**. Le sottocartelle utilizzate di frequente possono essere spostate di un livello più in alto dalla cartella **Avanzate**. Le sottocartelle utilizzate raramente possono essere spostate nella cartella **Avanzate**.

*Per spostare una sottocartella all'esterno della cartella **Avanzate**:*

1. Nella struttura della console selezionare la sottocartella che si desidera spostare all'esterno della cartella **Avanzate**.

2. Nel menu di scelta rapida della sottocartella selezionare **Visualizza → Sposta dalla cartella Avanzate**.

> È inoltre possibile spostare una sottocartella all'esterno della cartella **Avanzate** nell'area di lavoro della cartella **Avanzate** facendo clic sul collegamento **Sposta dalla cartella Avanzate** nella sezione con il nome della sottocartella.

*Per spostare una sottocartella nella cartella **Avanzate**:*

1. Nella struttura della console selezionare la sottocartella da spostare nella cartella **Avanzate**.

2. Nel menu di scelta rapida della sottocartella selezionare **Visualizza → Sposta nella cartella Avanzate**.

Come aggiornare i dati nell'area di lavoro

In Kaspersky Security Center i dati dell'area di lavoro (ad esempio, stati dei dispositivi, statistiche e rapporti) non vengono mai aggiornati automaticamente.

Per aggiornare i dati nell'area di lavoro:

- Premere il tasto **F5**.
- Nel menu di scelta rapida dell'oggetto nella struttura della console selezionare **Aggiorna**.
- Fare clic sull'icona di aggiornamento () nell'area di lavoro.

Come spostarsi nella struttura della console

Per spostarsi nella struttura della console, è possibile utilizzare i seguenti pulsanti della barra degli strumenti:

-  —Un passaggio indietro.
-  —Un passaggio avanti.
-  —Un livello più in alto.

È anche possibile utilizzare una struttura di spostamento nell'angolo superiore destro dell'area di lavoro. La struttura di spostamento contiene il percorso completo della cartella corrente nella struttura della console. Tutti gli elementi della struttura, tranne l'ultimo, sono collegamenti agli oggetti nella struttura della console.

Come aprire le proprietà degli oggetti nell'area di lavoro

È possibile modificare le proprietà della maggior parte degli oggetti di Administration Console nella finestra delle proprietà dell'oggetto.

Per aprire la finestra delle proprietà di un oggetto nell'area di lavoro:

- Dal menu di scelta rapida dell'oggetto selezionare **Proprietà**.
- Selezionare un oggetto, quindi premere **ALT**+**INVIO**.

Come selezionare un gruppo di oggetti nell'area di lavoro

È possibile selezionare un gruppo di oggetti nell'area di lavoro. È ad esempio possibile selezionare un gruppo di oggetti per creare un set di dispositivi per cui creare attività in un secondo momento.

Per selezionare un intervallo di oggetti:

1. Selezionare il primo oggetto dell'intervallo, quindi premere **MAIUSC**.
2. Tenere premuto il tasto **MAIUSC** e selezionare l'ultimo oggetto dell'intervallo.

L'intervallo verrà selezionato.

Per raggruppare oggetti separati:

1. Selezionare il primo oggetto del gruppo, quindi premere **CTRL**.
2. Tenere premuto il tasto **CTRL**, quindi selezionare gli altri oggetti che si desidera includere nel gruppo.

Gli oggetti verranno raggruppati.

Come modificare il set di colonne nell'area di lavoro

Administration Console consente di modificare il set di colonne visualizzate nell'area di lavoro.

Per modificare il set di colonne visualizzate nell'area di lavoro:

1. Nella struttura della console fare clic sull'oggetto per cui si desidera modificare il set di colonne.
2. Nell'area di lavoro della cartella aprire la finestra per la configurazione del set di colonne facendo clic sul collegamento **Aggiungi/Rimuovi colonne**.
3. Nella finestra **Aggiungi/Rimuovi colonne** specificare il set di colonne da visualizzare.

Informazioni di riferimento

Le tabelle di questa sezione forniscono informazioni di riepilogo sul menu di scelta rapida degli oggetti di Administration Console, oltre che sugli stati degli oggetti nella struttura della console e nell'area di lavoro.

Comandi del menu di scelta rapida

In questa sezione sono elencati gli oggetti di Administration Console e le voci corrispondenti del menu di scelta rapida (vedere la tabella seguente).

Voci del menu di scelta rapida degli oggetti di Administration Console

Oggetto	Voce di menu	Funzione della voce di menu
Voci generali del menu di scelta rapida	**Cerca**	Apre la finestra di ricerca dei dispositivi.
	Aggiorna	Aggiorna la visualizzazione dell'oggetto selezionato.
	Esporta elenco	Esporta l'elenco corrente in un file.
	Proprietà	Apre la finestra delle proprietà dell'oggetto selezionato.
	Visualizza → Aggiungi/Rimuovi colonne	Aggiunge o rimuove colonne nella tabella degli oggetti dell'area di lavoro.
	Visualizza → Icone grandi	Visualizza gli oggetti dell'area di lavoro come icone grandi.
	Visualizza → Icone piccole	Visualizza gli oggetti dell'area di lavoro come icone piccole.
	Visualizza → Elenco	Visualizza gli oggetti dell'area di lavoro come un elenco.
	Visualizza → Tabella	Visualizza gli oggetti dell'area di lavoro come una tabella.
	Visualizza → Configura	Configura la visualizzazione degli elementi di Administration Console.
Kaspersky Security Center	**Nuovo → Administration Server**	Aggiunge un Administration Server alla struttura della console.
<Nome Administration Server>	**Connetti ad Administration Server**	Esegue la connessione all'Administration Server.
	Disconnetti da Administration Server	Esegue la disconnessione dall'Administration Server.
Dispositivi gestiti	**Installa applicazione**	Avvia l'Installazione remota guidata.
	Visualizza → Configura interfaccia	Configura la visualizzazione degli elementi di interfaccia.
	Rimuovi	Rimuove l'Administration Server dalla struttura della console.
	Installa applicazione	Avvia l'Installazione remota guidata per il gruppo di amministrazione.
	Reimposta contatore virus	Azzera i contatori dei virus per i dispositivi inclusi nel gruppo di amministrazione.
	Visualizza rapporto sulle minacce	Consente di creare un rapporto sulle minacce e sull'attività dei virus nei dispositivi inclusi nel gruppo di amministrazione.
	Nuovo → Gruppo	Crea un gruppo di amministrazione.
	Tutte le attività → Nuova struttura di gruppi	Crea una struttura di gruppi di amministrazione basata sulla struttura di domini o Active Directory.
	Tutte le attività → Mostra messaggio	Avvia la Creazione guidata nuovo messaggio per l'utente per gli utenti dei dispositivi inclusi nel gruppo di amministrazione.
Dispositivi gestiti → Administration Server	**Nuovo → Administration Server secondario**	Avvia l'Aggiunta guidata Administration Server secondari.
	Nuovo → Administration Server virtuale	Avvia l'Aggiunta guidata nuovo Administration Server virtuale.
Mobile Device Management → Dispositivi mobili	**Nuovo → Dispositivo mobile**	Connette un nuovo dispositivo mobile dell'utente.
Mobile Device Management → Certificati	**Nuovo → Certificato**	Crea un certificato.
	Crea → Dispositivo mobile	Connette un nuovo dispositivo mobile dell'utente.
Selezioni dispositivi	**Nuovo → Nuova selezione**	Crea una selezione dispositivi.
	Tutte le attività → Importa	Importa una selezione da un file.

Oggetto	Voce di menu	Funzione della voce di menu
Licenze di Kaspersky	**Aggiungi codice di attivazione o file chiave**	Aggiunge una chiave di licenza all'archivio di Administration Server.
	Attiva l'applicazione	Avvia la Creazione guidata attività di attivazione dell'applicazione.
	Rapporto sull'utilizzo delle chiavi di licenza	Crea e visualizza un rapporto sulle chiavi di licenza nei dispositivi client.
Gestione applicazioni → Categorie di applicazioni	**Nuovo → Categoria**	Crea una categoria di applicazioni.
Gestione applicazioni → Registro delle applicazioni	**Filtro**	Configura un filtro per l'elenco delle applicazioni.
	Applicazioni monitorate	Configura la pubblicazione di eventi relativi all'installazione delle applicazioni.
	Rimuovi le applicazioni non installate	Cancella l'elenco con tutti i dettagli delle applicazioni che non sono più installate nei dispositivi in rete.
Gestione applicazioni → Aggiornamenti software	**Accetta Contratti di licenza per gli aggiornamenti**	Accetta i contratti di licenza degli aggiornamenti software.
Gestione applicazioni → Utilizzo licenze di terze parti	**Nuovo → Gruppo di applicazioni concesse in licenza**	Crea un gruppo di applicazioni concesse in licenza.
Installazione remota → Pacchetti di installazione	**Mostra versioni correnti delle applicazioni**	Visualizza l'elenco delle versioni correnti delle applicazioni Kaspersky disponibili nei server Web.
	Nuovo → Pacchetto di installazione	Crea un pacchetto di installazione.
	Tutte le attività → Aggiorna database	Aggiorna i database dell'applicazione nei pacchetti di installazione.
	Tutte le attività → Mostra l'elenco generale dei pacchetti indipendenti	Visualizza l'elenco dei pacchetti di installazione indipendenti creati per i pacchetti di installazione.
Device discovery → Domini	**Tutte le attività → Attività dei dispositivi**	Imposta la risposta di Administration Server in caso di inattività dei dispositivi in rete.
Device discovery → Intervalli IP	**Nuovo → Intervallo IP**	Crea un intervallo IP.
Archivi → Aggiornamenti per database e moduli software Kaspersky	**Scarica aggiornamenti**	Apre la finestra delle proprietà dell'attività Scarica aggiornamenti nell'archivio di Administration Server.
	Impostazioni di download degli aggiornamenti	Configura l'attività Scarica aggiornamenti nell'archivio di Administration Server.
	Rapporto sull'utilizzo dei database anti-virus	Crea e visualizza un rapporto sulle versioni dei database.
	Tutte le attività → Cancella archivio aggiornamenti	Cancella l'archivio degli aggiornamenti in Administration Server.
Archivi → Hardware	**Nuovo → Dispositivo**	Crea un nuovo dispositivo.

Elenco dei dispositivi gestiti. Descrizione delle colonne

Nella tabella seguente sono visualizzati i nomi e le rispettive descrizioni delle colonne dell'elenco dei dispositivi gestiti.

Descrizioni delle colonne dell'elenco dei dispositivi gestiti

Nome colonna	Valore
Nome	Nome NetBIOS del dispositivo client. Le descrizioni delle icone dei nomi dei dispositivi vengono fornite nell'appendice.
Tipo di sistema operativo	Tipo di sistema operativo installato nel dispositivo client.
Dominio Windows	Nome del dominio Windows a cui appartiene il dispositivo client.
Network Agent installato	Risultato dell'installazione di Network Agent nel dispositivo client: *Sì*, *No*, *Sconosciuto*.

Nome colonna	Valore
Network Agent è in esecuzione	Risultato del funzionamento di Network Agent: *Sì*, *No*, *Sconosciuto*.
Protezione in tempo reale	L'applicazione di protezione è installata: *Sì*, *No*, *Sconosciuto*.
Ultima connessione ad Administration Server	Periodo di tempo trascorso dalla connessione del dispositivo client ad Administration Server.
Ultimo aggiornamento dei database anti-virus	Il periodo di tempo trascorso dall'ultimo aggiornamento dei dispositivi gestiti.
Stato	Stato attuale del dispositivo client: *OK*, *Critical*, *or Warning*.
Descrizione stato	Condizione per la modifica dello stato del dispositivo client in *Critico* o *Avviso*. Lo stato del dispositivo cambia in *Avviso* o *Critico* in base alle seguenti condizioni: • Applicazione di protezione non installata. • Troppi virus rilevati. • Livello protezione in tempo reale diverso da quello impostato dall'amministratore. • Scansione malware non eseguita da molto tempo. • I database non sono aggiornati. • Connessione non eseguita da molto tempo. • Rilevate minacce attive. • È necessario il riavvio. Il motivo per cui è necessario riavviare il dispositivo può essere uno dei seguenti: ◦ Riavvio eseguito per motivo sconosciuto. ◦ L'applicazione non verrà eseguita fino al riavvio. ◦ È necessario il riavvio per completare l'aggiornamento. L'applicazione è in esecuzione. ◦ È necessario il riavvio per avviare l'aggiornamento. ◦ È necessario il riavvio per completare la scansione o la disinfezione. ◦ È necessario il riavvio per completare l'installazione o la disinstallazione remota. ◦ Completamento criptaggio dei dati su disco. È possibile impostare i motivi durante la configurazione della commutazione degli stati dei dispositivi. • Applicazioni incompatibili installate. • Rilevate vulnerabilità del software. • Verifica disponibilità aggiornamenti di Windows Update non eseguita da molto tempo. • Stato criptaggio non valido. • Impostazioni dispositivo mobile non conformi al criterio. • Problemi di sicurezza non elaborati rilevati. • Stato dispositivo definito dall'applicazione. • Spazio su disco esaurito nel dispositivo. • La licenza sta per scadere. Lo stato del dispositivo cambia in *Critico* solo per i seguenti motivi: • La licenza è scaduta. • Il dispositivo è diventato non gestito. • Protezione disattivata. • Applicazione di protezione non in esecuzione. Le applicazioni Kaspersky gestite nei dispositivi client possono aggiungere descrizioni dello stato all'elenco. Kaspersky Security Center può ricevere la descrizione di uno stato del dispositivo client dalle applicazioni Kaspersky gestite installate nel dispositivo. Se lo stato che è stato assegnato al dispositivo dall'applicazione gestita è diverso da quello assegnato da Kaspersky Security Center, Administration Console visualizza lo stato più critico per la sicurezza del dispositivo. Se ad esempio un'applicazione gestita ha assegnato lo stato *Critico* al dispositivo mentre Kaspersky Security Center ha assegnato lo stato *Avviso*, Administration Console visualizza per il dispositivo lo stato *Critico* con la descrizione corrispondente fornita dall'applicazione gestita.
Informazioni aggiornate	Periodo di tempo trascorso dall'ultima sincronizzazione del dispositivo client con Administration Server (cioè dall'ultima scansione di rete).
Nome DNS	Nome dominio DNS del dispositivo client.
Dominio DNS	Suffisso DNS principale.

Nome colonna	Valore
Indirizzo IP	Indirizzo IP del dispositivo client. È consigliabile utilizzare l'indirizzo IPv4.
Ultima visibilità	Periodo di tempo per cui il dispositivo client è rimasto visibile in rete.
Ultima scansione completa	Data e ora dell'ultima scansione del dispositivo client eseguita dall'applicazione di protezione su richiesta dell'utente.
Numero totale di minacce rilevate	Numero di minacce rilevate.
Stato protezione in tempo reale	Stato protezione in tempo reale: *Avvio in corso*, *In esecuzione*, *In esecuzione (protezione massima)*, *In esecuzione (velocità massima)*, *In esecuzione (impostazione consigliata)*, *In esecuzione (impostazioni personalizzate)*, *Arrestato*, *Sospeso*, *Non riuscito*.
Indirizzo IP connessione	Indirizzo IP utilizzato per la connessione a Kaspersky Security Center Administration Server.
Versione di Network Agent	Versione di Network Agent.
Versione applicazione	Versione dell'applicazione di protezione installata nel dispositivo client.
Database anti-virus rilasciati	Versione dei database anti-virus.
Ultimo avvio del sistema	Data e ora dell'ultima accensione del dispositivo client.
È necessario il riavvio	È richiesto il riavvio del dispositivo client.
Punto di distribuzione	Nome del dispositivo che opera come punto di distribuzione per questo dispositivo client.
Descrizione	Descrizione del dispositivo client ricevuta dopo una scansione della rete.
Stato criptaggio	Stato di criptaggio dei dati del dispositivo client.
Stato WUA	Stato dell'Agente di Windows Update nel dispositivo client. *Sì* corrisponde ai dispositivi client che ricevono gli aggiornamenti tramite Windows Update da Administration Server. *No* corrisponde ai dispositivi client che ricevono gli aggiornamenti tramite Windows Update da altre origini.
Dimensioni in bit del sistema operativo	Dimensioni in bit del sistema operativo installato nel dispositivo client.
Stato protezione Anti-Spam	Stato del componente della protezione Anti-Spam: *In esecuzione*, *Avvio in corso*, *Arrestata*, *Sospesa*, *Non riuscito*, *Sconosciuto*
Stato prevenzione fughe di dati	Stato del componente di prevenzione della perdita dei dati: *In esecuzione*, *Avvio in corso*, *Arrestata*, *Sospesa*, *Non riuscito*, *Sconosciuto*
Stato protezione server di collaborazione	Stato del componente di filtro contenuti: *In esecuzione*, *Avvio in corso*, *Arrestata*, *Sospesa*, *Non riuscito*, *Sconosciuto*
Stato protezione anti-virus server di posta	Stato del componente della protezione anti-virus del server di posta: *In esecuzione*, *Avvio in corso*, *Arrestata*, *Sospesa*, *Non riuscito*, *Sconosciuto*
Stato Endpoint Sensor	Stato del componente Endpoint Detection and Response (KATA): *In esecuzione*, *Avvio in corso*, *Arrestata*, *Sospesa*, *Non riuscito*, *Sconosciuto*
Data creazione	Momento in cui è stata creata l'icona di <Nome dispositivo>. Questo attributo viene utilizzato per confrontare tra loro vari eventi.
Nome dell'Administration Server virtuale o secondario	Nome dell'Administration Server virtuale o secondario. Questa colonna è disponibile solo negli elenchi che contengono dispositivi di diversi Administration Server.
Gruppo padre	Nome del gruppo di amministrazione in cui si trova l'icona di <Nome dispositivo>. Questa colonna è disponibile solo negli elenchi che contengono dispositivi di diversi Administration Server.

Nome colonna	Valore
Gestito da un altro Administration Server	Il parametro può assumere uno dei seguenti valori: • True, se durante l'installazione remota delle applicazioni di protezione nel dispositivo, risulta che il dispositivo è gestito da un altro Administration Server. • False, in caso contrario.
Build del sistema operativo	Numero di build del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un numero di build uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti i numeri di build ad eccezione di quello specificato.
ID di rilascio del sistema operativo	Identificatore della versione (ID) del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un ID di rilascio uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti gli ID di rilascio ad eccezione di quello specificato.

Stati di dispositivi, attività e criteri

La tabella seguente contiene un elenco delle icone visualizzate nella struttura della console e nell'area di lavoro di Administration Console accanto al nome dei dispositivi, delle attività e dei criteri. Queste icone definiscono lo stato degli oggetti.

Stati di dispositivi, attività e criteri

Icona	Stato
	Dispositivo con un sistema operativo per workstation, rilevato nel sistema ma non ancora incluso in alcun gruppo di amministrazione.
	Dispositivo con un sistema operativo per workstation incluso in un gruppo di amministrazione, con stato *OK*.
	Dispositivo con un sistema operativo per workstation incluso in un gruppo di amministrazione, con stato *Avviso*.
	Dispositivo con un sistema operativo per workstation incluso in un gruppo di amministrazione, con stato *Critico*.
	Dispositivo con un sistema operativo per workstation incluso in un gruppo di amministrazione, che ha perso la connessione con l'Administration Server.
	Dispositivo con un sistema operativo per server, rilevato nel sistema ma non ancora incluso in alcun gruppo di amministrazione.
	Dispositivo con un sistema operativo per server incluso in un gruppo di amministrazione, con stato *OK*.
	Dispositivo con un sistema operativo per server incluso in un gruppo di amministrazione, con stato *Avviso*.
	Dispositivo con un sistema operativo per server incluso in un gruppo di amministrazione, con stato *Critico*.
	Dispositivo con un sistema operativo per server incluso in un gruppo di amministrazione, che ha perso la connessione con l'Administration Server.
	Dispositivo mobile rilevato nella rete e non incluso in alcun gruppo di amministrazione.
	Dispositivo mobile incluso in un gruppo di amministrazione con stato *OK*.
	Dispositivo mobile incluso in un gruppo di amministrazione con stato *Avviso*.
	Dispositivo mobile incluso in un gruppo di amministrazione con stato *Critico*.
	Dispositivo mobile incluso in un gruppo di amministrazione che ha perso la connessione con l'Administration Server.
	Dispositivo di protezione UEFI rilevato nella rete, ma non incluso in alcun gruppo di amministrazione. Il dispositivo di protezione UEFI si trova nella rete.
	Dispositivo di protezione UEFI rilevato nella rete, ma non incluso in alcun gruppo di amministrazione. Il dispositivo di protezione UEFI non si trova nella rete.

	Dispositivo di protezione UEFI incluso in un gruppo di amministrazione con stato *OK*. Il dispositivo di protezione UEFI si trova nella rete.
	Dispositivo di protezione UEFI incluso in un gruppo di amministrazione con stato *OK*. Il dispositivo di protezione UEFI non si trova nella rete.
	Dispositivo di protezione UEFI incluso in un gruppo di amministrazione con stato *Avviso*. Il dispositivo di protezione UEFI si trova nella rete.
	Dispositivo di protezione UEFI incluso in un gruppo di amministrazione con stato *Avviso*. Il dispositivo di protezione UEFI non si trova nella rete.
	Dispositivo di protezione UEFI incluso in un gruppo di amministrazione con stato *Critico*. Il dispositivo di protezione UEFI si trova nella rete.
	Dispositivo di protezione UEFI incluso in un gruppo di amministrazione con stato *Critico*. Il dispositivo di protezione UEFI non si trova nella rete.
	Criterio attivo.
	Criterio inattivo.
	Criterio attivo ereditato da un gruppo che è stato creato nell'Administration Server primario.
	Criterio attivo ereditato da un gruppo di livello superiore.
	Attività (attività di gruppo, attività di Administration Server o attività per dispositivi specifici) con stato *Pianificato* o *Completato*.
	Attività (attività di gruppo, attività di Administration Server o attività per dispositivi specifici) con stato *In esecuzione*.
	Attività (attività di gruppo, attività di Administration Server o attività per dispositivi specifici) con stato *Non riuscito*.
	Attività ereditata da un gruppo che è stato creato nell'Administration Server primario.
	Attività ereditata da un gruppo di livello superiore.

Icone di stato dei file in Administration Console

Per semplificare la gestione dei file in Kaspersky Security Center Administration Console, accanto ai nomi dei file vengono visualizzate delle icone (vedere la tabella di seguito). Le icone indicano gli stati assegnati ai file dalle applicazioni Kaspersky gestite nei dispositivi client. Le icone sono visualizzate nelle aree di lavoro delle cartelle **Quarantena**, **Backup** e **Minacce attive**.

Gli stati vengono assegnati agli oggetti da Kaspersky Endpoint Security installato nel dispositivo client in cui si trova l'oggetto.

Corrispondenza tra icone e stati dei file

Icona	Stato
	File con lo stato *Infetto*.
	File con lo stato *Avviso* o *Potenzialmente infetto*.
	File con lo stato *Aggiunto dall'utente*.
	File con lo stato *Falso positivo*.
	File con lo stato *Disinfettato*.
	File con lo stato *Eliminato*.
	File nella cartella **Quarantena** con lo stato *Non infetto*, *Protetto da password* o *Deve essere inviato a Kaspersky*. Se non è disponibile alcuna descrizione dello stato accanto a un'icona, l'applicazione Kaspersky gestita nel dispositivo client ha segnalato uno stato sconosciuto a Kaspersky Security Center.

	File nella cartella **Backup** con lo stato *Non infetto, Protetto da password* o *Deve essere inviato a Kaspersky*. Se non è disponibile alcuna descrizione dello stato accanto a un'icona, l'applicazione Kaspersky gestita nel dispositivo client ha segnalato uno stato sconosciuto a Kaspersky Security Center.
	File nella cartella **Minacce attive** con lo stato *Non infetto, Protetto da password* o *Deve essere inviato a Kaspersky*. Se non è disponibile alcuna descrizione dello stato accanto a un'icona, l'applicazione Kaspersky gestita nel dispositivo client ha segnalato uno stato sconosciuto a Kaspersky Security Center.

Ricerca ed esportazione dei dati

Questa sezione contiene informazioni sui metodi di ricerca dei dati e sull'esportazione dei dati.

Ricerca di dispositivi

Kaspersky Security Center consente di individuare i dispositivi sulla base dei criteri specificati. I risultati della ricerca possono essere salvati in un file di testo.

La funzionalità di ricerca consente di trovare i seguenti dispositivi:

- I dispositivi client nei gruppi di amministrazione di un Administration Server e dei relativi server secondari.
- I dispositivi non assegnati gestiti da un Administration Server e dai relativi server secondari.

Per trovare i dispositivi client inclusi in un gruppo di amministrazione:

1. Nella struttura della console selezionare la cartella di un gruppo di amministrazione.
2. Selezionare **Cerca** dal menu di scelta rapida della cartella del gruppo di amministrazione.
3. Nelle schede della finestra **Ricerca** specificare i criteri per la ricerca dei dispositivi, quindi fare clic sul pulsante **Trova**.

   I dispositivi che soddisfano i criteri di ricerca specificati adesso vengono visualizzati in una tabella nella parte inferiore della finestra **Ricerca**.

Per trovare i dispositivi non assegnati:

1. Nella struttura della console selezionare la cartella **Dispositivi non assegnati**.
2. Selezionare **Cerca** dal menu di scelta rapida della cartella **Dispositivi non assegnati**.
3. Nelle schede della finestra **Ricerca** specificare i criteri per la ricerca dei dispositivi, quindi fare clic sul pulsante **Trova**.

   I dispositivi che soddisfano i criteri di ricerca specificati adesso vengono visualizzati in una tabella nella parte inferiore della finestra **Ricerca**.

Per trovare i dispositivi indipendentemente dalla loro appartenenza a un gruppo di amministrazione:

1. Nella struttura della console selezionare il nodo **Administration Server %s**.
2. Nel menu di scelta rapida del nodo selezionare **Cerca**.
3. Nelle schede della finestra **Ricerca** specificare i criteri per la ricerca dei dispositivi, quindi fare clic sul pulsante **Trova**.

I dispositivi che soddisfano i criteri di ricerca specificati adesso vengono visualizzati in una tabella nella parte inferiore della finestra **Ricerca**.

Nella finestra **Ricerca** è inoltre possibile cercare gruppi di amministrazione e Administration Server secondari tramite un elenco a discesa nell'angolo superiore destro della finestra. La funzionalità di ricerca dei gruppi di amministrazione e degli Administration Server secondari non è disponibile se la finestra **Ricerca** è stata aperta dalla cartella **Dispositivi non assegnati**.

Per trovare i dispositivi, è possibile utilizzare espressioni regolari nei campi della finestra **Ricerca**.

La ricerca full-text nella finestra **Ricerca** è disponibile:

- Nella scheda **Rete**, nel campo **Descrizione**
- Nella scheda **Hardware**, nei campi **Dispositivo**, **Fornitore** e **Descrizione**

Impostazioni di ricerca del dispositivo

Di seguito sono descritte le impostazioni utilizzate per la ricerca dei dispositivi gestiti. I risultati di ricerca vengono visualizzati nella parte inferiore della finestra.

Rete

Nella scheda **Rete** è possibile specificare i criteri che verranno utilizzati per la ricerca dei dispositivi in base ai dati della rete:

- **Nome o indirizzo IP dispositivo**

  Nome di rete Windows (nome NetBIOS) del dispositivo o indirizzo IPv4 o IPv6.

- **Dominio Windows**

  Visualizza tutti i dispositivi inclusi nel dominio Windows specificato.

- **Gruppo di amministrazione**

  Visualizza i dispositivi inclusi nel gruppo di amministrazione specificato.

- **Descrizione**

  Testo contenuto nella finestra delle proprietà del dispositivo: nel campo **Descrizione** della sezione **Generale**.

  Per inserire il testo nel campo **Descrizione**, è possibile utilizzare i seguenti caratteri:

  - All'interno di una parola:

    - *****. Sostituisce qualsiasi stringa con qualsiasi numero di caratteri.

    Esempio:

    Per descrivere parole come **Server** o **Server's**, è possibile immettere **Server***.

    - **?.** Sostituisce qualsiasi carattere singolo.

    Esempio:

    Per descrivere parole come **Finestra** o **Finestre**, è possibile immettere **Finestr?**.

    Non è possibile utilizzare l'asterisco (*****) o il punto interrogativo (**?**) come primo carattere nella query.

  - Per trovare più parole:

    - Spazio. Visualizza tutti i dispositivi le cui descrizioni contengono una delle parole elencate.

    Esempio:

    Per trovare una frase contenente le parole **Secondario** o **Virtuale**, è possibile includere la riga **Secondario Virtuale** nella query.

    - **+**. Quando una parola è preceduta dal segno +, tutti i risultati della ricerca conterranno tale parola.

    Esempio:

    Per trovare una frase contenente sia **Secondario** che **Virtuale**, immettere la query **+Secondario+Virtuale**.

    - **-**. Quando una parola è preceduta dal segno -, nessun risultato della ricerca conterrà tale parola.

    Esempio:

    Per trovare una frase contenente **Secondario** e non contenente **Virtuale**, immettere la query **+Secondario-Virtuale**.

    - **"<testo>"**. Verranno visualizzati i risultati che contengono il testo racchiuso tra virgolette.

    Esempio:

    Per trovare una frase contenente la combinazione di parole **Server secondario**, è possibile immettere **"Server secondario"** nella query.

- Intervallo IP

  Se questa opzione è abilitata, è possibile immettere gli indirizzi IP iniziale e finale dell'intervallo IP in cui i dispositivi rilevanti devono essere inclusi.

  Per impostazione predefinita, questa opzione è disabilitata.

- Gestito da un altro Administration Server

  Selezionare uno dei seguenti valori:

  - **Sì**. Vengono considerati solo i dispositivi client gestiti da altri Administration Server.
  - **No**. Vengono considerati solo i dispositivi client gestiti dallo stesso Administration Server.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Tag

Nella scheda **Tag** è possibile configurare una ricerca dei dispositivi in base alle parole chiave (tag) aggiunte in precedenza alle descrizioni dei dispositivi gestiti:

- Applica se almeno uno dei tag specificati corrisponde

  Se questa opzione è abilitata, i risultati di ricerca visualizzeranno i dispositivi con descrizioni contenenti almeno uno dei tag selezionati.

  Se questa opzione è disabilitata, i risultati di ricerca visualizzeranno solo i dispositivi con descrizioni contenenti tutti i tag selezionati.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il tag deve essere incluso

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

  Per impostazione predefinita, questa opzione è selezionata.

- Il tag deve essere escluso

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni non contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

Active Directory

Nella scheda **Active Directory** è possibile specificare che la ricerca dei dispositivi deve avvenire nel gruppo o nell'unità organizzativa di Active Directory. È inoltre possibile includere nella selezione i dispositivi di tutte le unità organizzative secondarie dell'unità organizzativa di Active Directory specificata. Per selezionare i dispositivi, definire le seguenti impostazioni:

- Il dispositivo si trova in un'unità organizzativa di Active Directory

  Se questa opzione è abilitata, la selezione includerà i dispositivi dell'unità organizzativa Active Directory specificata nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

- Includi unità organizzative secondarie

  Se questa opzione è abilitata, la selezione includerà i dispositivi in tutte le unità organizzative secondarie dell'unità organizzativa del dominio specificato.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il dispositivo fa parte di un gruppo di Active Directory

  Se questa opzione è abilitata, la selezione includerà i dispositivi del gruppo Active Directory specificato nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

Attività di rete

Nella scheda **Attività di rete** è possibile specificare i criteri che verranno utilizzati per la ricerca dei dispositivi in base all'attività della rete:

- Il dispositivo è un punto di distribuzione

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione include i dispositivi che operano come punti di distribuzione.
  - **No**. I dispositivi che operano come punti di distribuzione non sono inclusi nella selezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Non eseguire la disconnessione da Administration Server

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Abilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è selezionata.
  - **Disabilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è deselezionata.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Profilo connessione cambiato

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **No**. La selezione non includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Ultima connessione ad Administration Server

  È possibile utilizzare questa casella di controllo per impostare un criterio di ricerca per i dispositivi in base all'ora dell'ultima connessione ad Administration Server.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stata stabilita l'ultima connessione tra Network Agent installato nel dispositivo client e Administration Server. La selezione includerà i dispositivi che rientrano nell'intervallo specificato.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Rilevati nuovi dispositivi durante il polling della rete

  Cerca nuovi dispositivi rilevati dal polling della rete negli ultimi giorni.

  Se questa opzione è abilitata, la selezione includerà soltanto i nuovi dispositivi rilevati dalla device discovery nel numero di giorni specificato nel campo **Periodo di rilevamento (giorni)**.

  Se questa opzione è disabilitata, la selezione includerà tutti i dispositivi rilevati dalla device discovery.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il dispositivo è visibile

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. L'applicazione include nella selezione i dispositivi attualmente visibili nella rete.
  - **No**. L'applicazione include nella selezione i dispositivi attualmente invisibili nella rete.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Applicazione

Nella scheda **Applicazione** è possibile specificare i criteri che verranno utilizzati per la ricerca dei dispositivi in base all'applicazione gestita selezionata:

- **Nome applicazione**

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome di un'applicazione Kaspersky.

  L'elenco contiene solo i nomi delle applicazioni con plug-in di gestione installati nella workstation dell'amministratore.

  Se non è selezionata alcuna applicazione, il criterio non verrà applicato.

- **Versione applicazione**

  Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al numero versione di un'applicazione Kaspersky.

  Se non è specificato alcun numero di versione, il criterio non verrà applicato.

- **Nome aggiornamento critico**

  Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome dell'applicazione o al numero del pacchetto di aggiornamento.

  Se il campo è vuoto, il criterio non verrà applicato.

- **Ultimo aggiornamento dei moduli**

  È possibile utilizzare questa opzione per impostare un criterio per la ricerca dei dispositivi in base all'ora dell'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stato eseguito l'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Il dispositivo è gestito tramite Kaspersky Security Center

  Nell'elenco a discesa è possibile includere nella selezione i dispositivi gestiti tramite Kaspersky Security Center:

  - **Sì**. L'applicazione include nella selezione i dispositivi gestiti tramite Kaspersky Security Center.
  - **No**. L'applicazione include nella selezione i dispositivi non gestiti tramite Kaspersky Security Center.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- L'applicazione di protezione è installata

  Nell'elenco a discesa è possibile includere nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione:

  - **Sì**. L'applicazione include nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione.
  - **No**. L'applicazione include nella selezione tutti i dispositivi in cui non è installata un'applicazione di protezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Sistema operativo

Nella scheda **Sistema operativo** è possibile configurare i seguenti criteri per la ricerca dei dispositivi in base al tipo di sistema operativo:

- Versione del sistema operativo

  Se la casella di controllo è selezionata, è possibile selezionare un sistema operativo dall'elenco. I dispositivi in cui sono installati i sistemi operativi specificati saranno inclusi nei risultati della ricerca.

- Dimensioni in bit del sistema operativo

  Nell'elenco a discesa è possibile selezionare l'architettura del sistema operativo da cui dipenderà l'applicazione della regola di spostamento al dispositivo (**Sconosciuto**, **x86**, **AMD64** o **IA64**). Per impostazione predefinita, non è selezionata alcuna opzione nell'elenco, pertanto l'architettura del sistema operativo non è definita.

- Versione Service Pack del sistema operativo

  In questo campo è possibile specificare la versione del pacchetto del sistema operativo (nel formato *X.Y*), da cui dipenderà l'applicazione della regola di spostamento al dispositivo. Per impostazione predefinita, non è specificato alcun valore per la versione.

- **Build del sistema operativo**

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Numero di build del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un numero di build uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti i numeri di build ad eccezione di quello specificato.

- **ID di rilascio del sistema operativo**

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Identificatore della versione (ID) del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un ID di rilascio uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti gli ID di rilascio ad eccezione di quello specificato.

Stato dispositivo

Nella scheda **Stato dispositivo** è possibile specificare i criteri per la ricerca dei dispositivi in base allo stato del dispositivo ottenuto dall'applicazione gestita:

- **Stato dispositivo**

  Elenco a discesa in cui è possibile selezionare uno degli stati del dispositivo: *OK*, *Critico* o *Avviso*.

- **Stato protezione in tempo reale**

  Elenco a discesa in cui è possibile selezionare lo stato della protezione in tempo reale. I dispositivi con lo stato della protezione in tempo reale specificato vengono inclusi nella selezione.

- **Descrizione stato del dispositivo**

  In questo campo è possibile selezionare le caselle di controllo accanto alle condizioni che, se soddisfatte, assegnano al dispositivo uno dei seguenti stati: *OK*, *Critico* o *Avviso*.

- **Stato dispositivo definito dall'applicazione**

  Elenco a discesa in cui è possibile selezionare lo stato della protezione in tempo reale. I dispositivi con lo stato della protezione in tempo reale specificato vengono inclusi nella selezione.

Componenti della protezione

Nella scheda **Componenti della protezione** è possibile configurare i criteri di ricerca dei dispositivi client in base allo stato della protezione.

- **Data rilascio database**

  Se questa opzione è selezionata, è possibile eseguire la ricerca dei dispositivi client in base alla data di rilascio del database anti-virus. Nei campi di immissione è possibile impostare l'intervallo di tempo in base al quale eseguire la ricerca.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Ultima scansione**

  Se questa opzione è abilitata, è possibile eseguire la ricerca dei dispositivi client in base all'ora dell'ultima scansione malware. Nei campi di immissione è possibile specificare il periodo di tempo entro il quale è stata eseguita l'ultima scansione malware.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Numero totale di minacce rilevate**

  Se questa opzione è abilitata, è possibile eseguire la ricerca di dispositivi client in base al numero di virus rilevati. Nei campi di immissione è possibile impostare i valori di soglia inferiore e superiore per il numero di virus trovati.

  Per impostazione predefinita, questa opzione è disabilitata.

Registro delle applicazioni

Nella scheda **Registro delle applicazioni** è possibile configurare la ricerca dei dispositivi in base alle applicazioni installate:

- **Nome applicazione**

  Elenco a discesa da cui è possibile selezionare un'applicazione. I dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- **Versione applicazione**

  Campo di immissione in cui è possibile specificare la versione dell'applicazione selezionata.

- **Fornitore**

  Elenco a discesa da cui è possibile selezionare il produttore di un'applicazione installata nel dispositivo.

- **Stato applicazione**

  Elenco a discesa da cui è possibile selezionare lo stato di un'applicazione (*Installata*, *Non installata*). Verranno inclusi nella selezione i dispositivi in cui è installata o non è installata l'applicazione specificata, in base allo stato selezionato.

- **Trova per aggiornamento**

  Se questa opzione è abilitata, la ricerca verrà eseguita utilizzando i dettagli degli aggiornamenti per le applicazioni installate nei dispositivi. Dopo aver selezionato la casella di controllo, i campi **Nome applicazione**, **Versione applicazione** e **Stato applicazione** diventano rispettivamente **Nome aggiornamento**, **Versione aggiornamento** e **Stato**.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Nome applicazione di protezione incompatibile**

  Elenco a discesa da cui è possibile selezionare applicazioni di protezione di terze parti. Durante la ricerca, i dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- **Tag applicazione**

  Nell'elenco a discesa è possibile selezionare il tag di un'applicazione. Tutti i dispositivi che hanno applicazioni installate con il tag selezionato nella descrizione sono inclusi nella selezione dispositivi.

Gerarchia di Administration Server

Nella scheda **Gerarchia di Administration Server** selezionare la casella **Includi dati degli Administration Server secondari (fino al livello)** se si desidera valutare le informazioni archiviate negli Administration Server secondari durante la ricerca di dispositivi e, nel campo di immissione, è possibile specificare il livello di annidamento dell'Administration Server secondario da cui vengono valutate le informazioni durante la ricerca dei dispositivi. Per impostazione predefinita, questa casella di controllo è deselezionata.

Macchine virtuali

Nella scheda **Macchine virtuali** è possibile configurare la ricerca dei dispositivi in base al fatto che siano macchine virtuali o facciano parte di Microsoft Virtual Desktop Infrastructure (VDI):

- Questa è una macchina virtuale

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Non importante**.
  - **No**. I dispositivi che non sono macchine virtuali vengono trovati.
  - **Sì**. Vengono trovati i dispositivi che sono macchine virtuali.

- Tipo di macchina virtuale

  Nell'elenco a discesa è possibile selezionare il produttore della macchina virtuale.

  Questo elenco a discesa è disponibile se è selezionato il valore **Sì** o **Non importante** nell'elenco a discesa **Questa è una macchina virtuale**.

- Parte di Virtual Desktop Infrastructure

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Non importante**.
  - **No**. Vengono trovati i dispositivi che non fanno parte di Virtual Desktop Infrastructure.
  - **Sì**. Vengono trovati i dispositivi che fanno parte di Microsoft Virtual Desktop Infrastructure (VDI).

Hardware

Nella scheda **Hardware** è possibile configurare la ricerca dei dispositivi client in base al relativo hardware:

- Dispositivo

  Nell'elenco a discesa è possibile selezionare un tipo di unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- Fornitore

  Nell'elenco a discesa è possibile selezionare il nome di un produttore dell'unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- **Descrizione**

  Descrizione del dispositivo o dell'unità hardware. I dispositivi con la descrizione specificata in questo campo verranno inclusi nella selezione.

  La descrizione di un dispositivo in qualsiasi formato può essere immessa nella finestra delle proprietà del dispositivo. Il campo supporta la ricerca full-text.

- **Numero di inventario**

  L'apparecchiatura con il numero di inventario specificato in questo campo verrà inclusa nella selezione.

- **Frequenza CPU (MHz)**

  L'intervallo di frequenze di una CPU. I dispositivi con CPU corrispondenti all'intervallo di frequenze in questi campi (compresi) verranno inclusi nella selezione.

- **Core CPU virtuali**

  Intervallo del numero di core virtuali in una CPU. I dispositivi con CPU corrispondenti all'intervallo in questi campi (compresi) verranno inclusi nella selezione.

- **Volume disco rigido (GB)**

  Intervallo di valori per le dimensioni del disco rigido nel dispositivo. I dispositivi con dischi rigidi corrispondenti all'intervallo in questi campi di immissione (compresi) verranno inclusi nella selezione.

- **Dimensione RAM (MB)**

  Intervallo di valori per le dimensioni della RAM del dispositivo. I dispositivi con RAM corrispondenti all'intervallo presente in questi campi di immissione (compresi i valori specificati) verranno inclusi nella selezione.

Vulnerabilità e aggiornamenti

Nella scheda **Vulnerabilità e aggiornamenti** è possibile impostare il criterio di ricerca dei dispositivi in base all'origine di Windows Update:

- **WUA è passato ad Administration Server**

  È possibile selezionare una delle seguenti opzioni di ricerca nell'elenco a discesa:

  - **Sì**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da Administration Server.
  - **No**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da altre origini.

Utenti

Nella scheda **Utenti** è possibile impostare i criteri di ricerca dei dispositivi in base agli account degli utenti che hanno eseguito l'accesso al sistema operativo.

- **Ultimo utente che ha eseguito l'accesso al sistema**

  Se questa opzione è abilitata, fare clic sul pulsante **Sfoglia** per specificare un account utente. I risultati della ricerca includeranno i dispositivi in cui l'utente specificato ha eseguito l'ultimo accesso al sistema.

- **Utente che ha eseguito l'accesso al sistema almeno una volta**

  Se questa opzione è abilitata, fare clic sul pulsante **Sfoglia** per specificare un account utente. I risultati della ricerca includeranno i dispositivi in cui l'utente specificato ha eseguito l'accesso al sistema almeno una volta.

Problemi che influiscono sullo stato nelle applicazioni gestite

Nella scheda **Problemi che influiscono sullo stato nelle applicazioni gestite** è possibile impostare la ricerca dei dispositivi in base alle descrizioni dei relativi stati forniti dall'applicazione gestita:

- **Descrizione stato del dispositivo**

  È possibile selezionare le caselle di controllo relative alle descrizioni degli stati dall'applicazione gestita. Alla ricezione di questi stati, i dispositivi verranno inclusi nella selezione. Quando si seleziona uno stato elencato per diverse applicazioni, è possibile selezionare automaticamente questo stato in tutti gli elenchi.

Stati dei componenti nelle applicazioni gestite

Nella scheda **Stati dei componenti nelle applicazioni gestite** è possibile impostare i criteri per la ricerca dei dispositivi in base agli stati dei componenti nelle applicazioni gestite:

- **Stato prevenzione fughe di dati**

  Cercare i dispositivi in base allo stato di prevenzione della perdita dei dati (*Sconosciuto, Arrestata, Avvio in corso, Sospesa, In esecuzione, Non riuscito*).

- **Stato protezione server di collaborazione**

  Cercare i dispositivi in base allo stato della protezione della collaborazione server (*Sconosciuto*, *Arrestata*, *Avvio in corso, Sospesa*, *In esecuzione*, *Non riuscito*).

- **Stato protezione anti-virus server di posta**

  Cercare i dispositivi in base allo stato della protezione dei server di posta (*Sconosciuto, Arrestata, Avvio in corso, Sospesa, In esecuzione, Non riuscito*).

- **Stato Endpoint Sensor**

  Cercare i dispositivi in base allo stato del componente Sensore Endpoint (*Sconosciuto, Arrestata, Avvio in corso, Sospesa, In esecuzione, Non riuscito*).

Criptaggio

- **Criptaggio**

  Algoritmo di cifratura a blocchi AES (Advanced Encryption Standard). Nell'elenco a discesa è possibile selezionare le dimensioni della chiave di criptaggio (56 bit, 128 bit, 192 bit o 256 bit).

  Valori disponibili: *AES56*, *AES128*, *AES192* e *AES256*.

Segmenti cloud

Nella scheda **Segmenti cloud** è possibile configurare una ricerca in base all'appartenenza di un dispositivo a segmenti cloud specifici:

- **Il dispositivo si trova in un segmento cloud**

  Se questa opzione è abilitata, è possibile fare clic sul pulsante **Sfoglia** per specificare il segmento in cui eseguire la ricerca.

  Se anche l'opzione **Includi gli oggetti figlio** è abilitata, la ricerca viene eseguita in tutti gli oggetti figlio del segmento specificato.

  I risultati di ricerca includono solo i dispositivi del segmento selezionato.

- **Dispositivo rilevato tramite l'API**

  Nell'elenco a discesa, è possibile selezionare se un dispositivo deve essere rilevato o meno dagli strumenti API:

  - **AWS**. Il dispositivo viene rilevato tramite l'API AWS, quindi si trova senz'altro nell'ambiente cloud AWS.
  - **Azure**. Il dispositivo viene rilevato tramite l'API Azure, quindi si trova senz'altro nell'ambiente cloud Azure.
  - **Google Cloud.** Il dispositivo viene rilevato tramite l'API Google, quindi si trova senz'altro nell'ambiente cloud Google.
  - **No**. Il dispositivo non può essere rilevato tramite l'API AWS, Azure o Google, ad esempio perché si trova all'esterno dell'ambiente cloud oppure si trova nell'ambiente cloud ma non può essere rilevato tramite un'API.
  - **Nessun valore**. Questa condizione non viene applicata.

Componenti dell'applicazione

Questa sezione contiene un elenco dei componenti delle applicazioni per cui sono installati plug-in di gestione corrispondenti in Administration Console.

Nella sezione **Componenti dell'applicazione** è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base agli stati e ai numeri di versione dei componenti che fanno riferimento all'applicazione selezionata:

- **Stato**

  Ricerca dei dispositivi in base allo stato dei componenti inviato da un'applicazione all'Administration Server. È possibile selezionare uno dei seguenti stati: *Nessun dato dal dispositivo*, *Arrestato*, *Avvio in corso*, *Sospeso*, *In esecuzione*, *Malfunzionamento* o *Non installato*. Se il componente selezionato dell'applicazione installata in un dispositivo gestito presenta lo stato specificato, il dispositivo viene incluso nella selezione dispositivi.

  Stati inviati dalle applicazioni:

  - *Avvio in corso* - Il componente è attualmente in fase di inizializzazione.
  - *In esecuzione* - Il componente è abilitato e correttamente in esecuzione.
  - *Sospeso* - Il componente è sospeso, ad esempio dopo che l'utente ha sospeso la protezione nell'applicazione gestita.
  - *Malfunzionamento* - Si è verificato un errore durante l'esecuzione del componente.
  - *Arrestato* - Il componente è disabilitato e al momento non è in esecuzione.
  - *Non installato* - L'utente non ha selezionato il componente per l'installazione durante la configurazione dell'installazione personalizzata dell'applicazione.

  A differenza degli altri stati, lo stato *Nessun dato dal dispositivo* non viene inviato dalle applicazioni. Questa opzione indica che le applicazioni non dispongono di alcuna informazione sullo stato del componente selezionato. Ciò può ad esempio verificarsi quando il componente selezionato non appartiene ad alcuna delle applicazioni installate nel dispositivo o quando il dispositivo è spento.

- **Versione**

  Ricerca dei dispositivi in base al numero di versione del componente selezionato nell'elenco. È possibile digitare un numero di versione, ad esempio `3.4.1.0`, e quindi specificare se il componente selezionato deve avere una versione uguale, precedente o successiva. È anche possibile configurare la ricerca di tutte le versioni ad eccezione di quella specificata.

Utilizzo di maschere nelle variabili stringa

L'utilizzo di maschere per le variabili stringa è consentito. Per creazione delle maschere, è possibile utilizzare le seguenti espressioni regolari:

- Carattere jolly (*) – Qualsiasi stringa di 0 o più caratteri.
- Punto interrogativo (?)– Qualsiasi carattere singolo.
- [<intervallo>]– Qualsiasi carattere singolo da un intervallo o un set specificato.
  Ad esempio: [0–9] – qualsiasi cifra; [abcdef] – uno dei caratteri a, b, c, d, e, f.

Utilizzo di espressioni regolari nel campo di ricerca

È possibile utilizzare le seguenti espressioni regolari nel campo di ricerca per cercare parole e caratteri specifici:

- *. Sostituisce qualsiasi sequenza di caratteri. Per cercare parole come Server, Servers o Server room, immettere l'espressione `Server*` nel campo di ricerca.
- ?. Sostituisce qualsiasi carattere singolo. Per cercare parole come Parte o Porte, immettere l'espressione `P?rte` nel campo di ricerca.

  > Il testo nel campo di ricerca non può iniziare con un punto interrogativo (?).

- [<intervallo>]. Sostituisce qualsiasi carattere singolo da un intervallo o un set specificato. Per cercare qualsiasi numero, immettere l'espressione `[0-9]` nel campo di ricerca. Per cercare uno dei caratteri (a, b, c, d, e o f), immettere l'espressione `[abcdef]` nel campo di ricerca.

Utilizzare le seguenti espressioni regolari nel campo di ricerca per eseguire una ricerca full-text:

- Spazio. Come risultato verranno restituiti tutti i dispositivi le cui descrizioni contengono una delle parole elencate. Ad esempio, per cercare una frase che contiene parole come "Secondario" o "Virtuale" (o entrambe queste parole), immettere l'espressione `Secondario Virtuale` nel campo di ricerca.
- Segno più (+), AND o &&. Quando una parola è preceduta dal segno +, tutti i risultati della ricerca conterranno tale parola. Ad esempio, per cercare una frase che contiene sia la parola "Secondario" che la parola "Virtuale", è possibile immettere una delle seguenti espressioni nel campo di ricerca: `+Secondario+Virtuale`, `Secondario AND Virtuale`, `Secondario && Virtuale`.
- OR o ||. Quando viene inserito tra due parole, indica che una delle due parole può essere trovata nel testo. Per cercare una frase che contiene la parola "Secondario" o la parola "Virtuale", è possibile immettere una delle seguenti espressioni nel campo di ricerca: `Secondario OR Virtuale`, `Secondario || Virtuale`.
- Segno meno (-). Quando una parola è preceduta dal segno -, nessun risultato della ricerca conterrà tale parola. Per cercare una frase che deve contenere parole come Secondario e non deve contenere parole come Virtuale, è necessario immettere l'espressione `+Secondario-Virtuale` nel campo di ricerca.
- `"< testo >"`. Verranno visualizzati i risultati che contengono il testo racchiuso tra virgolette. Per cercare una frase che contiene la combinazione di parole Server secondario, immettere l'espressione `" Server secondario "` nel campo di ricerca.

La ricerca full-text è disponibile nelle seguenti sezioni di filtro:

- Nella sezione di filtro dell'elenco di eventi, in base alle colonne **Evento** e **Descrizione**.
- Nella sezione di filtro dell'account utente, in base alla colonna **Nome**.
- Nella sezione di filtro del registro delle applicazioni, in base alla colonna **Nome**, se nella sezione **Mostra nell'elenco** è selezionato **nessun raggruppamento** come criterio di filtro.

Esportazione di elenchi dalle finestre di dialogo

Nelle finestre di dialogo dell'applicazione è possibile esportare elenchi di oggetti in file di testo.

L'esportazione di un elenco di oggetti è possibile per le sezioni delle finestre di dialogo contenenti il pulsante **Esporta in un file**.

Impostazioni delle attività

In questa sezione sono elencate tutte le impostazioni delle attività in Kaspersky Security Center.

Impostazioni generali delle attività

Questa sezione contiene le impostazioni che è possibile configurare per la maggior parte delle attività. L'elenco delle impostazioni disponibili dipende dall'attività che si sta configurando.

Impostazioni specificate durante la creazione dell'attività

È possibile specificare le seguenti impostazioni durante la creazione di un'attività. Alcune di queste impostazioni possono anche essere modificate nelle proprietà dell'attività creata.

- Impostazioni per il riavvio del sistema operativo:
  - **Non riavviare il dispositivo**

    I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

  - **Riavvia il dispositivo**

    I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

  - **Richiedi l'intervento dell'utente**

    Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  - **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

- Impostazioni di pianificazione dell'attività:

  I tipi di pianificazione possono variare a seconda dell'attività.

  - **Impostazione Avvio pianificato:**

    - Ogni N ore

      L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

      Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

    - Ogni N giorni

      L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

      Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

    - Ogni N minuti

      L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

      Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

    - In base ai giorni della settimana

      L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

      Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

    - Mensile

L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Una sola volta**

  L'attività viene eseguita una volta, nella data e nell'ora specificate (per impostazione predefinita, il giorno in cui è stata creata l'attività).

- **Immediatamente**

  L'attività viene eseguita immediatamente dopo il salvataggio delle impostazioni.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- **Quando vengono scaricati nuovi aggiornamenti nell'archivio**

  L'attività viene eseguita dopo il download degli aggiornamenti nell'archivio. È ad esempio possibile utilizzare questa pianificazione per l'attività Trova vulnerabilità e aggiornamenti richiesti.

- **Durante un'epidemia di virus**

L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

- Anti-virus per workstation e file server
- Anti-virus per la difesa perimetrale
- Anti-virus per i sistemi di posta

Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

  L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

  È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

  Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

  - Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
  - Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

    Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
  - Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale per l'avvio delle attività con un intervallo di (min.)**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

- Dispositivi a cui assegnare l'attività:
  - Seleziona i dispositivi della rete rilevati da Administration Server

    L'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

    Questa opzione può ad esempio essere utilizzata in un'attività per l'installazione di Network Agent nei dispositivi non assegnati.

  - Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco

    È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

    Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

  - Assegna un'attività a una selezione dispositivi

    L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

    Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

  - Assegna un'attività a un gruppo di amministrazione

    L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

    Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

    Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

- Impostazioni per l'account:
  - Account predefinito

    L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

    Per impostazione predefinita, questa opzione è selezionata.

  - Specifica account

    Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

  - Account

Account tramite il quale viene eseguita l'attività.

- **Password**

  Password dell'account con cui verrà eseguita l'attività.

Se Network Agent non è installato nel dispositivo di destinazione, è necessario specificare l'account da utilizzare nel dispositivo di destinazione per accedere alla condivisione admin$. L'account specificato ha solo lo scopo di copiare i dati nel dispositivo. Se Network Agent è installato nel dispositivo di destinazione, i dati vengono copiati tramite Network Agent e non è necessario specificare alcun account durante la creazione dell'attività.

Impostazioni specificate dopo la creazione dell'attività

È possibile specificare le seguenti impostazioni solo dopo la creazione di un'attività.

- Impostazioni delle attività di gruppo:
  - **Distribuisci ai sottogruppi**

    Questa opzione è disponibile solo nelle impostazioni delle attività di gruppo.

    Quando questa opzione è abilitata, l'ambito dell'attività include:

    - Il gruppo di amministrazione selezionato durante la creazione dell'attività.
    - I gruppi di amministrazione subordinati al gruppo di amministrazione selezionato a qualsiasi livello inferiore nella gerarchia dei gruppi.

    Quando questa opzione è disabilitata, l'ambito dell'attività include solo il gruppo di amministrazione selezionato durante la creazione dell'attività.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Distribuisci negli Administration Server secondari e virtuali**

    Quando questa opzione è abilitata, l'attività valida nell'Administration Server primario viene applicata anche negli Administration Server secondari (compresi quelli virtuali). Se un'attività dello stesso tipo esiste già nell'Administration Server secondario, nell'Administration Server secondario vengono applicate entrambe le attività: quella esistente e quella ereditata dall'Administration Server primario.

    Questa opzione è disponibile solo quando l'opzione **Distribuisci ai sottogruppi** è abilitata.

    Per impostazione predefinita, questa opzione è disabilitata.

- Impostazioni di pianificazione avanzate:
  - **Accendi i dispositivi utilizzando la funzione Wake-on-LAN prima di avviare l'attività (min)**

    Il sistema operativo nel dispositivo verrà avviato in base al periodo di tempo specificato prima dell'avvio dell'attività pianificata. Il periodo di tempo predefinito è cinque minuti.

    Abilitare questa opzione se si desidera eseguire l'attività in tutti i dispositivi client nell'ambito dell'attività, inclusi quelli che sono spenti al momento dell'avvio dell'attività.

    Se si desidera che il dispositivo si spenga automaticamente al termine dell'attività, abilitare l'opzione **Spegni i dispositivi dopo il completamento dell'attività**. Questa opzione è disponibile nella stessa finestra.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Spegni i dispositivi dopo il completamento dell'attività**

    Questa opzione può ad esempio essere abilitata per un'attività di aggiornamento dell'installazione che installa gli aggiornamenti nei dispositivi client ogni venerdì dopo l'orario lavorativo e quindi spegne tali dispositivi per il fine settimana.

    Per impostazione predefinita, questa opzione è disabilitata.

- **Arresta se l'attività viene eseguita per più di (min)**

  Al termine del periodo di tempo specificato, l'attività viene arrestata automaticamente, che sia stata completata o meno.

  Abilitare questa opzione se si desidera interrompere (o arrestare) le attività che richiedono troppo tempo per l'esecuzione.

  Per impostazione predefinita, questa opzione è disabilitata. Il tempo predefinito per l'esecuzione dell'attività è 120 minuti.

- Impostazioni di notifica:
  - Blocco **Salva cronologia attività**:
    - Su Administration Server per (giorni)

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività in tutti i dispositivi client nell'ambito dell'attività vengono archiviati nell'Administration Server per il numero di giorni specificato. Al termine di questo periodo, le informazioni vengono eliminate da Administration Server.

      Per impostazione predefinita, questa opzione è abilitata.

    - Archivia nel registro eventi del sistema operativo del dispositivo

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività vengono archiviati in locale nel registro eventi di Windows di ogni dispositivo client.

      Per impostazione predefinita, questa opzione è disabilitata.

    - Archivia nel registro eventi del sistema operativo in Administration Server

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività in tutti i dispositivi client nell'ambito dell'attività vengono archiviati in modo centralizzato nel registro eventi di Windows del sistema operativo di Administration Server.

      Per impostazione predefinita, questa opzione è disabilitata.

    - Salva tutti gli eventi

      Se questa opzione è selezionata, nei registri eventi vengono salvati tutti gli eventi relativi all'attività.

    - Salva eventi correlati all'avanzamento dell'attività

      Se questa opzione è selezionata, nei registri eventi vengono salvati solo gli eventi relativi all'esecuzione dell'attività.

    - Salva solo i risultati dell'esecuzione dell'attività

      Se questa opzione è selezionata, nei registri eventi vengono salvati solo gli eventi relativi ai risultati dell'attività.

  - Notifica all'amministratore i risultati dell'esecuzione dell'attività

    È possibile selezionare i metodi con cui inviare agli amministratori le notifiche relative ai risultati dell'esecuzione dell'attività: tramite e-mail, SMS o un file eseguibile. Per configurare la notifica, fare clic sul collegamento **Impostazioni**.

    Per impostazione predefinita, tutti i metodi di notifica sono disabilitati.

  - Notifica solo errori

Se questa opzione è abilitata, agli amministratori viene inviata una notifica solo quando l'esecuzione di un'attività viene completata con un errore.

Se questa opzione è disabilitata, agli amministratori viene inviata una notifica dopo il completamento dell'esecuzione di ogni attività.

Per impostazione predefinita, questa opzione è abilitata.

- Impostazioni di protezione
- Impostazioni dell'ambito dell'attività

  A seconda del modo in cui viene determinato l'ambito dell'attività, sono disponibili le seguenti impostazioni:

  - **Dispositivi**

    Se l'ambito di un'attività è determinato in base a un gruppo di amministrazione, è possibile visualizzare tale gruppo. In questo caso, non è possibile apportare modifiche. Tuttavia, è possibile impostare l'opzione **Esclusioni dall'ambito dell'attività**.

    Se l'ambito di un'attività è determinato in base a un elenco di dispositivi, è possibile modificare l'elenco aggiungendo e rimuovendo dispositivi.

  - **Selezione dispositivi**

    È possibile modificare la selezione dispositivi a cui viene applicata l'attività.

  - **Esclusioni dall'ambito dell'attività**

    È possibile specificare gruppi di dispositivi a cui non deve essere applicata l'attività. I gruppi da escludere possono essere solo sottogruppi del gruppo di amministrazione a cui è applicata l'attività.

- **Cronologia revisioni**

Impostazioni dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server

Impostazioni specificate durante la creazione dell'attività

È possibile specificare le seguenti impostazioni durante la creazione di un'attività. Alcune di queste impostazioni possono anche essere modificate nelle proprietà dell'attività creata.

- **Sorgenti degli aggiornamenti**

  È possibile utilizzare le seguenti risorse come sorgenti degli aggiornamenti per l'Administration Server:

  - Server degli aggiornamenti Kaspersky

    I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni. Per impostazione predefinita, Administration Server comunica con i server di aggiornamento Kaspersky e scarica gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server per fare in modo che utilizzi il protocollo HTTP anziché HTTPS.

    Opzione selezionata per impostazione predefinita.

  - Administration Server primario

    Questa risorsa si applica alle attività create per un Administration Server secondario o virtuale.

  - Cartella locale o di rete

    Un'unità locale o una cartella di rete che contiene gli aggiornamenti più recenti. Una cartella di rete può essere un server FTP o HTTP oppure una condivisione SMB. Se una cartella di rete richiede l'autenticazione, è supportato solo il protocollo SMB. Quando si seleziona una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server.

    > Una cartella di rete o un server FTP o HTTP utilizzato da una sorgente degli aggiornamenti deve contenere una struttura di cartelle (con gli aggiornamenti) che corrisponde alla struttura creata durante l'utilizzo dei server di aggiornamento Kaspersky.

- **Altre impostazioni**

  Forza aggiornamento degli Administration Server secondari

  Se questa opzione è abilitata, Administration Server avvia le attività di aggiornamento negli Administration Server secondari non appena vengono scaricati nuovi aggiornamenti. Le attività di aggiornamento vengono avviate utilizzando la sorgente dell'aggiornamento configurata nelle proprietà dell'attività negli Administration Server secondari.

  Se questa opzione è disabilitata, le attività di aggiornamento negli Administration Server secondari vengono avviate in base alla relativa pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata.

  Copia gli aggiornamenti scaricati in cartelle aggiuntive

Dopo avere ricevuto gli aggiornamenti, l'Administration Server li copia nelle cartelle specificate. Utilizzare questa opzione se si desidera gestire manualmente la distribuzione degli aggiornamenti nella rete.

Questa opzione può ad esempio essere utilizzata nella seguente situazione: la rete dell'organizzazione è composta da diverse subnet indipendenti e i dispositivi in ciascuna subnet non hanno accesso ad altre subnet. I dispositivi in tutte le subnet hanno tuttavia accesso a una condivisione di rete comune. In questo caso, è possibile impostare Administration Server in una delle subnet per il download degli aggiornamenti dai server di aggiornamento Kaspersky, abilitare questa opzione e quindi specificare la condivisione di rete. Nelle attività di download degli aggiornamenti nell'archivio per gli altri Administration Server specificare la stessa condivisione di rete come sorgente degli aggiornamenti.

Se si seleziona di copiare gli aggiornamenti scaricati in una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server. Il percorso della cartella dipende dal sistema operativo del dispositivo. Poiché la cartella locale si trova in Administration Server basato su Linux, è necessario specificare il percorso POSIX, ad esempio /path/to/dir.

Quando si seleziona una cartella di rete che si trova in Administration Server basato su Linux, è necessario garantire preventivamente l'accesso alla cartella di rete dal dispositivo in cui è installato Administration Server montando la cartella. L'accesso alla cartella viene eseguito utilizzando il protocollo SMB.

Per impostazione predefinita, questa opzione è disabilitata.

Non forzare l'aggiornamento dei dispositivi e degli Administration Server secondari prima del completamento della copia

Le attività di download degli aggiornamenti nei dispositivi client e negli Administration Server secondari vengono avviate solo una volta che gli aggiornamenti sono stati copiati dalla cartella degli aggiornamenti principale nelle cartelle degli aggiornamenti aggiuntive.

Questa opzione deve essere abilitata se i dispositivi client e gli Administration Server secondari scaricano gli aggiornamenti da cartelle di rete aggiuntive.

Per impostazione predefinita, questa opzione è disabilitata.

Impostazioni specificate dopo la creazione dell'attività

È possibile specificare le seguenti impostazioni solo dopo la creazione di un'attività.

- Sezione **Impostazioni**, blocco **Contenuto degli aggiornamenti**

  Scarica file diff

  Questa opzione consente di abilitare la funzionalità di download dei file diff.

  Per impostazione predefinita, questa opzione è disabilitata.

- Sezione **Verifica aggiornamenti**

  Verifica gli aggiornamenti prima della distribuzione

  Administration Server esegue il download degli aggiornamenti dalla sorgente, li salva in un archivio temporaneo ed esegue l'attività definita nel campo **Attività di verifica degli aggiornamenti**. Se l'attività viene completata correttamente, gli aggiornamenti verranno copiati dall'archivio temporaneo in una cartella condivisa di Administration Server e saranno distribuiti in tutti gli altri dispositivi per cui Administration Server opera come sorgente degli aggiornamenti (verranno avviate le attività con il tipo di pianificazione **Quando vengono scaricati nuovi aggiornamenti nell'archivio**). L'attività di download degli aggiornamenti nell'archivio viene conclusa solo una volta completata l'attività *Verifica aggiornamenti*.

  Per impostazione predefinita, questa opzione è disabilitata.

  Attività di verifica degli aggiornamenti

  Questa attività verifica gli aggiornamenti scaricati prima che siano distribuiti ai tutti i dispositivi per cui l'Administration Server opera come sorgente degli aggiornamenti.

  In questo campo è possibile specificare l'attività *Verifica aggiornamenti* creata in precedenza. In alternativa, è possibile creare una nuova attività *Verifica aggiornamenti*.

Impostazioni dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

Impostazioni specificate durante la creazione dell'attività

È possibile specificare le seguenti impostazioni durante la creazione di un'attività. Alcune di queste impostazioni possono anche essere modificate nelle proprietà dell'attività creata.

- **Sorgenti degli aggiornamenti**

  È possibile utilizzare le seguenti risorse come sorgenti degli aggiornamenti per il punto di distribuzione:

  - Server degli aggiornamenti Kaspersky

    I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.

    Questa opzione è selezionata per impostazione predefinita.

  - Administration Server primario

    Questa risorsa si applica alle attività create per un Administration Server secondario o virtuale.

  - Cartella locale o di rete

    Un'unità locale o una cartella di rete che contiene gli aggiornamenti più recenti. Una cartella di rete può essere un server FTP o HTTP oppure una condivisione SMB. Se una cartella di rete richiede l'autenticazione, è supportato solo il protocollo SMB. Quando si seleziona una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server.

    Una cartella di rete o un server FTP o HTTP utilizzato da una sorgente degli aggiornamenti deve contenere una struttura di cartelle (con gli aggiornamenti) che corrisponde alla struttura creata durante l'utilizzo dei server di aggiornamento Kaspersky.

- **Altre impostazioni** → **Cartella per l'archiviazione degli aggiornamenti**

  Il percorso della cartella specificata per l'archiviazione degli aggiornamenti salvati. È possibile copiare il percorso della cartella specificata negli appunti. Non è possibile modificare il percorso di una cartella specificata per un'attività di gruppo.

Impostazioni specificate dopo la creazione dell'attività

È possibile specificare la seguente impostazione nella sezione **Impostazioni**, nel blocco **Contenuto degli aggiornamenti** solo dopo la creazione di un'attività.

Scarica file diff

Questa opzione consente di abilitare la funzionalità di download dei file diff.

Per impostazione predefinita, questa opzione è disabilitata.

Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

Impostazioni specificate durante la creazione dell'attività

È possibile specificare le seguenti impostazioni durante la creazione di un'attività. Alcune di queste impostazioni possono anche essere modificate nelle proprietà dell'attività creata.

- **Cerca vulnerabilità e aggiornamenti elencati da Microsoft**

  Durante la ricerca di vulnerabilità e aggiornamenti, Kaspersky Security Center utilizza le informazioni sugli aggiornamenti Microsoft applicabili della sorgente degli aggiornamenti di Microsoft e disponibili al momento.

  È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft e gli aggiornamenti delle applicazioni di terze parti.

  Per impostazione predefinita, questa opzione è abilitata.

  Le informazioni sugli aggiornamenti facoltativi di Microsoft Windows non vengono inviate ad Administration Server.

  - **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati**

Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft. I seguenti server possono operare come sorgente degli aggiornamenti Microsoft:

- Kaspersky Security Center Administration Server (vedere le impostazioni del criterio di Network Agent)
- Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione
- Server degli aggiornamenti Microsoft

Se questa opzione è abilitata, Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft per aggiornare le informazioni sugli aggiornamenti di Microsoft Windows applicabili.

Se questa opzione è disabilitata, l'Agente di Windows Update in un dispositivo gestito utilizza le informazioni sugli aggiornamenti di Microsoft Windows applicabili ricevuti dalla sorgente degli aggiornamenti Microsoft in precedenza.

La connessione alla sorgente degli aggiornamenti Microsoft può comportare un notevole utilizzo di risorse. Potrebbe essere necessario disabilitare questa opzione se è stata impostata una connessione standard a questa sorgente degli aggiornamenti in un'altra attività o nelle proprietà del criterio Network Agent, nella sezione **Vulnerabilità e aggiornamenti software**. Se non si desidera disabilitare questa opzione, per ridurre l'overload del Server è possibile configurare la pianificazione delle attività in modo da utilizzare il ritardo casuale per l'avvio delle attività entro 360 minuti.

Per impostazione predefinita, questa opzione è abilitata.

La combinazione delle seguenti opzioni delle impostazioni del criterio di Network Agent definisce il modo in cui si ottengono gli aggiornamenti:

- In un dispositivo gestito, l'Agente di Windows Update si connette al server degli aggiornamenti per ottenere gli aggiornamenti solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è abilitata nelle proprietà dell'attività *Trova vulnerabilità e aggiornamenti richiesti* e l'opzione **Modalità di ricerca di Windows Update** è impostata su **Attiva** nelle impostazioni del criterio di Network Agent.
- Se non è necessario che Network Agent avvii una connessione alla sorgente degli aggiornamenti di Microsoft Windows e scarichi gli aggiornamenti durante l'esecuzione dell'attività *Scansione vulnerabilità*, è possibile impostare l'opzione **Modalità di ricerca di Windows Update** su **Passiva**, mentre l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** deve rimanere abilitata. In questo modo, è possibile risparmiare risorse e utilizzare gli aggiornamenti di Windows ricevuti in precedenza per la scansione delle vulnerabilità. È possibile utilizzare la modalità passiva se si configura la ricezione degli aggiornamenti DI Microsoft Windows in modo diverso. Se la ricezione degli aggiornamenti di Microsoft Windows non è configurata in altro modo, non impostare l'opzione **Modalità di ricerca di Windows Update** su **Passiva**, poiché in questo caso non si riceveranno le informazioni sugli aggiornamenti, in alcun caso.
- Indipendentemente dallo stato dell'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** (abilitata o disabilitata), se l'opzione **Modalità di ricerca di Windows Update** è impostata su **Disabilitata**, Kaspersky Security Center non richiede informazioni sugli aggiornamenti.

- Cerca vulnerabilità e aggiornamenti di terze parti elencati da Kaspersky

Se questa opzione è abilitata, Kaspersky Security Center esegue la ricerca delle vulnerabilità e degli aggiornamenti richiesti per le applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) nel Registro di sistema di Windows e nelle cartelle specificate con **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**. L'elenco completo delle applicazioni di terze parti supportate è gestito da Kaspersky.

Se questa opzione è disabilitata, Kaspersky Security Center non esegue la ricerca di vulnerabilità e aggiornamenti richiesti per le applicazioni di terze parti. È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft Windows e gli aggiornamenti delle applicazioni di terze parti.

Per impostazione predefinita, questa opzione è abilitata.

- **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**

  Cartelle in cui Kaspersky Security Center esegue la ricerca delle applicazioni di terze parti che richiedono la correzione delle vulnerabilità e l'installazione di aggiornamenti. È possibile utilizzare le variabili di sistema.

  Specificare le cartelle in cui sono installate le applicazioni. Per impostazione predefinita, l'elenco contiene le cartelle di sistema in cui viene installata la maggior parte delle applicazioni.

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive i file di traccia anche se la scrittura dei file di traccia è disabilitata per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

Impostazioni dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità

Impostazioni specificate durante la creazione dell'attività

È possibile specificare le seguenti impostazioni durante la creazione di un'attività. Alcune di queste impostazioni possono anche essere modificate nelle proprietà dell'attività creata.

- **Specificare le regole per l'installazione degli aggiornamenti**

  Queste regole vengono applicate all'installazione degli aggiornamenti nei dispositivi client. Se non si specificano regole, l'attività non esegue alcuna operazione. Per informazioni sulle operazioni con le regole, vedere Regole per l'installazione dell'aggiornamento.

- **Avvia l'installazione al riavvio o all'arresto del dispositivo**

  Se questa opzione è abilitata, gli aggiornamenti vengono installati al riavvio o all'arresto del dispositivo. In caso contrario, gli aggiornamenti vengono installati in base a una pianificazione.

  Utilizzare questa opzione se l'installazione degli aggiornamenti può influire sulle prestazioni del dispositivo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Installa i componenti generali del sistema richiesti**

  Se questa opzione è abilitata, prima di installare un aggiornamento l'applicazione installa automaticamente tutti i componenti di sistema generali (prerequisiti) richiesti per installare l'aggiornamento. Questi prerequisiti possono ad esempio essere aggiornamenti del sistema operativo.

  Se questa opzione è disabilitata, può essere necessario installare manualmente i prerequisiti.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Consenti l'installazione di nuove versioni dell'applicazione durante gli aggiornamenti**

  Se questa opzione è abilitata, gli aggiornamenti sono consentiti se implicano l'installazione di una nuova versione di un'applicazione software.

  Se questa opzione è disabilitata, l'upgrade del software non viene eseguito. È quindi possibile installare le nuove versioni del software manualmente o tramite un'altra attività. È ad esempio possibile utilizzare questa opzione se l'infrastruttura aziendale non è supportata da una nuova versione del software o se si desidera verificare un aggiornamento in un'infrastruttura di test.

  Per impostazione predefinita, questa opzione è abilitata.

  L'upgrade dell'applicazione può causare un malfunzionamento delle applicazioni dipendenti installate nei dispositivi client.

- **Scarica gli aggiornamenti nel dispositivo senza installarli**

  Se questa opzione è abilitata, l'applicazione scarica gli aggiornamenti nel dispositivo client ma non li installa automaticamente. È quindi possibile installare manualmente gli aggiornamenti scaricati.

  Gli aggiornamenti Microsoft vengono scaricati nell'archiviazione di sistema di Windows. Gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) vengono scaricati nella cartella specificata nel campo **Scarica aggiornamenti in**.

  Se questa opzione è disabilitata, gli aggiornamenti vengono installati automaticamente nel dispositivo.

  Per impostazione predefinita, questa opzione è disabilitata.

  - **Scarica aggiornamenti in**

    Questa cartella viene utilizzata per scaricare gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft).

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive i file di traccia anche se la scrittura dei file di traccia è disabilitata per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

  - **Dimensione massima (in MB) dei file di diagnostica avanzata**

    Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

Impostazioni specificate dopo la creazione dell'attività

È possibile specificare le impostazioni nelle sezioni elencate di seguito solo dopo la creazione di un'attività. Per una descrizione completa delle impostazioni dell'attività, consultare Impostazioni generali dell'attività.

- **Generale**. In questa sezione vengono visualizzate le informazioni generali sull'attività. Inoltre, è possibile specificare a quali dispositivi applicare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*:

  - **Distribuisci ai sottogruppi**

    Questa opzione è disponibile solo nelle impostazioni delle attività di gruppo.

    Quando questa opzione è abilitata, l'ambito dell'attività include:

    - Il gruppo di amministrazione selezionato durante la creazione dell'attività.
    - I gruppi di amministrazione subordinati al gruppo di amministrazione selezionato a qualsiasi livello inferiore nella gerarchia dei gruppi.

    Quando questa opzione è disabilitata, l'ambito dell'attività include solo il gruppo di amministrazione selezionato durante la creazione dell'attività.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Distribuisci negli Administration Server secondari e virtuali**

    Quando questa opzione è abilitata, l'attività valida nell'Administration Server primario viene applicata anche negli Administration Server secondari (compresi quelli virtuali). Se un'attività dello stesso tipo esiste già nell'Administration Server secondario, nell'Administration Server secondario vengono applicate entrambe le attività: quella esistente e quella ereditata dall'Administration Server primario.

    Questa opzione è disponibile solo quando l'opzione **Distribuisci ai sottogruppi** è abilitata.

    Per impostazione predefinita, questa opzione è disabilitata.

- Aggiornamenti da installare

  Nella sezione **Aggiornamenti da installare** è possibile visualizzare l'elenco degli aggiornamenti installati dall'attività. Vengono visualizzati solo gli aggiornamenti che corrispondono alle impostazioni delle attività applicate.

- Testare l'installazione degli aggiornamenti:

  - **Non eseguire scansione**. Selezionare questa opzione se non si desidera eseguire un'installazione di test degli aggiornamenti.
  - **Esegui scansione nei dispositivi selezionati**. Selezionare questa opzione se si desidera testare l'installazione degli aggiornamenti nei dispositivi selezionati. Fare clic sul pulsante **Aggiungi** e selezionare i dispositivi in cui si desidera eseguire l'installazione di test degli aggiornamenti.
  - **Esegui scansione nei dispositivi del gruppo specificato**. Selezionare questa opzione se si desidera testare l'installazione degli aggiornamenti in un gruppo di dispositivi. Nel campo **Specificare un gruppo di test** specificare un gruppo di dispositivi in cui si desidera eseguire un'installazione di test.
  - **Esegui scansione nella percentuale di dispositivi specificata**. Selezionare questa opzione se si desidera testare l'installazione solo su una parte dei dispositivi di destinazione. Nel campo **Percentuale di dispositivi di test su tutti i dispositivi di destinazione** specificare la percentuale dei dispositivi in cui si desidera eseguire un'installazione di test degli aggiornamenti.

Elenco globale delle subnet

Questa sezione fornisce informazioni sull'elenco globale delle subnet che è possibile utilizzare nelle regole.

Per archiviare le informazioni sulle subnet nella rete, è possibile impostare un elenco globale delle subnet per ciascun Administration Server in uso. Questo elenco consente di associare coppie {indirizzo IP, maschera} e unità fisiche, come ad esempio le filiali. È possibile utilizzare le subnet in questo elenco nelle regole e nelle impostazioni di rete.

Aggiunta di subnet all'elenco globale delle subnet

È possibile aggiungere subnet con le relative descrizioni all'elenco globale delle subnet.

Per aggiungere una subnet all'elenco globale delle subnet:

1. Nella struttura della console selezionare il nodo dell'Administration Server desiderato.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra **Proprietà** visualizzata, nel riquadro **Sezioni**, selezionare **Elenco delle subnet globali**.
4. Fare clic sul pulsante **Aggiungi**.
   Verrà aperta la finestra **Nuova subnet**.

5. Compilare i seguenti campi:

- **Impostazioni generali**

  Indirizzo IP subnet per la subnet da aggiungere.

- **Subnet mask**

  Subnet mask per la subnet da aggiungere.

- **Nome**

  Nome della subnet. Deve essere univoco nell'elenco globale delle subnet. Se si aggiunge un nome già presente nell'elenco, verrà aggiunto un indice, ad esempio: ~~1, ~~2.

- **Descrizione**

  La descrizione può contenere informazioni aggiuntive sulla filiale a cui appartiene la subnet. Il testo verrà visualizzato in tutti gli elenchi in cui è presente la subnet, ad esempio nell'elenco delle regole di limitazione del traffico.

  Questo campo non è obbligatorio e può essere lasciato vuoto.

6. Fare clic su **OK**.

La subnet verrà visualizzata nell'elenco delle subnet.

Visualizzazione e modifica delle proprietà delle subnet nell'elenco globale delle subnet

È possibile visualizzare e modificare le proprietà delle subnet nell'elenco globale delle subnet.

Per visualizzare o modificare le proprietà di una subnet nell'elenco globale delle subnet:

1. Nella struttura della console selezionare il nodo dell'Administration Server desiderato.
2. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
3. Nella finestra **Proprietà** visualizzata, nel riquadro sinistro **Sezioni**, selezionare **Elenco delle subnet globali**.
4. Selezionare nell'elenco la subnet da modificare.
5. Fare clic sul pulsante **Proprietà**.

   Verrà aperta la finestra **Nuova subnet**.
6. Se necessario, modificare le impostazioni della subnet.
7. Fare clic su **OK**.

Se sono state apportate modifiche, queste verranno memorizzate.

Utilizzo di Network Agent per Windows, Linux e macOS a confronto

L'utilizzo di Network Agent varia in base al sistema operativo del dispositivo. Anche le impostazioni del criterio e del pacchetto di installazione di Network Agent variano a seconda del sistema operativo. La tabella seguente mette a confronto le funzionalità di Network Agent e gli scenari di utilizzo disponibili per i sistemi operativi Windows, macOS e Linux.

Confronto fra le funzionalità di Network Agent

Funzionalità di Network Agent	Windows	Linux	macOS
Installazione			
Generazione automatica del pacchetto di installazione di Network Agent dopo l'installazione di Kaspersky Security Center	✓	–	–
Installazione in modalità forzata, utilizzando speciali opzioni nell'attività di installazione remota di Kaspersky Security Center	✓	✓	✓
Installazione tramite l'invio agli utenti dei dispositivi di collegamenti ai pacchetti indipendenti generati da Kaspersky Security Center	✓	✓	✓
Installazione tramite la clonazione di un'immagine del disco rigido dell'amministratore con il sistema operativo e Network Agent, utilizzando gli strumenti forniti da Kaspersky Security Center per la gestione delle immagini disco	✓	–	–
Installazione tramite la clonazione di un'immagine del disco rigido dell'amministratore con il sistema operativo e Network Agent tramite strumenti di terzi	✓	✓	✓
Installazione con strumenti di terzi per l'installazione remota delle applicazioni	✓	✓	✓
Installazione manuale, eseguendo i programmi di installazione delle applicazioni nei dispositivi	✓	✓	✓
Installazione di Network Agent in modalità automatica	✓	✓	✓
Connessione manuale di un dispositivo client ad Administration Server. Utilità Klmover	✓	✓	✓
Installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center	✓	✓	–
Distribuzione automatica di una chiave	✓	✓	✓
Sincronizzazione forzata	✓	✓	✓
Punto di distribuzione			

Funzionalità di Network Agent	Windows	Linux	macOS
Utilizzo come punto di distribuzione	✓	✓	✓
Assegnazione automatica dei punti di distribuzione	✓	✓ Senza utilizzare Network Location Awareness (NLA).	✓ Senza utilizzare Network Location Awareness (NLA).
Polling della rete	✓ • Polling della rete Windows • Polling intervallo IP • Polling del controller di dominio (Microsoft Active Directory)	✓ • Polling intervallo IP • Polling zeroconf • Polling del controller di dominio (Microsoft Active Directory, Samba 4 Active Directory)	—
Esecuzione del servizio proxy KSN da parte di un punto di distribuzione	✓	✓	—
Download degli aggiornamenti tramite i server degli aggiornamenti Kaspersky negli archivi dei punti di distribuzione che distribuiscono gli aggiornamenti ai dispositivi gestiti	✓	✓	— (Se uno o più dispositivi che eseguono Linux o macOS rientrano nell'ambito dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione, l'attività viene completata con lo stato Non riuscito, anche se è stata completata correttamente in tutti i dispositivi Windows.)
Installazione push delle applicazioni	✓	Limitata: non è possibile eseguire l'installazione push su dispositivi Linux utilizzando i punti di distribuzione macOS.	Limitata: non è possibile eseguire l'installazione push su dispositivi Windows utilizzando i punti di distribuzione macOS.
Utilizzo come server push	✓	✓	—
Gestione delle applicazioni di terzi			
Installazione remota delle applicazioni nei dispositivi	✓	—	✓ Per i dettagli, fare riferimento al seguente articolo: Installazione remota delle applicazioni nei dispositivi macOS.
Aggiornamenti software	✓	—	—
Configurazione degli aggiornamenti del sistema operativo in un criterio di Network Agent	✓	—	—
Visualizzazione delle informazioni sulle vulnerabilità del software	✓	—	—
Scansione delle applicazioni per rilevare la presenza di vulnerabilità	✓	—	—
Inventario del software installato nei dispositivi	✓	✓	—
Macchine virtuali			
Installazione di Network Agent in una macchina virtuale	✓	✓	✓
Ottimizzazione delle impostazioni per VDI (Virtual Desktop Infrastructure)	✓	✓	✓
Supporto delle macchine virtuali dinamiche	✓	✓	✓
Altro			

Funzionalità di Network Agent	Windows	Linux	macOS
Azioni di controllo in un dispositivo client remoto utilizzando Condivisione desktop Windows	✓	—	—
Monitoraggio dello stato della protezione anti-virus	✓	✓	✓
Gestione dei riavvii dei dispositivi	✓	—	—
Supporto del rollback del file system	✓	✓	✓
Utilizzo di un Network Agent come gateway di connessione	✓	✓	✓
Gestione connessioni	✓	✓	✓
Passaggio di Network Agent da un Administration Server all'altro (automaticamente in base alla posizione di rete)	✓	—	✓
Verifica della connessione tra un dispositivo client e Administration Server. utilità klnagchk	✓	✓	✓
Connessione remota al desktop di un dispositivo client	✓	—	✓ Utilizzando il sistema VNC (Virtual Network Computing).
Download di un pacchetto di installazione indipendente tramite la Migrazione guidata	✓	✓	✓
Polling zeroconf	—	✓	—
Visualizzazione delle informazioni sull'hardware dei dispositivi client	✓	✓ Le informazioni sull'hardware dei dispositivi Linux inviate ad Administration Server da Network Agent installato in questi dispositivi sono limitate alle informazioni specificate nella descrizione delle impostazioni del dispositivo gestito per Administration Console e Kaspersky Security Center Web Console.	✓ Le informazioni sull'hardware dei dispositivi macOS inviate ad Administration Server da Network Agent installato in questi dispositivi sono limitate alle informazioni specificate nella descrizione delle impostazioni del dispositivo gestito per Administration Console e Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console

Kaspersky Security Center Web Console (di seguito denominata anche Kaspersky Security Center Web Console) è un'applicazione Web progettata per gestire lo stato del sistema di protezione della rete protetta dalle applicazioni Kaspersky.

Utilizzando l'applicazione è possibile eseguire le seguenti operazioni:

- Gestire lo stato del sistema di protezione dell'organizzazione.
- Installare le applicazioni Kaspersky nei dispositivi della rete e gestire le applicazioni installate.
- Gestire i criteri creati per i dispositivi della rete.
- Gestire account utente.
- Gestire le attività per le applicazioni installate nei dispositivi della rete.
- Visualizzare i rapporti sullo stato del sistema di protezione.
- Gestire l'invio dei rapporti ad amministratori di sistema e altri esperti IT.

Per informazioni sui requisiti hardware e software, fare riferimento a Requisiti di Web Console.

Kaspersky Security Center Web Console fornisce un'interfaccia Web che assicura l'interazione tra il dispositivo e Administration Server tramite un browser. Administration Server è un'applicazione progettata per la gestione delle applicazioni Kaspersky installate nei dispositivi della rete. Administration Server si connette ai dispositivi della rete attraverso canali protetti con SSL (Secure Sockets Layer). Quando si esegue la connessione a Kaspersky Security Center Web Console utilizzando il browser, questo stabilisce una connessione con Kaspersky Security Center Web Console Server.

I prerequisiti per utilizzare Kaspersky Security Center Web Console sono:

1. Utilizzare un browser per connettersi a Kaspersky Security Center Web Console in cui venga visualizzata l'interfaccia del portale Web.
2. Utilizzare i controlli del portale Web per scegliere il comando da eseguire. Kaspersky Security Center Web Console esegue le seguenti operazioni:
    - Se si seleziona un comando per la ricezione di informazioni (ad esempio, per visualizzare un elenco di dispositivi), Kaspersky Security Center Web Console genera una richiesta di informazioni ad Administration Server, riceve i dati necessari e li invia al browser in un formato semplice da visualizzare.
    - Se è stato scelto un comando di gestione (ad esempio, l'installazione remota di un'applicazione), Kaspersky Security Center Web Console riceve il comando dal browser e lo invia ad Administration Server. L'applicazione riceve il risultato da Administration Server e lo invia al browser in un formato semplice da visualizzare.

Kaspersky Security Center Web Console è un'applicazione multilingue. È possibile modificare la lingua dell'interfaccia in qualsiasi momento, senza riaprire l'applicazione. Quando si installa Kaspersky Security Center Web Console insieme a Kaspersky Security Center, Kaspersky Security Center Web Console ha la stessa lingua di interfaccia del file di installazione. Quando si installa solo Kaspersky Security Center Web Console, l'applicazione ha la stessa lingua di interfaccia del sistema operativo. Se Kaspersky Security Center Web Console non supporta la lingua del file di installazione o del sistema operativo, viene utilizzato l'inglese per impostazione predefinita.

Mobile Device Management non è supportato in Kaspersky Security Center Web Console. Se tuttavia sono stati aggiunti dispositivi mobili a un gruppo di amministrazione tramite Microsoft Management Console, questi dispositivi vengono visualizzati anche in Kaspersky Security Center Web Console.

Diagramma di distribuzione di Kaspersky Security Center Administration Server e Kaspersky Security Center Web Console

La figura seguente mostra il diagramma di distribuzione di Kaspersky Security Center Administration Server e Kaspersky Security Center Web Console.

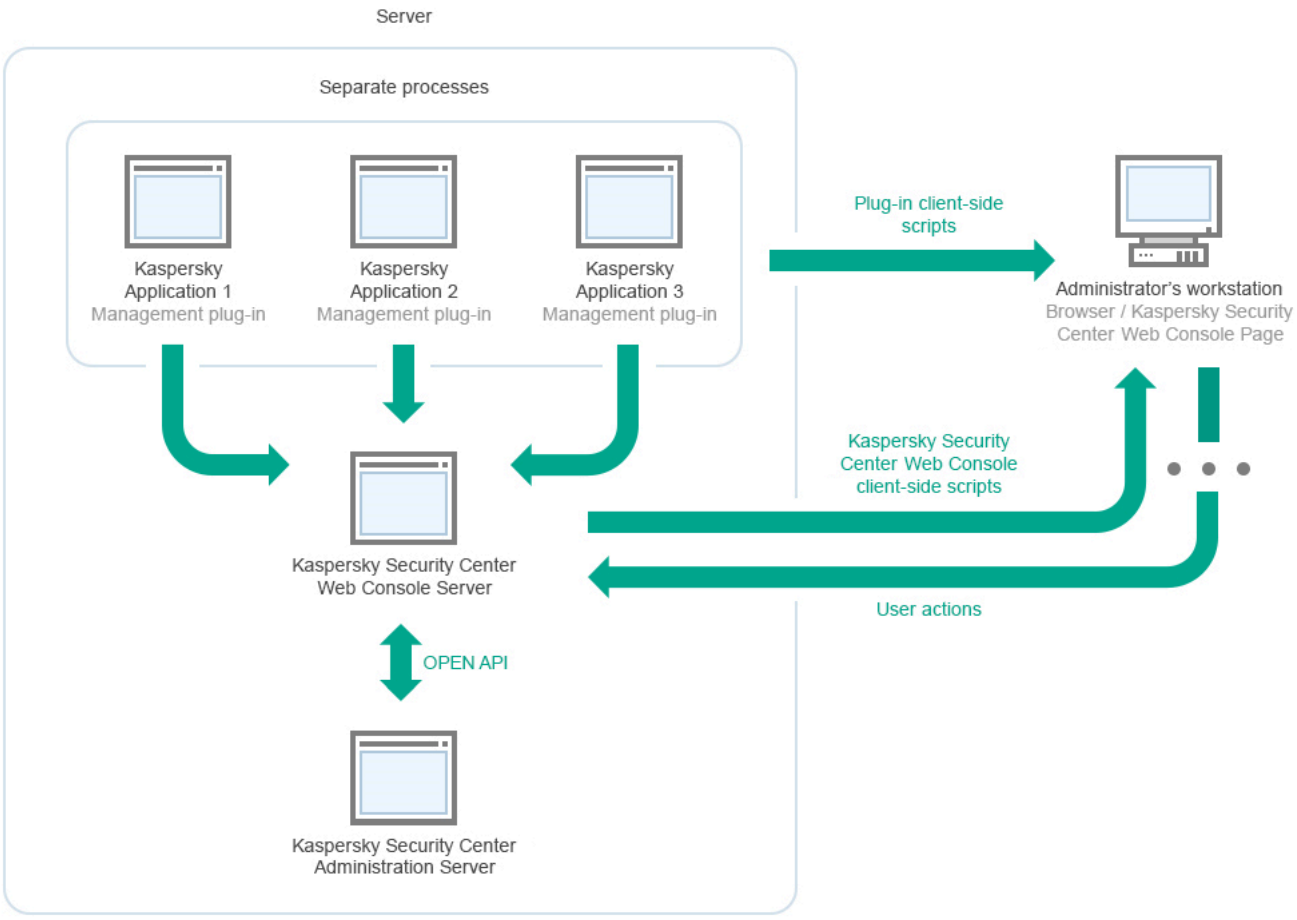


Diagramma di distribuzione di Kaspersky Security Center Administration Server e Kaspersky Security Center Web Console

I plug-in di gestione per le applicazioni Kaspersky installate nei dispositivi protetti (un plug-in per ogni applicazione) vengono distribuiti insieme a Kaspersky Security Center Web Console Server.

Come amministratore, accedere a Kaspersky Security Center Web Console utilizzando un browser sulla workstation.

Quando si eseguono azioni specifiche in Kaspersky Security Center Web Console, Kaspersky Security Center Web Console Server comunica con Kaspersky Security Center Administration Server tramite OpenAPI. Kaspersky Security Center Web Console Server richiede le informazioni necessarie a Kaspersky Security Center Administration Server e visualizza i risultati delle operazioni in Kaspersky Security Center Web Console.

Porte utilizzate da Kaspersky Security Center Web Console

La tabella seguente elenca le porte che devono essere aperte nel dispositivo in cui è installato Kaspersky Security Center Web Console Server (noto anche come Kaspersky Security Center Web Console).

Porte utilizzate da Kaspersky Security Center Web Console

Numero di porta	Nome servizio	Protocollo	Ambito della porta	Ambito
2001	Kaspersky Security Center Product Plugins Server	HTTPS	Porta API utilizzata dai processi del plug-in di gestione per ricevere richieste da "Kaspersky Security Center Web Console Management Service"	Esecuzione dei processi node.exe dei plug-in di gestione
1329, 2003	Kaspersky Security Center Web Console Management Service	HTTPS	Porte API utilizzate per ricevere richieste da "Kaspersky Security Center Web Console Management Service" in esecuzione nello stesso dispositivo	Aggiornamento dei componenti di Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	Porta API utilizzata per ricevere richieste da "Kaspersky Security Center Web Console Management Service" in esecuzione nello stesso dispositivo	Esecuzione dei processi node.exe di Kaspersky Security Center Web Console
3333	Kaspersky OSMP KAS Service	HTTPS	Porta dell'endpoint di autorizzazione OAuth2.0	Identity and Access Manager
4004	Kaspersky OSMP Facade Service	HTTPS	Porta del provider di identità OAuth2.0	Identity and Access Manager
4444	Kaspersky OSMP KAS Service	HTTPS	Porta dell'endpoint di introspezione del token OAuth2.0	Identity and Access Manager
8200	—	HTTP	Porta API utilizzata per generare certificati tramite HashiCorp Vault (per maggiori dettagli, consultare il sito Web di HashiCorp Vault)	Installazione di Kaspersky Security Center Web Console e aggiornamento dei componenti di Kaspersky Security Center Web Console
4150, 4151, 4152	Kaspersky Security Center Web Console Message Queue	HTTPS	Porte API del broker di messaggi utilizzate per la comunicazione tra i processi di Kaspersky Security Center Web Console e dei plug-in di gestione	Interazione tra Kaspersky Security Center Web Console e plug-in di gestione

La tabella di seguito elenca le porte che non devono essere aperte nel dispositivo in cui è installato Kaspersky Security Center Web Console Server. Tuttavia, Kaspersky Security Center Web Console utilizza queste porte per Identity and Access Manager.

Porte utilizzate da Kaspersky Security Center Web Console per Identity and Access Manager

Numero di porta	Nome servizio	Protocollo	Ambito della porta	Ambito
4445	Kaspersky OSMP KAS Service	HTTPS	Porta principale di Identity and Access Manager che riceve la configurazione da Kaspersky Security Center Web Console per la porta dell'endpoint di autorizzazione OAuth 2.0 (per ulteriori informazioni su OAuth 2.0, vedere il sito Web OAuth)	Identity and Access Manager
2444	Kaspersky OSMP Facade Service	HTTPS	Porta per la configurazione di Identity and Access Manager	Identity and Access Manager
2445	Kaspersky OSMP Facade Service	HTTPS	Porta per la connessione di "Kaspersky OSMP KAS Service" to "Kaspersky OSMP Facade Service"	Identity and Access Manager

Interfaccia di Kaspersky Security Center Web Console

Kaspersky Security Center è gestito tramite l'interfaccia di Kaspersky Security Center Web Console.

La finestra Kaspersky Security Center Web Console contiene i seguenti elementi:

- Menu principale nella parte sinistra della finestra
- Area di lavoro nella parte destra della finestra

Menu principale

Il menu principale contiene le seguenti sezioni:

- **Administration Server**. Mostra il nome dell'Administration Server a cui si è attualmente connessi. Fare clic sull'icona delle impostazioni ( ) per aprire le proprietà di Administration Server.
- **Monitoraggio e generazione dei rapporti**. Offre una panoramica dell'infrastruttura, degli stati di protezione e delle statistiche.
- **Risorse (dispositivi)**. Contiene strumenti per le risorse, nonché attività e criteri dell'applicazione Kaspersky.
- **Utenti e ruoli**. Consente di gestire utenti e ruoli, configurare i diritti degli utenti assegnando ruoli agli utenti e associare i profili dei criteri ai ruoli.
- **Operazioni**. Contiene una serie di operazioni, tra cui la gestione delle licenze delle applicazioni, la visualizzazione e la gestione di unità criptate ed eventi di criptaggio e la gestione di applicazioni di terze parti. Fornisce anche accesso agli archivi delle applicazioni.
- **Individuazione e distribuzione**. Consente di eseguire il polling della rete per rilevare i dispositivi client e distribuire i dispositivi ai gruppi di amministrazione manualmente o automaticamente. Questa sezione contiene anche l'Avvio rapido guidato e la Distribuzione guidata della protezione.
- **Marketplace**. Contiene informazioni sull'intera gamma di soluzioni aziendali Kaspersky e consente di selezionare quelle necessarie, nonché di procedere all'acquisto di tali soluzioni sul sito Web di Kaspersky.
- **Impostazioni**. Consente di eseguire il backup dello stato corrente di un plug-in Web per poter ripristinare lo stato salvato in un secondo momento. Contiene anche le impostazioni personali relative all'aspetto dell'interfaccia, ad esempio la lingua o il tema dell'interfaccia.
- **Menu dell'account personale**. Contiene un collegamento alla Guida di Kaspersky Security Center. Consente inoltre di disconnettersi da Kaspersky Security Center e di visualizzare la versione di Kaspersky Security Center Web Console e l'elenco dei plug-in Web di gestione installati.

Area di lavoro

L'area di lavoro mostra le informazioni che si sceglie di visualizzare nelle sezioni della finestra dell'interfaccia Web di Kaspersky Security Center Web Console. Contiene inoltre elementi di controllo che è possibile utilizzare per configurare la modalità di visualizzazione delle informazioni.

Blocco e sblocco delle sezioni del menu principale

È possibile bloccare sezioni di Kaspersky Security Center Web Console per aggiungerle ai preferiti e accedervi rapidamente dalla sezione **Bloccato** nel menu principale.

Se non sono presenti elementi bloccati, la sezione **Bloccato** non viene visualizzata nel menu principale.

È possibile bloccare le sezioni che mostrano solo pagine. Ad esempio, se si accede a **Risorse (dispositivi)** → **Dispositivi gestiti**, si apre una pagina con la tabella dei dispositivi, che consente di aggiungere la sezione **Dispositivi gestiti**. Se una finestra o nessun elemento viene visualizzato dopo aver selezionato la sezione nel menu principale, non è possibile bloccare tale sezione.

Per bloccare una sezione:

1. Nel menu principale, passare il cursore del mouse sulla sezione che si desidera bloccare.

   Viene visualizzata l'icona del blocco (📌).

2. Fare clic sull'icona del blocco (📌).

   La sezione viene bloccata e visualizzata nella sezione **Bloccato**.

È inoltre possibile rimuovere elementi dai preferiti sbloccandoli.

Per sbloccare una sezione:

1. Nel menu principale, accedere alla sezione **Bloccato**.
2. Passare il cursore del mouse sulla sezione che si desidera sbloccare, quindi fare clic sull'icona di sblocco (📌).

   La sezione viene rimossa dai preferiti.

Scenario: Installazione e configurazione iniziale di Kaspersky Security Center Web Console

Questo scenario descrive come installare Kaspersky Security Center Administration Server e Kaspersky Security Center Web Console, eseguire la configurazione iniziale di Administration Server tramite l'Avvio rapido guidato e installare le applicazioni Kaspersky nei dispositivi gestiti utilizzando la Distribuzione guidata della protezione.

L'installazione e la configurazione iniziale di Kaspersky Security Center Web Console prevedono diversi passaggi:

1. **Installazione di un sistema di gestione database (DBMS)**

   Installare il DBMS che verrà utilizzato da Kaspersky Security Center o utilizzarne uno esistente.

   Per informazioni su come installare il DBMS selezionato, consultare la relativa documentazione.

2. **Installazione di Administration Server, Administration Console e Network Agent**

Administration Console e la versione del server di Network Agent vengono installate insieme ad Administration Server.

Durante l'installazione di Kaspersky Security Center Administration Server, specificare se si desidera installare Kaspersky Security Center Web Console nello stesso dispositivo. Se si sceglie di installare entrambi i componenti nello stesso dispositivo, non è necessario installare separatamente Kaspersky Security Center Web Console, poiché viene installato automaticamente. Se si desidera installare Kaspersky Security Center Web Console in un dispositivo diverso, dopo l'installazione di Kaspersky Security Center Administration Server, procedere con l'installazione di Kaspersky Security Center Web Console.

3. **Installazione di Kaspersky Security Center Web Console**

   Se non si è scelto di installare Kaspersky Security Center Web Console insieme a Kaspersky Security Center Administration Server nel passaggio precedente, installare Kaspersky Security Center Web Console separatamente. È possibile installare Kaspersky Security Center Web Console in un dispositivo diverso o nello stesso dispositivo in cui è installato Administration Server.

4. **Esecuzione della configurazione iniziale**

   Quando l'installazione di Administration Server è completa, alla prima connessione ad Administration Server viene avviato automaticamente l'Avvio rapido guidato. Eseguire la configurazione iniziale di Administration Server in base ai requisiti esistenti. Durante la fase di configurazione iniziale, la procedura guidata utilizza le impostazioni predefinite per creare i criteri e le attività necessari per la distribuzione della protezione. Le impostazioni predefinite potrebbero tuttavia non essere ottimali per le esigenze dell'organizzazione. Se necessario, è possibile modificare le impostazioni dei criteri e delle attività.

5. **Licenza di Kaspersky Security Center (facoltativo)**

   Kaspersky Security Center con il supporto delle funzionalità di base di Administration Console non richiede una licenza. È necessaria una licenza commerciale se si desidera utilizzare una o più funzionalità aggiuntive, tra cui Vulnerability e patch management, Mobile Device Management e Integrazione con i sistemi SIEM. È possibile aggiungere un file chiave o un codice di attivazione per queste funzionalità nel passaggio corrispondente dell'Avvio rapido guidato o manualmente.

6. **Individuazione dei dispositivi nella rete**

   Questo passaggio viene gestito dall'Avvio rapido guidato. È inoltre possibile individuare i dispositivi manualmente. Kaspersky Security Center riceve gli indirizzi e i nomi di tutti i dispositivi rilevati nella rete. È quindi possibile utilizzare Kaspersky Security Center per installare le applicazioni Kaspersky e software di altri produttori nei dispositivi rilevati. Kaspersky Security Center avvia periodicamente la device discovery, pertanto eventuali nuove istanze che compaiono nella rete verranno rilevate automaticamente.

7. **Organizzazione dei dispositivi in gruppi di amministrazione**

   Questo passaggio viene gestito dall'Avvio rapido guidato, ma è anche possibile spostare manualmente i dispositivi rilevati nei gruppi.

8. **Installazione di Network Agent e di applicazioni di protezione nei dispositivi in rete**

   La distribuzione della protezione in una rete aziendale implica l'installazione di Network Agent e delle applicazioni di protezione (ad esempio, Kaspersky Endpoint Security for Windows) nei dispositivi rilevati da Administration Server durante la device discovery.

   Per installare le applicazioni in remoto, eseguire la Distribuzione guidata della protezione.

   Le applicazioni di protezione proteggono i dispositivi da virus e da altri programmi che costituiscono una minaccia. Network Agent garantisce la comunicazione tra il dispositivo e Administration Server. Le impostazioni di Network Agent vengono configurate automaticamente per impostazione predefinita.

   Prima di iniziare a installare Network Agent e le applicazioni di protezione nei dispositivi nella rete, verificare che questi dispositivi siano accessibili (attivati).

9. **Distribuzione delle chiavi di licenza ai dispositivi client**

Distribuire le chiavi di licenza ai dispositivi client per attivare applicazioni di protezione gestite in tali dispositivi.

10. **Installazione di Kaspersky Security for Mobile (opzionale)**

    Se si intende gestire i dispositivi mobili aziendali, seguire le istruzioni fornite nella Guida di Kaspersky Security for Mobile per informazioni sulla distribuzione di Kaspersky Endpoint Security for Android.

11. **Configurazione dei criteri delle applicazioni Kaspersky**

    Per applicare differenti impostazioni dell'applicazione ai diversi dispositivi, è possibile utilizzare la gestione della protezione incentrata sui dispositivi e/o la gestione della protezione incentrata sugli utenti. La gestione della protezione incentrata sui dispositivi può essere implementata utilizzando criteri e attività. È possibile applicare le attività solo ai dispositivi che soddisfano condizioni specifiche. Per impostare le condizioni per il filtro dei dispositivi, utilizzare le selezioni dispositivi e i tag.

12. **Monitoraggio dello stato della protezione della rete**

    È possibile monitorare la rete utilizzando i widget nel dashboard, generare rapporti dalle applicazioni Kaspersky, configurare e visualizzare selezioni degli eventi ricevuti dalle applicazioni nei dispositivi gestiti e visualizzare elenchi di notifiche.

Installazione

Questa sezione descrive l'installazione di Kaspersky Security Center e Kaspersky Security Center Web Console.

Installazione di Kaspersky Security Center (Installazione standard)

Questa procedura descrive come installare Kaspersky Security Center. Prima dell'installazione, è necessario installare un sistema di gestione database.

Per installare Kaspersky Security Center:

1. Con un account con privilegi di amministratore, avviare il file eseguibile ksc_<numero build>_full_<lingua localizzazione>.exe.
2. Nella finestra di selezione dell'applicazione visualizzata fare clic su **Installa Kaspersky Security Center**.

   Verrà avviata l'Installazione guidata di Kaspersky Security Center Administration Server.
3. A partire dalla pagina iniziale, procedere con la procedura guidata utilizzando il pulsante **Avanti**.
4. Se Microsoft .NET Framework non è installato, installarlo.
5. Accettare i termini del Contratto di licenza e dell'Informativa sulla privacy.
6. Selezionare il tipo di installazione. A scopo di valutazione, è consigliabile mantenere il valore predefinito **Standard**.

7. Se si desidera installare Kaspersky Security Center Web Console nello stesso dispositivo, selezionare la casella di controllo **Installa Kaspersky Security Center Web Console**.

   Se si deseleziona la casella di controllo, in seguito sarà possibile installare Kaspersky Security Center Web Console separatamente, nello stesso dispositivo o in un altro.

8. Selezionare la dimensione della rete. A scopo di valutazione, è consigliabile mantenere il valore predefinito **Meno di 100 dispositivi nella rete**.

9. Selezionare il tipo di server di database installato in precedenza.

10. Specificare i parametri di connessione per il server di database installato in precedenza.

11. Specificare i parametri di autenticazione per il server di database installato in precedenza.

12. Fare clic sul pulsante **Installa** per avviare l'installazione.

13. Al termine dell'installazione, scegliere se si desidera avviare o meno Administration Console subito dopo aver chiuso la procedura guidata.

    Se si sceglie di aprire Kaspersky Security Center Web Console, verrà aperta la schermata di accesso. Sarà quindi possibile eseguire la configurazione iniziale di Administration Server utilizzando l'Avvio rapido guidato.

    È possibile aprire Kaspersky Security Center Web Console solo se è già installato. Non è possibile aprire Kaspersky Security Center Web Console se non è stato installato durante l'installazione di Kaspersky Security Center o separatamente.

14. Nella finestra Administration Console visualizzata fare clic sull'Administration Server installato.

15. Nella finestra del certificato di Administration Server visualizzata fare clic sul pulsante **Sì** per continuare.

    Viene avviato l'Avvio rapido guidato di Administration Server, se non è stato eseguito nell'Administration Console basata sul Web.

Risoluzione dei problemi

Se la finestra del certificato di Administration Server non si apre e vengono visualizzati errori di connessione, provare quanto segue:

1. In Windows, aprire **Servizi** (**Pannello di controllo** → **Strumenti di amministrazione** → **Servizi**). Verificare che i servizi Kaspersky Security Center Network Agent e Kaspersky Security Center Administration Server siano in esecuzione.

2. In Windows, aprire **Visualizzatore eventi** (**Pannello di controllo** → **Strumenti di amministrazione** → **Visualizzatore eventi**), quindi selezionare **Registri applicazioni e servizi** → **Registro eventi Kaspersky**. Verificare che il log non contenga errori e che includa eventi come **Administration Server <numero versione> è in esecuzione**.

Installazione di Kaspersky Security Center Web Console

Questa sezione descrive come installare Kaspersky Security Center Web Console Server (anche noto come Kaspersky Security Center Web Console) separatamente. Prima dell'installazione, è necessario installare un DBMS e Kaspersky Security Center Administration Server. È possibile installare Kaspersky Security Center Web Console nello stesso dispositivo in cui è installato Kaspersky Security Center o in un altro dispositivo.

Per installare Kaspersky Security Center Web Console:

1. Con un account con privilegi di amministratore, avviare il file di installazione ksc-web-console-<numero versione>.<numero build>.exe.

   Verrà avviata l'Installazione guidata.

2. Selezionare una lingua per l'Installazione guidata.

3. Nella finestra iniziale fare clic su **Avanti**.

4. Nella finestra **Contratto di licenza** leggere e accettare i termini del Contratto di licenza con l'utente finale. L'installazione continua dopo aver accettato il Contratto di licenza con l'utente finale. In caso contrario, il pulsante **Avanti** non è disponibile.

5. Nella finestra **Cartella di destinazione** selezionare una cartella in cui verrà installato Kaspersky Security Center Web Console (per impostazione predefinita, %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Se tale cartella non esiste, verrà creata automaticamente durante l'installazione.

   È possibile modificare la cartella di destinazione utilizzando il pulsante **Sfoglia**.

6. Nella finestra **Impostazioni di connessione di Kaspersky Security Center Web Console** specificare le seguenti informazioni:

   - L'indirizzo di Kaspersky Security Center Web Console (per impostazione predefinita, 127.0.0.1).
   - La porta che Kaspersky Security Center Web Console utilizzerà per le connessioni in entrata, ovvero la porta che dà accesso a Kaspersky Security Center Web Console da un browser (per impostazione predefinita, 8080).

   È consigliabile mantenere inalterati l'indirizzo e il numero di porta.

   Se si desidera, è possibile fare clic su **Test** per verificare che la porta selezionata sia disponibile.

   Se si desidera abilitare la registrazione delle attività di Kaspersky Security Center Web Console, selezionare l'opzione appropriata. Se non si seleziona questa opzione, i file di log di Kaspersky Security Center Web Console non verranno creati.

7. Nella finestra **Impostazioni account** specificare i nomi e le password degli account.

   È consigliabile utilizzare gli account predefiniti.

8. Nella finestra **Certificato client** selezionare uno dei seguenti elementi:

- **Genera nuovo certificato**. Questa opzione è consigliata se non si dispone di un certificato del browser.
- **Scegli certificato esistente**. È possibile selezionare questa opzione se si dispone già di un certificato del browser. In tal caso, specificare il percorso.
- Se si sceglie di generare un nuovo certificato, quando si apre Kaspersky Security Center Web Console, il browser può segnalare la connessione a Kaspersky Security Center Web Console non è privata e il certificato di Kaspersky Security Center Web Console non è valido. Questo avviso viene visualizzato perché il certificato di Kaspersky Security Center Web Console è autofirmato e generato automaticamente da Kaspersky Security Center. Per rimuovere questo avviso, creare un certificato attendibile nella propria infrastruttura e che soddisfi i requisiti per i certificati personalizzati. Selezionare quindi l'opzione **Scegli certificato esistente** nella finestra **Certificato client**, quindi specificare il percorso del certificato personalizzato.

I certificati in formato PFX non sono supportati da Kaspersky Security Center Web Console. Per utilizzare tale certificato, è prima necessario convertirlo nel formato PEM supportato tramite un'utilità multipiattaforma basata su OpenSSL, come OpenSSL per Windows.

9. Nella finestra **Administration Server attendibili** verificare che Administration Server sia presente nell'elenco e fare clic su **Avanti** per passare all'ultima finestra del programma di installazione.

   Se è necessario aggiungere un nuovo Administration Server all'elenco, fare clic sul pulsante **Aggiungi**. Nella finestra visualizzata, specificare le proprietà di un nuovo Administration Server attendibile:

   - **Nome Administration Server**

     Il nome dell'Administration Server che verrà visualizzato nella finestra di accesso di Kaspersky Security Center Web Console.

   - **Indirizzo di Administration Server**

     L'indirizzo IP del dispositivo in cui si installa Administration Server.

   - **Porta di Administration Server**

     La porta OpenAPI utilizzata da Kaspersky Security Center Web Console per la connessione ad Administration Server (il valore predefinito è 13299).

   - **Certificato di Administration Server**

     Il file del certificato viene archiviato nel dispositivo in cui è installato Administration Server. Il percorso predefinito del certificato di Administration Server.

     - Per Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
     - Per Linux—/var/opt/kaspersky/klnagent_srv/1093/cert/

     Se si installa Kaspersky Security Center Web Console nello stesso dispositivo in cui è installato Administration Server, utilizzare uno dei percorsi sopra indicati. In caso contrario, copiare il file del certificato dal dispositivo in cui è installato Administration Server nel dispositivo in cui si installa Kaspersky Security Center Web Console, quindi specificare il percorso locale del certificato.

10. Nella finestra **IAM (Identity and Access Manager)** specificare se si desidera installare Identity and Access Manager (denominato anche IAM). Se si sceglie di installare Identity and Access Manager, specificare i seguenti numeri di porta:

    - **Porta amministratore KAS**. Per impostazione predefinita, viene utilizzata la porta 4445 per ricevere la configurazione da Kaspersky Security Center Web Console per la porta dell'endpoint di autorizzazione OAuth 2.0.
    - **Porta amministratore Facade**. Per impostazione predefinita, viene utilizzata la porta 2444 per la configurazione di Identity and Access Manager.
    - **Porta interazione Facade**. Per impostazione predefinita, viene utilizzata la porta 2445 per la connessione di Kaspersky OSMP KAS Service a Kaspersky OSMP Facade Service.

    Se si desidera, è possibile modificare i numeri di porta predefiniti. Non sarà possibile modificarli in futuro tramite Kaspersky Security Center Web Console.

11. Nell'ultima finestra del programma di installazione fare clic su **Installa** per avviare l'installazione.

Al termine dell'installazione sul desktop viene visualizzato un collegamento ed è possibile accedere a Kaspersky Security Center Web Console.

Viene avviato l'Avvio rapido guidato di Administration Server, se non è stato eseguito nell'Administration Console basata su Microsoft Management Console.

Risoluzione dei problemi

Se Kaspersky Security Center Web Console non viene visualizzato nel browser in corrispondenza dell'URL digitata, provare quanto segue:

1. Verificare di avere specificato il nome host o l'indirizzo IP corretto del dispositivo in cui è installato Kaspersky Security Center Web Console.
2. Verificare che il dispositivo che si desidera utilizzare abbia accesso al dispositivo in cui è installato Kaspersky Security Center Web Console.
3. Verificare che le impostazioni del firewall nel dispositivo in cui è installato Kaspersky Security Center Web Console consentano le connessioni in entrata tramite la porta 8080 e per l'applicazione node.exe.
4. In Windows, aprire **Servizi**. Verificare che il servizio di Kaspersky Security Center Web Console sia in esecuzione.
5. Verificare di poter accedere a Kaspersky Security Center tramite Administration Console.
6. In Windows, aprire **Visualizzatore eventi**, quindi selezionare **Registri applicazioni e servizi → Registro eventi Kaspersky**. Verificare che il log non contenga errori.

Installazione di Kaspersky Security Center Web Console connesso all'Administration Server installato nei nodi del cluster di failover

Questa sezione descrive come installare Kaspersky Security Center Web Console Server (di seguito anche Kaspersky Security Center Web Console), che si connette all'Administration Server installato nei nodi del cluster di failover Kaspersky Security Center o nei nodi del cluster di failover di Windows Server. Prima di installare Kaspersky Security Center Web Console, installare un DBMS e Kaspersky Security Center Administration Server nei nodi del cluster di failover Kaspersky Security Center o nei nodi del cluster di failover di Windows Server.

Se si utilizza un cluster di failover di Windows Server, si consiglia di non installare Kaspersky Security Center Web Console in un nodo del cluster di failover. In caso di errore del nodo, si perderà l'accesso ad Administration Server.

Per installare Kaspersky Security Center Web Console che si connette all'Administration Server installato nei nodi del cluster di failover:

1. Eseguire i passaggi dell'installazione di Kaspersky Security Center Web Console, partendo dal passaggio 1 al passaggio 8.

2. Nel passaggio 9, nella finestra **Administration Server attendibili**, fare clic sul pulsante **Aggiungi** per aggiungere un cluster di failover Microsoft come Administration Server attendibile.

   Nella finestra visualizzata, specificare le seguenti proprietà:

   - **Nome Administration Server**

     Il nome del cluster che verrà visualizzato nella finestra di accesso di Kaspersky Security Center Web Console.

   - **Indirizzo di Administration Server**

     A seconda del tipo di cluster di failover, specificare l'indirizzo del cluster:

     - **Cluster di failover Kaspersky Security Center**. Specificare l'indirizzo IP della scheda di rete secondaria come indirizzo del cluster se la scheda è stata creata in fase di preparazione dei nodi del cluster. In caso contrario, specificare l'indirizzo IP del sistema di bilanciamento del carico di terzi in uso.

     - **Cluster di failover di Windows Server**. Specificare l'indirizzo del cluster ottenuto durante la creazione del cluster di failover di Windows Server.

   - **Porta di Administration Server**

     La porta OpenAPI utilizzata da Kaspersky Security Center Web Console per la connessione ad Administration Server (il valore predefinito è 13299).

   - **Certificato di Administration Server**

     Il certificato di Administration Server si trova nell'archivio dati condiviso del cluster di failover Kaspersky Security Center o del cluster di failover di Windows Server. Il percorso predefinito del file del certificato: <cartella dati condivisa> \1093\cert\klserver.cer. Copiare il file del certificato dall'archivio dati condiviso nel dispositivo in cui si installa Kaspersky Security Center Web Console. Specificare il percorso locale del certificato di Administration Server.

3. Continuare con l'installazione standard di Kaspersky Security Center Web Console.

Al termine dell'installazione, sul desktop viene visualizzato un collegamento ed è possibile accedere a Kaspersky Security Center Web Console.

Upgrade di Kaspersky Security Center Web Console

Se si desidera utilizzare una versione più recente di Kaspersky Security Center Web Console senza rimuovere l'istanza attualmente installata, è possibile utilizzare la procedura di upgrade standard fornita nel programma di installazione di Kaspersky Security Center Web Console.

Per eseguire l'upgrade di Kaspersky Security Center Web Console:

1. Con un account che dispone di diritti di amministratore eseguire il file di installazione ksc-web-console-<numero versione><numero build>.exe, dove <numero build> rappresenta una build di Kaspersky Security Center Web Console il cui numero è successivo a quello dell'istanza attualmente installata.

2. Nella finestra dell'Installazione guidata visualizzata selezionare una lingua, quindi fare clic su **OK**.

3. Nella finestra di benvenuto selezionare l'opzione **Upgrade**, quindi fare clic su **Avanti**.

4. Nella finestra **Contratto di licenza** leggere e accettare i termini del Contratto di licenza con l'utente finale. L'installazione continua dopo aver accettato il Contratto di licenza con l'utente finale. In caso contrario, il pulsante **Avanti** non è disponibile.

5. Continuare con i passaggi dell'Installazione guidata fino al termine dell'installazione. Durante la procedura è inoltre possibile modificare le impostazioni di Kaspersky Security Center Web Console specificate durante l'installazione precedente. Quando si arriva al passaggio **Pronto per la modifica di Kaspersky Security Center Web Console**, fare clic sul pulsante **Upgrade**. Attendere l'applicazione delle nuove impostazioni e nel passaggio successivo dell'Installazione guidata fare clic su **Fine**. È inoltre possibile fare clic sul collegamento **Avviare Kaspersky Security Center Web Console nel browser** per avviare immediatamente l'istanza aggiornata di Kaspersky Security Center Web Console.

   La modifica delle impostazioni di Kaspersky Security Center Web Console durante l'upgrade è disponibile solo in Kaspersky Security Center Web Console versione 12.2 o successiva.

   L'istanza di Kaspersky Security Center Web Console è stata aggiornata.

Certificati per l'utilizzo con Kaspersky Security Center Web Console

La sezione descrive come emettere e sostituire certificati per Kaspersky Security Center Web Console e come rinnovare un certificato per Administration Server se il Server interagisce con Kaspersky Security Center Web Console.

Riemissione del certificato per Kaspersky Security Center Web Console

La maggior parte dei browser impone un limite relativo al periodo di validità di un certificato. Per rientrare in questo limite, il periodo di validità del certificato di Kaspersky Security Center Web Console è limitato a 397 giorni. È possibile sostituire un certificato esistente ricevuto da un'autorità di certificazione (CA) emettendo manualmente un nuovo certificato autofirmato. In alternativa, è possibile riemettere il certificato scaduto di Kaspersky Security Center Web Console.

La riemissione automatica del certificato per Kaspersky Security Center Web Console non è supportata È necessario riemettere manualmente il certificato scaduto.

Se si utilizza già un certificato autofirmato, è anche possibile riemetterlo eseguendo l'upgrade di Kaspersky Security Center Web Console tramite la procedura standard nel programma di installazione (opzione **Upgrade**).

Quando si apre Web Console, il browser potrebbe informare che la connessione a Web Console non è privata e il certificato Web Console non è valido. Questo avviso viene visualizzato perché il certificato di Web Console è autofirmato e generato automaticamente da Kaspersky Security Center. Per rimuovere o impedire questo avviso, è possibile eseguire una delle seguenti operazioni:

- Specificare un certificato personalizzato quando lo si emette nuovamente (opzione consigliata). Creare un certificato attendibile nella propria infrastruttura e che soddisfi i requisiti per i certificati personalizzati.
- Aggiungere il certificato di Web Console all'elenco dei certificati del browser attendibili dopo la riemissione del certificato. È consigliabile utilizzare questa opzione solo se non è possibile creare un certificato personalizzato.

Per emettere un nuovo certificato quando si installa per la prima volta Kaspersky Security Center Web Console:

1. Eseguire l'installazione di routine di Kaspersky Security Center Web Console.
2. Quando si arriva al passaggio **Certificato client** dell'Installazione guidata, selezionare l'opzione **Genera nuovo certificato**, quindi fare clic sul pulsante **Avanti**.
3. Procedere con i passaggi rimanenti dell'Installazione guidata fino al termine dell'installazione.

   Viene emesso un nuovo certificato per Kaspersky Security Center Web Console con un periodo di validità di 397 giorni.

Per riemettere il certificato scaduto di Kaspersky Security Center Web Console:

1. Con un account con diritti di amministratore, avviare il file di installazione ksc-web-console-<numero versione>.<numero build>.exe.
2. Nella finestra dell'Installazione guidata visualizzata selezionare una lingua, quindi fare clic su **OK**.
3. Nella finestra di benvenuto selezionare l'opzione **Riemetti certificato**, quindi fare clic su **Avanti**.
4. Nel passaggio successivo attendere il completamento della riconfigurazione di Kaspersky Security Center Web Console, quindi fare clic su **Fine**.

   Il certificato di Kaspersky Security Center Web Console viene riemesso per un altro periodo di validità di 397 giorni.

Se si utilizza Identity and Access Manager, è anche necessario riemettere tutti i certificati TLS per le porte utilizzate da Identity and Access Manager. Kaspersky Security Center Web Console visualizza una notifica allo scadere di un certificato. È necessario seguire le istruzioni della notifica.

Sostituzione del certificato per Kaspersky Security Center Web Console

Per impostazione predefinita, quando si installa Kaspersky Security Center Web Console Server, viene generato automaticamente un certificato del browser per l'applicazione. È possibile sostituire il certificato generato automaticamente con uno personalizzato.

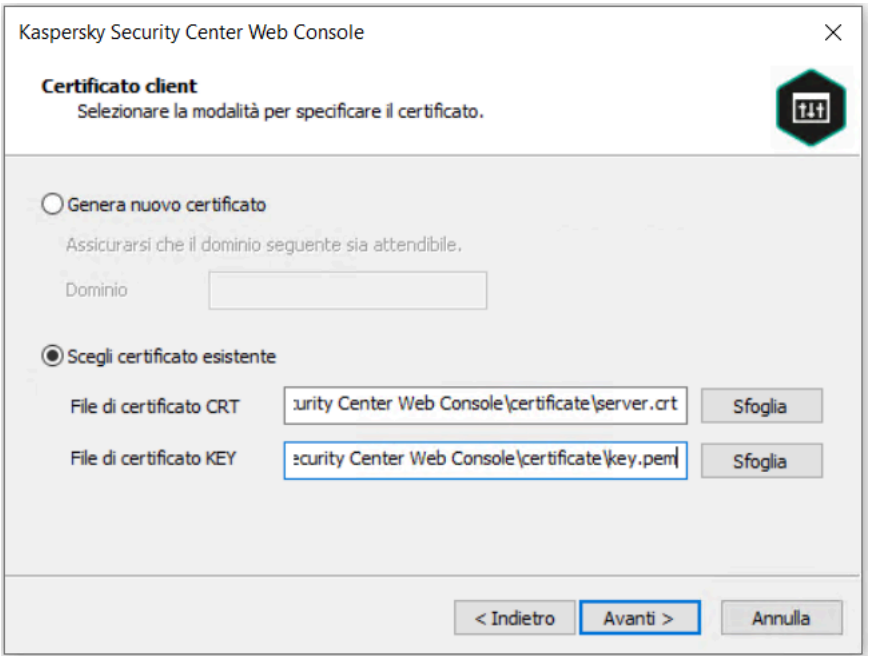
Per sostituire il certificato per Kaspersky Security Center Web Console Server con uno personalizzato:

1. Nel dispositivo in cui è installato Kaspersky Security Center Web Console, avviare il file di installazione ksc-web-console-<numero versione><numero build>.exe con un account con privilegi di amministratore.

   Verrà avviata l'Installazione guidata.

2. Nella prima pagina dell'Installazione guidata, selezionare l'opzione **Upgrade**.

3. Nella pagina **Certificato client** selezionare l'opzione **Scegli il certificato esistente** e specificare il percorso del certificato personalizzato.



Specificazione del certificato client

4. Nell'ultima pagina della procedura guidata, fare clic su **Modifica** per applicare le nuove impostazioni.

5. Al termine della riconfigurazione dell'applicazione, fare clic sul pulsante **Fine**.

Kaspersky Security Center Web Console funziona con il certificato specificato.

Specifica dei certificati per gli Administration Server attendibili in Kaspersky Security Center Web Console

Il certificato di Administration Server esistente viene automaticamente sostituito con uno nuovo prima della data di scadenza del certificato. È inoltre possibile sostituire il certificato di Administration Server esistente con uno personalizzato. Ogni volta che il certificato viene modificato, il nuovo certificato deve essere specificato nelle impostazioni di Kaspersky Security Center Web Console. In caso contrario, Kaspersky Security Center Web Console non sarà in grado di connettersi all'Administration Server.

Per specificare un nuovo certificato per l'Administration Server:

1. Nel dispositivo in cui è installato Administration Server copiare il file del certificato, ad esempio in un dispositivo di archiviazione di massa.

   Per impostazione predefinita, il file del certificato è archiviato nella seguente cartella:

   - Per Windows—%ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - Per Linux—/var/opt/kaspersky/klnagent_srv/1093/cert/

2. Nel dispositivo in cui è installato Kaspersky Security Center Web Console posizionare il file del certificato in una cartella locale.

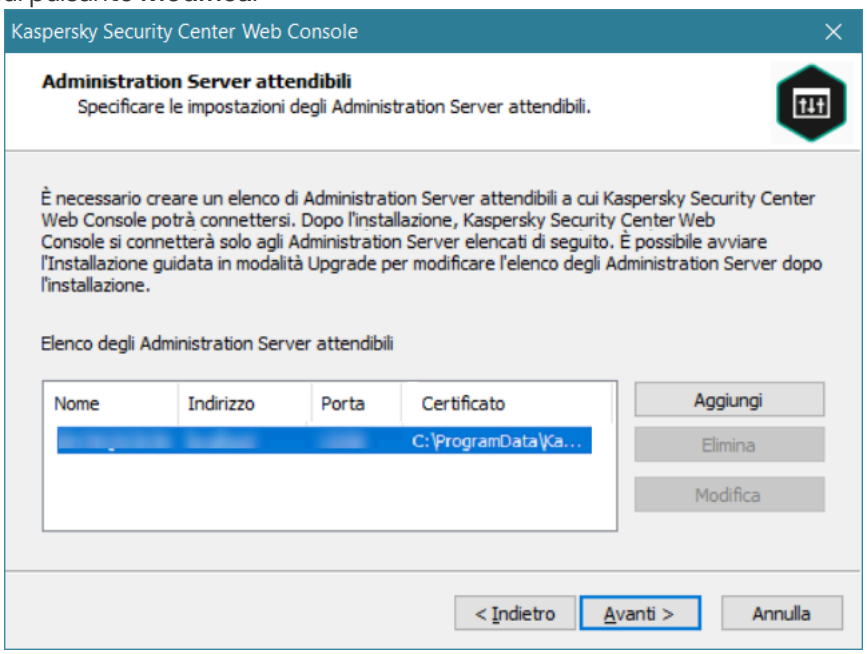
3. Eseguire il file di installazione ksc-web-console-<numero versione>.<numero build>.exe con un account con privilegi di amministratore.

   Verrà avviata l'Installazione guidata.

4. Nella prima pagina della procedura guidata, selezionare l'opzione **Upgrade**.

   Seguire le istruzioni della procedura guidata.

5. Nella pagina **Administration Server attendibili** della procedura guidata, selezionare l'Administration Server richiesto e fare clic sul pulsante **Modifica**.



Specificazione degli Administration Server attendibili

6. Nella finestra **Modifica Administration Server** visualizzata fare clic sul pulsante **Sfoglia**, specificare il percorso del nuovo file del certificato, quindi fare clic sul pulsante **Aggiornamento** per applicare le modifiche.

7. Nella pagina di **Pronto per la modifica di Kaspersky Security Center Web Console** della procedura guidata, fare clic sul pulsante **Upgrade** per avviare l'upgrade.

8. Al termine della riconfigurazione dell'applicazione, fare clic sul pulsante **Fine**.

9. Accedere a Kaspersky Security Center Web Console.

Kaspersky Security Center Web Console funziona con il certificato specificato.

Conversione di un certificato PFX nel formato PEM

Per utilizzare un certificato PFX in Kaspersky Security Center Web Console, è prima necessario convertirlo nel formato PEM utilizzando un'utilità multipiattaforma basata su OpenSSL.

Per convertire un certificato PFX nel formato PEM nel sistema operativo Windows:

1. In un'utilità multipiattaforma basata su OpenSSL, eseguire i seguenti comandi:

   ```
   openssl pkcs12 -in <nome file.pfx> -clcerts -nokeys -out server.crt
   openssl pkcs12 -in <nome file.pfx> -nocerts -nodes -out key.pem
   ```

   Di conseguenza, è necessario procurarsi una chiave pubblica come file .crt e una chiave privata come file .pem protetto da passphrase.

2. Assicurarsi che i file .crt e .pem siano generati nella stessa cartella in cui è archiviato il file .pfx.

3. Se il file .crt o .pem contiene gli "attributi bag", eliminare questi attributi utilizzando qualsiasi editor di testo, quindi salvare il file.

4. Riavviare il servizio Windows.

5. Kaspersky Security Center Web Console non supporta i certificati protetti da passphrase. Pertanto, eseguire il comando seguente in un'utilità multipiattaforma basata su OpenSSL per rimuovere una passphrase dal file .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Non utilizzare lo stesso nome per i file .pem di input e output.

   Di conseguenza, il nuovo file .pem non risulta criptato. Non è necessario inserire una passphrase per utilizzarlo.

I file .crt e .pem sono pronti per l'uso e possono essere specificati nel programma di installazione di Kaspersky Security Center Web Console.

Per convertire un certificato PFX nel formato PEM nel sistema operativo Linux:

1. In un'utilità multipiattaforma basata su OpenSSL, eseguire i seguenti comandi:

   ```
   openssl pkcs12 -in <filename.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <nome file.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Assicurarsi che il file del certificato e la chiave privata siano generati nella stessa directory in cui è archiviato il file .pfx.

3. Kaspersky Security Center Web Console non supporta i certificati protetti da passphrase. Pertanto, eseguire il comando seguente in un'utilità multipiattaforma basata su OpenSSL per rimuovere una passphrase dal file .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Non utilizzare lo stesso nome per i file .pem di input e output.

   Di conseguenza, il nuovo file .pem non risulta criptato. Non è necessario inserire una passphrase per utilizzarlo.

I file .crt e .pem sono pronti per l'uso e possono essere specificati nel programma di installazione di Kaspersky Security Center Web Console.

Migrazione da Kaspersky Security Center Windows

Questa sezione descrive la migrazione dei dispositivi gestiti e degli oggetti correlati (criteri, attività, gruppi, tag e altri oggetti) da Kaspersky Security Center Windows a:

- Kaspersky Security Center Cloud Console
- Kaspersky Security Center Linux

Migrazione a Kaspersky Security Center Cloud Console

È possibile eseguire la migrazione da Kaspersky Security Center Web Console a Kaspersky Security Center Cloud Console. Successivamente, si ottiene l'accesso ad Administration Server e al sistema di gestione dei database (DBMS), che sono ospitati nell'infrastruttura Kaspersky. Non è necessario un server fisico o un DBMS: entrambi vengono gestiti dagli esperti di Kaspersky.

È possibile eseguire la migrazione dei dispositivi gestiti che eseguono un sistema operativo Windows, Linux o macOS nell'ambito di Kaspersky Security Center Cloud Console. Se la rete include una gerarchia di Administration Server, è possibile salvarla in Kaspersky Security Center Cloud Console. È inoltre possibile trasferire:

- Attività e criteri delle applicazioni gestite
- Attività globali
- Selezioni dispositivi personalizzate
- Struttura di gruppi di amministrazione e dispositivi inclusi
- Tag assegnati ai dispositivi soggetti a migrazione

Al termine della migrazione, è possibile gestire i dispositivi utilizzando Kaspersky Security Center Cloud Console. Allo stesso tempo, gli oggetti trasferiti vengono mantenuti e Network Agent viene reinstallato in tutti i dispositivi gestiti.

Per informazioni su come eseguire la migrazione e un elenco dei prerequisiti, consultare la *Guida di Kaspersky Security Center Cloud Console*.

Migrazione a Kaspersky Next XDR Expert

Seguendo questo scenario, è possibile trasferire la struttura del gruppo di amministrazione, inclusi i dispositivi gestiti e altri oggetti del gruppo (criteri, attività, attività globali, tag e selezioni di dispositivi) da Kaspersky Security Center Windows sotto la gestione di Kaspersky Next XDR Expert.

Limitazioni:

- La migrazione è possibile solo da Kaspersky Security Center 14.2 Windows a Kaspersky Next XDR Expert a partire dalla versione 1.0.
- È possibile eseguire questo scenario solo utilizzando Kaspersky Security Center Web Console.

Passaggi

Lo scenario di migrazione procede per fasi:

1. **Scegliere un metodo di migrazione**

   Si esegue la migrazione a Kaspersky Next XDR Expert tramite la Migrazione guidata. I passaggi della Migrazione guidata dipendono dalla disposizione gerarchica degli Administration Server di Kaspersky Security Center Windows e Kaspersky Next XDR Expert:

- Migrazione con l'utilizzo di una gerarchia di Administration Server

  Scegliere questa opzione se l'Administration Server di Kaspersky Security Center Windows funge da secondario rispetto all'Administration Server di Kaspersky Next XDR Expert. L'utente gestisce il processo di migrazione e passa da un server all'altro all'interno di OSMP Console. Se si preferisce questa opzione, è possibile disporre gli Administration Server in una gerarchia per semplificare la procedura di migrazione. A tale scopo, creare la gerarchia prima di avviare la migrazione.

- Migrazione utilizzando un file di esportazione (archivio ZIP)

  Scegliere questa opzione se gli Administration Server di Kaspersky Security Center Windows e Kaspersky Next XDR Expert non sono disposti in una gerarchia. Il processo di migrazione viene gestito con due console: un'istanza per Kaspersky Security Center Windows e OSMP Console. In questo caso, si utilizzerà il file di esportazione creato e scaricato durante l'esportazione da Kaspersky Security Center Windows e si importerà questo file in Kaspersky Next XDR Expert.

2. **Esportare i dati da Kaspersky Security Center Windows**

   Aprire Kaspersky Security Center Windows, quindi eseguire la Migrazione guidata.

3. **Importare i dati in Kaspersky Next XDR Expert**

   Continuare la Migrazione guidata per importare i dati esportati in Kaspersky Next XDR Expert.

   Se i server sono organizzati in una gerarchia, l'importazione viene avviata automaticamente dopo un'esportazione riuscita all'interno della stessa procedura guidata. Se i server non sono organizzati in una gerarchia, continuare con la Migrazione guidata dopo essere passati a Kaspersky Next XDR Expert.

4. **Eseguire azioni aggiuntive per trasferire manualmente oggetti e impostazioni da Kaspersky Security Center Windows a Kaspersky Next XDR Expert (passaggio facoltativo)**

   È inoltre possibile trasferire gli oggetti e le impostazioni che non possono essere trasferiti tramite la Migrazione guidata. Ad esempio, è possibile eseguire anche le seguenti operazioni:

   - Configurare le attività globali di Administration Server
   - Configurare le impostazioni del criterio di Network Agent
   - Creare pacchetti di installazione delle applicazioni
   - Creare server virtuali
   - Assegnare e configurare punti di distribuzione
   - Configurare regole di spostamento dei dispositivi
   - Configurare regole per il tagging automatico dei dispositivi
   - Creare categorie di applicazioni

5. **Spostare i dispositivi gestiti importati sotto la gestione di Kaspersky Next XDR Expert**

   Per completare la migrazione, spostare i dispositivi gestiti importati sotto la gestione di Kaspersky Next XDR Expert. È possibile procedere utilizzando uno dei seguenti metodi:

   - Tramite l'attività di gruppo di Kaspersky Security Center

     Utilizzare l'attività Modifica Administration Server per modificare l'Administration Server con uno diverso per dispositivi client specifici.

   - Tramite l'utilità klmover

     Utilizzare l'utilità klmover e specificare le impostazioni di connessione per il nuovo Administration Server.

- Tramite installazione o reinstallazione di Network Agent nei dispositivi gestiti

  Creare un nuovo pacchetto di installazione di Network Agent e specificare le impostazioni di connessione per il nuovo Administration Server nelle proprietà del pacchetto di installazione. Utilizzare il pacchetto di installazione per installare Network Agent nei dispositivi gestiti importati tramite un'attività di installazione remota.

  È inoltre possibile creare e utilizzare un pacchetto di installazione indipendente per installare Network Agent in locale.

6. **Aggiornare Network Agent all'ultima versione**

   Si consiglia di aggiornare Network Agent alla stessa versione di OSMP Console.

7. **Verificare che i dispositivi gestiti siano visibili nel nuovo Administration Server**

   In Kaspersky Next XDR Expert Administration Server, aprire l'elenco dei dispositivi gestiti (**Risorse (dispositivi)** → **Dispositivi gestiti**) e controllare i valori nelle colonne **Visibile**, **Network Agent installato** e **Ultima connessione ad Administration Server**.

Altri metodi di migrazione dei dati

Oltre alla Migrazione guidata, è inoltre possibile trasferire attività e criteri specifici:

- Esportare le attività da Kaspersky Security Center Windows, quindi importare le attività in Kaspersky Next XDR Expert.
- Esportare i criteri da Kaspersky Security Center Windows, quindi importare i criteri in Kaspersky Next XDR Expert. I profili dei criteri correlati vengono esportati e importati insieme ai criteri selezionati.

Migrazione a Kaspersky Security Center Linux

La migrazione da Kaspersky Security Center Windows a Kaspersky Security Center Linux è disponibile tramite il backup dei dati di Administration Server (con l'utilità klbackup) e Migrazione guidata.

La tabella seguente consente di confrontare le principali funzionalità e limitazioni della migrazione tramite il backup dei dati di Administration Server e Migrazione guidata, per decidere quale approccio è più adatto alla propria organizzazione.

Confronto degli approcci di migrazione

Parametri	Backup dei dati di Administration Server	Migrazione guidata
Processo di migrazione	Creazione di un backup completo dei dati di Kaspersky Security Center Windows Administration Server e ripristino su un Kaspersky Security Center Linux Administration Server	Selezione ed esportazione dei dati di Administration Server per la migrazione, importazione di tali dati in Kaspersky Security Center Linux Administration Server e passaggio dei dispositivi gestiti sotto la gestione di Kaspersky Security Center Linux da parte dell'amministratore di Kaspersky Security Center.
Caratteristiche del metodo di migrazione	• Migrazione di tutti i dati dell'Administration Server • Migrazione di un numero qualsiasi di dispositivi gestiti • Utilizzata per ottenere una copia completa dei dati di Kaspersky Security Center Windows Administration Server e trasferirli a Kaspersky Security Center Linux Administration Server	• Migrazione parziale dei dati di Administration Server • È disponibile la selezione degli oggetti per la migrazione • Il gruppo o sottogruppo di amministrazione da migrare non può contenere più di 10.000 dispositivi • Utilizzata per trasferire parzialmente i dati di Administration Server, inclusi solo gli oggetti di gruppo all'interno dell'ambito di migrazione; gli oggetti di gruppo al di fuori dell'ambito di migrazione devono essere ripristinati manualmente

Ambito della migrazione	Trasferimento completo dei dati dell'Administration Server con un numero illimitato di dispositivi gestiti	• Struttura dei gruppi di amministrazione • Dispositivi gestiti inclusi nei gruppi di amministrazione (**non più di 10.000 dispositivi**) • Tag assegnati ai dispositivi di migrazione • Attività globali di Network Agent e applicazioni gestite (non per Administration Server) • Attività di gruppo di Network Agent e applicazioni gestite • Criteri delle applicazioni gestite • Modelli di rapporto • Ruoli utente • Utenti e gruppi di protezione interni • Categorie di applicazioni personalizzate con contenuti aggiunti manualmente • Selezioni dispositivi personalizzate
Ambito non migrato	—	• Attività globali di Administration Server • Eventi salvati in Administration Server • Archivio dei pacchetti di distribuzione delle applicazioni per l'installazione remota • Certificato di Administration Server • Chiavi di licenza utilizzate da Administration Server e dalle applicazioni gestite • Administration Server virtuali • Impostazioni del criterio di Network Agent • Regole di spostamento dei dispositivi • Regole per il tagging automatico dei dispositivi • Punti di distribuzione • Impostazioni dell'applicazione Kaspersky salvate sull'Administration Server
Versioni di Kaspersky Security Center che supportano la migrazione	• Qualsiasi versione supportata di Kaspersky Security Center Windows • Kaspersky Security Center Linux versione 15.2 o successiva	• Kaspersky Security Center Windows versione 14.2 o successiva • Kaspersky Security Center Linux versione 15 o successiva
DBMS tra cui è possibile effettuare la migrazione	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (solo per la migrazione da Kaspersky Security Center Windows versione 14.2 o successiva con la patch installata su Kaspersky Security Center Linux versione 15.3 o successiva) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB • PostgreSQL → PostgreSQL Postgres Pro → Postgres Pro (solo per la migrazione da Kaspersky Security Center Windows versione 15.1 o successiva a Kaspersky Security Center Linux versione 16 o successiva)	Migrazione tra DBMS supportati senza limitazioni

Migrazione a Kaspersky Security Center Linux utilizzando il backup dei dati di Administration Server

È possibile utilizzare un backup dei dati per migrare i dati di Kaspersky Security Center Windows Administration Server a Kaspersky Security Center Linux. Prima della migrazione, assicurarsi che le funzionalità necessarie di Kaspersky Security Center Windows siano supportate in Kaspersky Security Center Linux.

Limitazioni:

- La migrazione può essere eseguita tra i seguenti DBMS:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
  - PostgreSQL → PostgreSQL
  - Postgres Pro → Postgres Pro
- La migrazione dei dati diAdministration Server archiviati nel database Microsoft SQL Server, MySQL o MariaDB a MySQL o MariaDB è supportata per la migrazione da qualsiasi versione supportata di Kaspersky Security Center Windows a Kaspersky Security Center Linux versione 15.2 o successiva.
- La migrazione dei dati di Administration Server archiviati nel database di PostgreSQL a PostgreSQL o nel database Postgres Pro a Postgres Pro è supportata per la migrazione da Kaspersky Security Center Windows versione 15.1 o successiva a Kaspersky Security Center Linux versione 16 o successiva.
- La migrazione dei dati di Administration Server archiviati nel database Microsoft SQL Server a PostgreSQL o Postgres Pro è supportata per la migrazione da Kaspersky Security Center Windows versione 14.2 o successiva a Kaspersky Security Center Linux versione 15.3 o successiva.

  Per supportare la migrazione a PostgreSQL o Postgres Pro, è possibile eseguire una delle seguenti operazioni:

  - Installare la patch 15.1.0.20748-pf2 per Kaspersky Security Center Windows Administration Server. Contattare l'Assistenza tecnica di Kaspersky per ottenere questa patch.
  - Aggiornare Kaspersky Security Center Windows alla versione 15.1.0.22239.
- Se si utilizza MySQL o MariaDB come DBMS per Kaspersky Security Center Windows e Kaspersky Security Center Linux, il parametro `lower_case_table_names` deve corrispondere per il DBMS corrente e quello nuovo.

  Prima di creare un backup dei dati, controllare il parametro `lower_case_table_names`. Quindi, durante l'installazione di MySQL o MariaDB for Kaspersky Security Center Linux, è necessario impostare questo parametro sullo stesso valore specificato per questo parametro per Windows.

Passaggi

La migrazione tramite il backup dei dati di Administration Server avviene in fasi:

1. **Verificare di disporre dell'account utente interno dell'amministratore con cui è possibile accedere ad Administration Server**

   L'account dell'amministratore verrà utilizzato per accedere a Kaspersky Security Center Linux Administration Server. Se non si dispone di questo account e si è effettuato l'accesso solo con un account Windows locale o con un account di dominio, non sarà possibile accedere a Kaspersky Security Center Linux Administration Server dopo aver ripristinato il backup. Kaspersky Security Center Linux Administration Server non supporta l'accesso tramite l'account Windows locale. È possibile effettuare l'accesso con l'account di dominio, ma potrebbe essere necessaria una configurazione aggiuntiva di Administration Server.

Se non si dispone dell'account amministratore, sarà necessario crearlo dopo aver ripristinato la copia di backup utilizzando l'utilità kladduser.

2. **Creazione di una copia di backup aggiornata dei dati di Kaspersky Security Center Windows Administration Server**

   A seconda del tipo di DBMS utilizzato per Kaspersky Security Center Windows e Kaspersky Security Center Linux, effettuare una delle seguenti operazioni:

   - Per la migrazione di MySQL o MariaDB a MySQL o MariaDB: creare una copia di backup utilizzando l'utilità klbackup o un'attività di backup dei dati sul dispositivo con Administration Server installato.
   - Per la migrazione di PostgreSQL a PostgreSQL e Postgres Pro a Postgres Pro: creare una copia di backup utilizzando l'utilità klbackup o un'attività di backup dei dati nel dispositivo in cui è installato Administration Server.
   - Per la migrazione da Microsoft SQL Server a MySQL o MariaDB: creare una copia di backup utilizzando l'utilità klbackup con l'opzione **Esegui la migrazione al formato MySQL/MariaDB** abilitata.
   - Per la migrazione di Microsoft SQL Server a PostgreSQL o Postgres Pro:

     1. Richiedere supporto all'Assistenza tecnica di Kaspersky e installare la patch 15.1.0.20748-pf2 per Administration Server per supportare la migrazione a PostgreSQL e Postgres Pro.

        In alternativa, è possibile aggiornare Kaspersky Security Center Windows alla versione 15.1.0.22239.

     2. Creare una copia di backup utilizzando l'utilità klbackup.

        Se si esegue klbackup dalla riga di comando, utilizzare il flag `-migrate postgres`.

        Se si utilizza l'interfaccia klbackup, abilitare l'opzione **Migrate to Postgres format**.

   Dopo aver creato una copia di backup, scollegare Kaspersky Security Center Windows Administration Server dalla rete.

3. **Preparazione di un nuovo dispositivo per l'installazione di Kaspersky Security Center Linux**

   In questa fase dello scenario, effettuare le seguenti operazioni:

   1. Selezionare un nuovo dispositivo in cui installare Administration Server. Questo dispositivo deve soddisfare i requisiti hardware e software. Controllare inoltre che le porte utilizzate in Administration Server siano disponibili.
   2. Assegnare lo stesso indirizzo al nuovo dispositivo.

      È possibile assegnare al nuovo Administration Server il nome NetBIOS, l'FQDN e l'indirizzo IP statico. Dipende dall'indirizzo di Administration Server impostato nel pacchetto di installazione di Network Agent al momento della distribuzione dei Network Agent. In alternativa, è possibile utilizzare l'indirizzo di connessione che determina l'Administration Server a cui Network Agent si connette (è possibile ottenere questo indirizzo nei dispositivi gestiti utilizzando l'utilità klnagchk).

4. **Installazione e configurazione del DBMS**

   In questa fase dello scenario, effettuare le seguenti operazioni:

   1. Selezionare il tipo di DBMS che offre prestazioni ottimali. Prendere in considerazione il numero di dispositivi in rete, la topologia della rete e il carico di lavoro nella rete. È possibile scegliere uno dei DBMS supportati.
   2. Installare il DBMS in base al tipo di DBMS selezionato durante la creazione di un backup. Per informazioni su come installare il DBMS selezionato, consultare la relativa documentazione.

Una nuova versione del database non deve essere precedente a quella corrente.

3. Configurare il DBMS per l'utilizzo con Kaspersky Security Center Linux.

5 Installazione di Kaspersky Security Center Linux

Installare Kaspersky Security Center Linux nel nuovo dispositivo.

L'account utente interno dell'amministratore creato durante il programma di installazione, così come altri oggetti (gruppi, criteri, attività, utenti) creati prima di ripristinare i dati di Administration Server dal backup, andranno persi dopo il ripristino. Questi oggetti verranno sostituiti dagli oggetti contenuti nel backup.

6 Ripristino dei dati dell'Administration Server dalla copia di backup

In questa fase dello scenario, effettuare le seguenti operazioni:

1. Ripristinare i dati dell'Administration Server sul nuovo dispositivo utilizzando l'utilità klbackup.

2. Se non si dispone dell'account utente interno dell'amministratore con cui si è effettuato l'accesso a Kaspersky Security Center Windows Administration Server e si è utilizzato un account Windows locale o un account di dominio, creare un account amministratore utilizzando l'utilità kladduser come segue:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   dove il parametro `<password>` soddisfa i seguenti requisiti:

   - La password utente non può contenere meno di 8 o più di 256 caratteri.
   - La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
     - Lettere maiuscole (A-Z)
     - Lettere minuscole (a-z)
     - Numeri (0-9)
     - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7 Installazione di Kaspersky Security Center Web Console e configurazione di Administration Server

In questa fase dello scenario, effettuare le seguenti operazioni:

1. Installare Kaspersky Security Center Web Console.

   Se Kaspersky Security Center Web Console è stato installato in precedenza, reinstallarlo con lo stesso file di risposta.

   Accedere a Kaspersky Security Center Web Console con l'account utente interno dell'amministratore.

   Il processo di inizializzazione dei dati richiede in genere fino a 15 minuti dopo il ripristino dei dati di Administration Server, ma il tempo dipende dalle prestazioni hardware e dalle dimensioni dei dati di Administration Server. Durante questo periodo, Kaspersky Security Center Web Console potrebbe non riuscire a connettersi e mostrare gli errori.

2. Controllare la funzionalità delle caratteristiche principali di Administration Server al termine dell'inizializzazione dei dati nel database. Verificare che Administration Server venga sincronizzato con i dispositivi gestiti e che i dati di Administration Server vengano ripristinati.

3. Eseguire il polling dei controller di dominio per ripristinare le informazioni sulla struttura dei domini, sugli account utente, sui gruppi di protezione e sui nomi DNS dei dispositivi inclusi nei domini.

4. Se necessario, disinstallare Administration Server e il server del database dal dispositivo precedente.

   Non devono esistere più Administration Server nella stessa rete con lo stesso indirizzo di connessione e lo stesso certificato di Administration Server.

L'amministratore ha accesso ai dati e ai dispositivi gestiti di Administration Server che erano presenti in Kaspersky Security Center Windows, tenendo conto delle funzionalità supportate in Kaspersky Security Center Linux.

Migrazione a Kaspersky Security Center Linux tramite la Migrazione guidata

Seguendo questo scenario, è possibile trasferire la struttura del gruppo di amministrazione, inclusi i dispositivi gestiti e altri oggetti del gruppo (criteri, attività, attività globali, tag e selezioni di dispositivi) da Kaspersky Security Center Windows sotto la gestione di Kaspersky Security Center Linux. Prima della migrazione, assicurarsi che le funzionalità necessarie di Kaspersky Security Center Windows siano supportate in Kaspersky Security Center Linux.

Limitazioni:

- La migrazione è possibile solo da Kaspersky Security Center Windows versione 14.2 o successiva a Kaspersky Security Center Linux versione 15 o successiva.
- È possibile eseguire questo scenario solo utilizzando Kaspersky Security Center Web Console.

Passaggi

Lo scenario di migrazione procede per fasi:

1. **Scegliere un metodo di migrazione**

   Si esegue la migrazione a Kaspersky Security Center Linux tramite la Migrazione guidata. I passaggi della Migrazione guidata dipendono dalla disposizione gerarchica degli Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux:

   - Migrazione con l'utilizzo di una gerarchia di Administration Server

     Scegliere questa opzione se l'Administration Server di Kaspersky Security Center Windows funge da secondario rispetto all'Administration Server di Kaspersky Security Center Linux. Il processo di migrazione viene gestito e passa da un server all'altro all'interno di una singola istanza di Kaspersky Security Center Web Console. Se si preferisce questa opzione, è possibile disporre gli Administration Server in una gerarchia per semplificare la procedura di migrazione. A tale scopo, creare la gerarchia prima di avviare la migrazione.

   - Migrazione utilizzando un file di esportazione (archivio ZIP)

     Scegliere questa opzione se gli Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux non sono disposti in una gerarchia. Il processo di migrazione viene gestito con due istanze di Kaspersky Security Center Web Console: un'istanza per Kaspersky Security Center Windows e un'altra per Kaspersky Security Center Linux. In questo caso, si utilizzerà il file di esportazione creato e scaricato durante l'esportazione da Kaspersky Security Center Windows e si importerà questo file in Kaspersky Security Center Linux.

2. **Eseguire il backup del certificato e della chiave privata di Kaspersky Security Center Windows Administration Server (passaggio facoltativo)**

   È possibile porre i dispositivi gestiti sotto la gestione di Administration Server di Kaspersky Security Center Linux ripristinando il certificato e la chiave privata di Administration Server da una copia di backup. In questo caso, eseguire il backup del certificato e della chiave privata di Kaspersky Security Center Windows Administration Server. Nel passaggio 6, ripristinare il certificato e la chiave privata.

3. **Esportare i dati da Kaspersky Security Center Windows**

   Aprire Kaspersky Security Center Windows, quindi eseguire la Migrazione guidata.

4. **Importare i dati in Kaspersky Security Center Linux.**

   Continuare la Migrazione guidata per importare i dati esportati in Kaspersky Security Center Linux. Se i server sono organizzati in una gerarchia, l'importazione viene avviata automaticamente dopo un'esportazione riuscita all'interno della stessa procedura guidata. Se i server non sono organizzati in una gerarchia, continuare con la Migrazione guidata dopo essere passati a Kaspersky Security Center Linux.

5. **Eseguire azioni aggiuntive per trasferire manualmente oggetti e impostazioni da Kaspersky Security Center Windows a Kaspersky Security Center Linux (passaggio facoltativo)**

   È inoltre possibile trasferire gli oggetti e le impostazioni che non possono essere trasferiti tramite la Migrazione guidata. Ad esempio, è possibile eseguire anche le seguenti operazioni:

   - Trasferire le chiavi di licenza utilizzate da Administration Server e dalle applicazioni gestite
   - Configurare le attività globali di Administration Server
   - Configurare le impostazioni del criterio di Network Agent
   - Creare pacchetti di installazione delle applicazioni
   - Creare server virtuali
   - Assegnare e configurare punti di distribuzione
   - Configurare regole di spostamento dei dispositivi
   - Configurare regole per il tagging automatico dei dispositivi
   - Creare categorie di applicazioni

6. **Spostare i dispositivi gestiti importati sotto la gestione di Kaspersky Security Center Linux**

   Per completare la migrazione, spostare i dispositivi gestiti importati sotto la gestione di Kaspersky Security Center Linux. È possibile procedere utilizzando uno dei seguenti metodi:

   - Tramite l'utilità klmover

     Utilizzare l'utilità klmover e specificare le impostazioni di connessione per il nuovo Administration Server.

   - Tramite l'attività *Change Administration Server*

     Creare un'attività *Change Administration Server*, specificare i dispositivi gestiti importati, il nuovo Administration Server e altre impostazioni dell'attività. Eseguire quindi l'attività per mettere i dispositivi gestiti sotto la gestione di Administration Server di Kaspersky Security Center Linux.

   - Tramite la rimozione (se già installato) e l'ulteriore installazione di Network Agent nei dispositivi gestiti

     Creare un nuovo pacchetto di installazione di Network Agent e specificare le impostazioni di connessione per il nuovo Administration Server nelle proprietà del pacchetto di installazione. Rimuovere Network Agent nei dispositivi gestiti importati, quindi utilizzare il pacchetto di installazione per installare Network Agent nei dispositivi gestiti importati tramite un'attività di installazione remota. È inoltre possibile creare e utilizzare un pacchetto di installazione indipendente per installare Network Agent in locale. Per ulteriori informazioni, vedere Passaggio dei dispositivi gestiti alla gestione di Kaspersky Security Center Linux.

   - Tramite il ripristino del certificato e della chiave privata di Administration Server da una copia di backup (solo per la migrazione a Kaspersky Security Center Linux 15.1 o versioni successive).

Assegnare lo stesso indirizzo di rete dal dispositivo con Administration Server di Kaspersky Security Center Linux come in Administration Server di Kaspersky Security Center Windows. Eseguire l'utilità klbackup con il parametro `-cert_only` per ripristinare il certificato di Administration Server e la chiave privata dalla copia di backup salvata nel passaggio 2. Nella riga di comando, eseguire il seguente comando: percorso `/opt/kaspersky/ksc64/sbin/klbackup -path <alla copia di backup del certificato di Administration Server> -restore -cert_only`. Per ulteriori informazioni, consultare Utilizzo dell'utilità klbackup per cambiare i dispositivi gestiti sotto la gestione di un altro Administration Server.

7. **Aggiornare Network Agent all'ultima versione**

   Si consiglia di aggiornare Network Agent per Linux alla stessa versione di Kaspersky Security Center.

8. **Verificare che i dispositivi gestiti siano visibili nel nuovo Administration Server**

   In Kaspersky Security Center Linux Administration Server, aprire l'elenco dei dispositivi gestiti (**Risorse (dispositivi)** → DISPOSITIVI **Dispositivi gestiti**) e controllare i valori nelle colonne **Visibile**, **Network Agent installato** e **Ultima connessione ad Administration Server**.

Altri metodi di migrazione dei dati

Oltre alla Migrazione guidata, è inoltre possibile trasferire attività e criteri specifici:

- Esportare le attività da Kaspersky Security Center Windows, quindi importare le attività in Kaspersky Security Center Linux.
- Esportare i criteri specifici da Kaspersky Security Center Windows, quindi importare i criteri in Kaspersky Security Center Linux. I profili dei criteri correlati vengono esportati e importati insieme ai criteri selezionati.

Esportazione di oggetti di gruppo da Kaspersky Security Center Windows

La struttura dei gruppi di amministrazione della migrazione, inclusi i dispositivi gestiti e altri oggetti di gruppo da Kaspersky Security Center Windows a Kaspersky Security Center Linux, richiede che si selezionino prima i dati per l'esportazione e si crei un file di esportazione. Il file di esportazione contiene informazioni su tutti gli oggetti del gruppo di cui si desidera eseguire la migrazione. Questo file di esportazione verrà utilizzato per la successiva importazione in Kaspersky Security Center Linux.

È possibile esportare i seguenti oggetti:

- Attività e criteri delle applicazioni gestite
- Attività globali
- Selezioni dispositivi personalizzate
- Struttura di gruppi di amministrazione e dispositivi inclusi
- Tag assegnati ai dispositivi soggetti a migrazione

Prima di iniziare a esportare, leggere le informazioni generali sulla migrazione a Kaspersky Security Center Linux. Scegliere il metodo di migrazione, utilizzando o meno la gerarchia di Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux.

Per esportare i dispositivi gestiti e gli oggetti di gruppo correlati tramite la Migrazione guidata:

1. A seconda che gli Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux siano organizzati o meno in una gerarchia, effettuare una delle seguenti operazioni:

   - Se i server sono disposti in una gerarchia, aprire Kaspersky Security Center Web Console, quindi passare al server di Kaspersky Security Center Windows.

   - Se i server non sono disposti in una gerarchia, aprire Kaspersky Security Center Web Console connesso a Kaspersky Security Center Windows.

2. Nel menu principale, passare a **Operazioni** → **Migrazione**.

3. Per avviare la procedura guidata e seguirne i passaggi, selezionare la posizione in cui si desidera trasferire i dati e le impostazioni.

   - Se si desidera trasferire i dati e le impostazioni in Kaspersky Security Center Cloud Console, selezionare **Migra a Kaspersky Security Center Cloud Console**.

   - Se si desidera trasferire i dati e le impostazioni in Kaspersky Security Center Linux o Kaspersky Next XDR Expert, selezionare **Migra a Kaspersky Security Center Linux o Open Single Management Platform**.

4. Selezionare il gruppo o il sottogruppo di amministrazione da esportare. Accertarsi che il gruppo o il sottogruppo di amministrazione selezionato non contengano più di 10.000 dispositivi.

5. Selezionare le applicazioni gestite di cui esportare le attività e i criteri. Selezionare solo le applicazioni supportate da Kaspersky Security Center Linux. Gli oggetti delle applicazioni non supportate verranno comunque esportati, ma non saranno utilizzabili.

6. Utilizzare i collegamenti a sinistra per selezionare le attività globali, le selezioni di dispositivi e i rapporti da esportare. Il collegamento **Oggetti del gruppo** consente di escludere ruoli personalizzati, utenti interni, gruppi di sicurezza e categorie di applicazioni personalizzate dall'esportazione.

Il file di esportazione (archivio ZIP) viene creato. A seconda che si esegua o meno la migrazione con il supporto della gerarchia di Administration Server, il file di esportazione viene salvato come segue:

- Se i server sono organizzati in una gerarchia, il file di esportazione viene salvato nella cartella temporanea in Kaspersky Security Center Web Console Server.

- Se i server non sono organizzati in una gerarchia, il file di esportazione viene scaricato nel dispositivo.

Per la migrazione con il supporto della gerarchia di Administration Server, l'importazione viene avviata automaticamente al termine dell'esportazione. Per la migrazione senza il supporto della gerarchia di Administration Server, è possibile importare manualmente il file di esportazione salvato in Kaspersky Security Center Linux.

Importazione del file di esportazione in Kaspersky Security Center Linux

Per trasferire le informazioni sui dispositivi gestiti, gli oggetti e le relative impostazioni esportate da Kaspersky Security Center Windows, è necessario importarle in Kaspersky Security Center Linux o Kaspersky Next XDR Expert.

Per importare i dispositivi gestiti e gli oggetti di gruppo correlati tramite la Migrazione guidata:

1. A seconda che gli Administration Server di Kaspersky Security Center Windows e Kaspersky Security Center Linux siano organizzati o meno in una gerarchia, effettuare una delle seguenti operazioni:

   - Se i server sono organizzati in una gerarchia, procedere al passaggio successivo della Migrazione guidata al termine dell'esportazione. L'importazione viene avviata automaticamente dopo un'esportazione riuscita all'interno di questa procedura guidata (vedere il passaggio 2 di questa istruzione).

   - Se i server non sono organizzati in una gerarchia:

     a. Aprire Kaspersky Security Center Web Console connesso a Kaspersky Security Center Linux o Kaspersky Next XDR Expert.

     b. Nel menu principale, passare a **Operazioni** → **Migrazione**.

     c. Selezionare il file di esportazione (archivio ZIP) creato e scaricato durante l' esportazione da Kaspersky Security Center Windows. Viene avviato il caricamento del file di esportazione.

2. Dopo che il file di esportazione è stato caricato correttamente, è possibile continuare l'importazione. Se si desidera specificare un altro file di esportazione, fare clic sul collegamento **Modifica**, quindi selezionare il file richiesto.

3. Viene visualizzata l'intera gerarchia dei gruppi di amministrazione di Kaspersky Security Center Linux.

   Selezionare la casella di controllo accanto al gruppo di amministrazione di destinazione in cui devono essere ripristinati gli oggetti del gruppo di amministrazione esportato (dispositivi gestiti, criteri, attività e altri oggetti del gruppo).

4. Viene avviata l'importazione degli oggetti di gruppo. Non è possibile ridurre a icona la Migrazione guidata ed eseguire operazioni simultanee durante l'importazione. Attendere finché le icone di aggiornamento (🔄) accanto a tutti gli elementi nell'elenco di oggetti non vengono sostituite con segni di spunta verdi (✓). A questo punto, l'importazione è stata completata.

5. Al termine dell'importazione, la struttura esportata dei gruppi di amministrazione, inclusi i dettagli dei dispositivi, viene visualizzata sotto il gruppo di amministrazione di destinazione selezionato. Se il nome dell'oggetto ripristinato è identico al nome di un oggetto esistente, all'oggetto ripristinato viene aggiunto un suffisso incrementale.

> Se in un'attività migrata sono specificati i dettagli dell'account con cui viene eseguita l'attività, è necessario aprire l'attività e immettere nuovamente la password al termine dell'importazione.

Se l'importazione è stata completata con un errore, è possibile eseguire una delle seguenti operazioni:

- Per la migrazione con il supporto della gerarchia di Administration Server, è possibile iniziare a importare nuovamente il file di esportazione.

- Per la migrazione senza il supporto della gerarchia di Administration Server, è possibile avviare la Migrazione guidata per selezionare un altro file di esportazione e quindi importarlo di nuovo.

È possibile verificare se gli oggetti del gruppo inclusi nell'ambito di esportazione sono stati importati correttamente in Kaspersky Security Center Linux. A tale scopo, accedere alla sezione **Risorse (dispositivi)** e verificare che gli oggetti importati vengano visualizzati nelle sottosezioni corrispondenti.

Si noti che i dispositivi gestiti importati vengono visualizzati nella sottosezione **Dispositivi gestiti**, ma sono invisibili nella rete e Network Agent non è installato e in esecuzione su di essi (il valore *No* nelle colonne **Visibile**, **Network Agent installato** e **Network Agent è in esecuzione**).

Per completare la migrazione, è necessario impostare i dispositivi gestiti in modo che siano gestiti da Kaspersky Security Center Linux.

Passaggio dei dispositivi gestiti alla gestione di Kaspersky Security Center Linux

Dopo aver importato correttamente le informazioni sui dispositivi gestiti, gli oggetti e le relative impostazioni in Kaspersky Security Center Linux, è necessario impostare i dispositivi gestiti in modo che siano gestiti da Kaspersky Security Center Linux per completare la migrazione.

È possibile spostare i dispositivi gestiti in Kaspersky Security Center Linux in uno dei seguenti metodi:

- Utilizzando l'utilità klmover.
- Utilizzando l'attività *Change Administration Server*.
- Ripristino del certificato e della chiave privata di Administration Server da una copia di backup (solo per la migrazione a Kaspersky Security Center Linux 15.1 o versioni successive).

  Per ulteriori dettagli, fare riferimento alla fase 6 dello scenario di migrazione principale.
- Installazione di Network Agent nei dispositivi gestiti tramite un'attività di installazione remota.

Per impostare i dispositivi gestiti in modo che siano gestiti da Kaspersky Security Center Linux installando Network Agent:

1. Rimuovere Network Agent nei dispositivi gestiti importati di cui verrà eseguito il passaggio durante la gestione di Kaspersky Security Center Linux.
2. Passare ad Administration Server di Kaspersky Security Center Windows.
3. Accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**, quindi aprire le proprietà di un pacchetto di installazione esistente di Network Agent.

   Se il pacchetto di installazione di Network Agent non è presente nell'elenco dei pacchetti, scaricarne uno nuovo.

   È inoltre possibile creare e utilizzare un pacchetto di installazione indipendente per installare Network Agent in locale.
4. Nella scheda **Impostazioni**, selezionare la sezione **Connessione**. Specificare le impostazioni di connessione di Administration Server di Kaspersky Security Center Linux.
5. Creare un'attività di installazione remota per i dispositivi gestiti importati, quindi specificare il pacchetto di installazione di Network Agent riconfigurato.

   È possibile installare Network Agent tramite Administration Server di Kaspersky Security Center Windows o tramite un dispositivo basato su Windows che funge da punto di distribuzione. Se si utilizza Administration Server, abilitare l'opzione **Utilizzando le risorse del sistema operativo tramite Administration Server**. Se si utilizza un punto di distribuzione, abilitare l'opzione **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**.
6. Eseguire l'attività di installazione remota.

Al termine dell'attività di installazione remota, accedere ad Administration Server di Kaspersky Security Center Linux e verificare che i dispositivi gestiti siano visibili nella rete e che Network Agent sia installato e in esecuzione (il valore *Sì* nelle colonne **Visibile**, **Network Agent installato** e **Network Agent è in esecuzione**).

Accesso a Kaspersky Security Center Web Console e disconnessione

È possibile accedere a Kaspersky Security Center Web Console dopo aver installato Administration Server e Web Console Server. È necessario conoscere l'indirizzo Web di Administration Server e il numero di porta specificato durante l'installazione (per impostazione predefinita, la porta è 8080). JavaScript deve essere abilitato nel browser.

È possibile accedere a Kaspersky Security Center Web Console utilizzando i seguenti metodi:

- Usando l'autenticazione del dominio

  > Se si sceglie questo metodo, verificare che il polling dei controller di dominio sia stato attivato e gli utenti del dominio vengano aggiunti all'Administration Server.

- Specificando il nome utente e la password di dominio
- Specificando il nome utente e la password dell'amministratore

Accesso tramite l'autenticazione del dominio

Per accedere a Kaspersky Security Center Web Console utilizzando l'autenticazione del dominio:

1. Nel browser, accedere a https://`<indirizzo di Kaspersky Security Center Web Console>:<numero di porta>`

   Viene visualizzata la pagina di accesso.

2. Se sono stati aggiunti più server attendibili, nell'elenco Administration Server selezionare l'Administration Server a cui si desidera connettersi.

   Se è stato aggiunto un solo Administration Server, l'elenco degli Administration Server non viene visualizzato.

3. Eseguire una delle seguenti operazioni:

   - Fare clic sul pulsante **Usa autenticazione dominio**.
   - Se nel server vengono creati uno o più Administration Server virtuali e si desidera accedere a un server virtuale utilizzando l'autenticazione del dominio:

     a. Fare clic su **Mostra opzioni server virtuale**.

     b. Digitare il nome dell'Administration Server virtuale specificato durante la creazione del server virtuale.

     c. Fare clic sul pulsante **Usa autenticazione dominio**.

4. Se la verifica in due passaggi è abilitata per l'account, specificare il codice di sicurezza generato dall'app di autenticazione nel dispositivo mobile.

   È possibile tornare alla pagina di accesso, se necessario.

Dopo l'accesso, viene visualizzato il dashboard, con la lingua e il tema utilizzati l'ultima volta. È possibile spostarsi in Kaspersky Security Center Web Console e utilizzarlo per lavorare con Kaspersky Security Center.

Accesso specificando il nome utente e la password dell'amministratore

Per accedere a Kaspersky Security Center Web Console specificando il nome utente e la password dell'amministratore:

1. Nel browser, accedere a https://`<indirizzo di Kaspersky Security Center Web Console>:<numero di porta>`

   Viene visualizzata la pagina di accesso.

2. Se sono stati aggiunti più server attendibili, nell'elenco Administration Server selezionare l'Administration Server a cui si desidera connettersi.

   Se è stato aggiunto un solo Administration Server, l'elenco degli Administration Server non viene visualizzato.

3. Eseguire una delle seguenti operazioni:

- Per accedere ad Administration Server con un account utente di dominio:

  a. Immettere il nome utente e la password dell'utente di dominio.

  È possibile immettere il nome utente dell'utente del dominio in uno dei seguenti formati:

  - `Username@dns.domain`
  - `NTDOMAIN\Nome utente`

  b. Fare clic sul pulsante **Accedi**.

  Prima di accedere con un account utente di dominio, eseguire il polling del controller di dominio per ottenere l'elenco degli utenti di dominio.

- Per accedere all'Administration Server:

  a. Immettere il nome utente e la password dell'amministratore locale.

  b. Fare clic sul pulsante **Accedi**.

- Se nel server vengono creati uno o più Administration Server virtuali e si desidera accedere a un server virtuale:

  a. Fare clic su **Mostra opzioni server virtuale**.

  b. Digitare il nome dell'Administration Server virtuale specificato durante la creazione del server virtuale.

  c. Immettere il nome utente e la password dell'amministratore che dispone dei diritti sull'Administration Server virtuale.

  d. Fare clic sul pulsante **Accedi**.

4. Se la verifica in due passaggi è abilitata per l'account, specificare il codice di sicurezza generato dall'app di autenticazione nel dispositivo mobile.

   È possibile tornare alla pagina di accesso, se necessario.

5. Se la modifica forzata della password è abilitata per l'account o la password è scaduta, verrà visualizzata la finestra di modifica della password. Impostare una nuova password per l'accesso a Kaspersky Security Center Web Console.

Dopo l'accesso, viene visualizzato il dashboard, con la lingua e il tema utilizzati l'ultima volta. È possibile spostarsi in Kaspersky Security Center Web Console e utilizzarlo per lavorare con Kaspersky Security Center.

Disconnessione

Per eseguire la disconnessione da Kaspersky Security Center Web Console:

Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Esci**.

Kaspersky Security Center Web Console verrà chiuso e sarà visualizzata la pagina di accesso.

Identity and Access Manager in Kaspersky Security Center Web Console

Questa sezione fornisce informazioni su Identity and Access Manager (denominato anche IAM).

Informazioni su Identity and Access Manager

Identity and Access Manager (denominato anche IAM) è un componente di Kaspersky Security Center Web Console che consente di utilizzare un Single Sign-On (SSO) tra Kaspersky Security Center Web Console e l'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks. IAM utilizza il protocollo OAuth 2.0 per garantire l'autorizzazione di Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Web Console.

In questo caso Kaspersky Industrial CyberSecurity for Networks, a cui è possibile accedere tramite Kaspersky Security Center Web Console, viene indicato come *server di risorse*, mentre Kaspersky Security Center Web Console e l'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks sono indicati come *client OAuth 2.0*. Un server di risorse è un programma che funziona con più utenti e richiede l'autorizzazione. Il client utilizza un *token* per l'autorizzazione nel server di risorse. Un token è una sequenza univoca di byte. Quando un token scade, viene automaticamente riemesso. IAM funge da unico server di autorizzazione per più client OAuth 2.0.

È possibile installare IAM durante l'installazione di Kaspersky Security Center Web Console. È possibile abilitarlo successivamente in qualsiasi momento nelle impostazioni di Kaspersky Security Center Web Console. Se un server Kaspersky Industrial CyberSecurity o un'interfaccia Web di Kaspersky Industrial Cybersecurity è installato in un dispositivo gestito dallo stesso Administration Server, IAM rileva questo programma e viene visualizzata una notifica in Kaspersky Security Center Web Console per informare l'utente. È possibile registrare Kaspersky Industrial CyberSecurity for Networks e successivamente utilizzare SSO sia per Kaspersky Security Center Web Console che per l'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks.

Se ci si disconnette da Kaspersky Security Center Web Console, la sessione nell'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks terminerà e sarà necessario accedere nuovamente a Kaspersky Security Center Web Console.

Abilitazione di Identity and Access Manager: scenario

Prerequisiti

Prima di iniziare, assicurarsi di avere accesso a Kaspersky Industrial CyberSecurity for Networks versione 3.1 o successiva.

Passaggi

L'abilitazione di Identity and Access Manager (denominato anche IAM) prevede diverse fasi:

1. **Controllo delle porte necessarie**

Assicurarsi che le porte 3333, 4004 e 4444 siano aperte nel dispositivo in cui è installato Kaspersky Security Center Web Console. Queste porte sono necessarie per utilizzare OAuth 2.0. Se si desidera, è possibile modificare i numeri di porta predefiniti nella finestra delle impostazioni di Kaspersky Security Center Web Console.

Oltre alle porte 3333, 4004 e 4444, Kaspersky Security Center Web Console utilizza anche le porte 4445, 2444 e 2445 per vari scopi.

2. **Installazione di Identity and Access Manager**

   Durante l'installazione di Kaspersky Security Center Web Console, specificare che si desidera installare Identity and Access Manager. In caso contrario, eseguire nuovamente l'Installazione guidata di Kaspersky Security Center Web Console.

3. **Configurazione di Identity and Access Manager**

   Nella finestra delle impostazioni di Kaspersky Security Center Web Console assicurarsi che l'interruttore **IAM (Identity and Access Manager)** sia abilitato. Specificare inoltre il nome DNS del dispositivo in cui è installato Kaspersky Security Center Web Console: le applicazioni client si connetteranno a questo dispositivo.

4. **Definizione delle impostazioni dei token**

   Nella finestra delle impostazioni di Kaspersky Security Center Web Console specificare la durata dei token e il timeout dell'autorizzazione che verrà utilizzato da Identity and Access Manager. È possibile utilizzare i valori predefiniti oppure specificare valori specifici in base alle proprie esigenze.

5. **Concessione dei certificati**

   Se si preferisce utilizzare i certificati generati da Administration Server, nella finestra delle impostazioni di Kaspersky Security Center Web Console scaricare i certificati radice per le porte utilizzate da IAM e distribuirli alle workstation degli utenti di Kaspersky Security Center Web Console. In caso contrario, i browser degli utenti visualizzeranno messaggi di errore durante il tentativo di connessione a Kaspersky Security Center Web Console.

6. **Registrazione dei server Kaspersky Industrial CyberSecurity for Networks e delle interfacce Web di Kaspersky Industrial CyberSecurity for Networks**

   Quando IAM è installato, Kaspersky Security Center Web Console visualizza un messaggio per informare che uno o più server Industrial CyberSecurity for Networks e una o più interfacce Web di Kaspersky Industrial CyberSecurity for Networks sono in attesa di registrazione. Fare clic su questo messaggio per registrare Kaspersky Industrial CyberSecurity for Networks Server (o più server) e l'interfaccia Web (o più interfacce Web).

Risultati

Dopo aver completato questo scenario, sarà possibile utilizzare SSO e IAM per Kaspersky Industrial CyberSecurity for Networks e Kaspersky Security Center Web Console.

Configurazione di Identity and Access Manager in Kaspersky Security Center Web Console

Per configurare Identity and Access Manager in base alle proprie esigenze:

1. Nel menu principale, passare a **Impostazioni** → **Identity and Access Manager**.
2. Nella sezione **Identity and Access Manager** assicurarsi che Identity and Access Manager sia abilitato.
3. Fare clic sul collegamento **Impostazioni** nella riga **Nome di rete del dispositivo Identity and Access Manager**.

4. Specificare il nome DNS del dispositivo in cui è stato installato Identity and Access Manager. Le applicazioni client si connetteranno a questo dispositivo.

5. Se si desidera, modificare le impostazioni predefinite dei token, le impostazioni del certificato e i numeri di porta facendo clic sul collegamento **Impostazioni** nel relativo gruppo di impostazioni.

Identity and Access Manager è abilitato e funziona in base alle proprie esigenze.

Registrazione dell'applicazione Kaspersky Industrial CyberSecurity for Networks in Kaspersky Security Center Web Console

Per iniziare a utilizzare l'applicazione Kaspersky Industrial CyberSecurity for Networks tramite Kaspersky Security Center Web Console, è prima necessario registrarla in Kaspersky Security Center Web Console.

Per registrare l'applicazione Kaspersky Industrial CyberSecurity for Networks:

1. Assicurarsi di aver eseguito le seguenti operazioni:

   - Download e installazione del plug-in Web di Kaspersky Industrial CyberSecurity for Networks.

     È tuttavia possibile eseguire questa operazione successivamente in attesa della sincronizzazione del server Kaspersky Industrial CyberSecurity for Networks con Administration Server.

   - Completamento dello scenario di preparazione all'utilizzo della tecnologia Single Sign-On (SSO).

   - Le impostazioni necessarie nell'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks sono specificate nella pagina di Kaspersky Security Center. Per informazioni dettagliate, fare riferimento alla Guida in linea di Kaspersky Industrial CyberSecurity for Networks.

   - Accesso a Kaspersky Security Center Web Console con un account amministratore.

   - Configurazione di IAM.

2. Spostare il dispositivo in cui è installato il server Kaspersky Industrial CyberSecurity for Networks dal gruppo Dispositivi non assegnati al gruppo Dispositivi gestiti:

   a. Nel menu principale accedere a **Individuazione e distribuzione** → **Dispositivi non assegnati**.

   b. Selezionare la casella di controllo accanto al dispositivo in cui è installato il server Kaspersky Industrial CyberSecurity for Networks.

   c. Fare clic sul pulsante **Sposta nel gruppo**.

   d. Nella gerarchia dei gruppi di amministrazione selezionare la casella di controllo accanto al gruppo Dispositivi gestiti.

   e. Fare clic sul pulsante **Sposta**.

3. Passare alle proprietà del dispositivo in cui è installato il server Kaspersky Industrial CyberSecurity for Networks.

4. Nella pagina delle proprietà del dispositivo, nella sezione **Generale**, selezionare l'opzione **Non eseguire la disconnessione da Administration Server**, quindi fare clic sul pulsante **Salva**.

5. Nella pagina delle proprietà del dispositivo selezionare la sezione **Applicazioni**.

6. Nella sezione **Applicazioni** selezionare Kaspersky Network Agent.

7. Se lo stato corrente dell'applicazione è *Arrestata*, attendere finché non diventa *In esecuzione*.

   L'operazione può richiedere fino a 15 minuti. Se non è ancora stato installato il plug-in Web di Kaspersky Industrial CyberSecurity for Networks, è possibile farlo durante l'attesa.

8. Nel menu principale, passare a **Impostazioni** → **Identity and Access Manager**.

   Nel campo **Richieste di registrazione** viene visualizzata una richiesta in sospeso.

9. Fare clic sul collegamento **Impostazioni** sotto il campo **Richieste di registrazione**.

10. Nell'elenco dei client registrati visualizzato selezionare la casella di controllo accanto al nome del server Kaspersky Industrial CyberSecurity for Networks con lo stato *In sospeso*, quindi fare clic sul pulsante **Approva**.

    Se non si desidera registrare il server Kaspersky Industrial CyberSecurity for Networks, è possibile fare clic sul pulsante Rifiuta e tornare all'elenco in un secondo momento.

    Dopo aver fatto clic sul pulsante **Approva**, lo stato diventa *Approvato* e successivamente *Pronto*. Se lo stato non cambia è possibile fare clic sul pulsante Aggiorna.

11. Chiudere l'elenco dei client registrati e assicurarsi che il valore nel campo **Client registrati** sia aumentato.

12. Per aggiungere il widget Kaspersky Industrial CyberSecurity for Networks al dashboard:

    a. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.

    b. Nella dashboard, fare clic sul pulsante **Aggiungi o ripristina widget Web**.

    c. Nel menu del widget visualizzato selezionare **Altro**.

    d. Selezionare il widget Kaspersky Industrial CyberSecurity for Networks.

    Adesso è possibile procedere all'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks utilizzando il collegamento presente nel widget.

Al termine della procedura di registrazione, nella pagina di accesso dell'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks viene visualizzato il nuovo pulsante **Kaspersky Security Center**. È possibile fare clic su questo pulsante per accedere all'interfaccia Web di Kaspersky Industrial CyberSecurity for Networks con le credenziali di Kaspersky Security Center.

Durata dei token e timeout dell'autorizzazione per Identity and Access Manager

Quando si configura Identity and Access Manager (denominato anche IAM), è necessario specificare le impostazioni per la durata dei token e il timeout dell'autorizzazione. Le impostazioni predefinite hanno l'obiettivo di rispecchiare sia gli standard di sicurezza che il carico del server. È tuttavia possibile modificare queste impostazioni in base ai criteri dell'organizzazione.

IAM riemette automaticamente un token quando sta per scadere.

La tabella seguente elenca le impostazioni predefinite relative alla durata dei token.

Impostazioni relative alla durata dei token

Token	Durata predefinita (in secondi)	Descrizione
Token dell'identità (id_token)	86400	Token di identità utilizzato dal client OAuth 2.0 (cioè Kaspersky Security Center Web Console o Kaspersky Industrial CyberSecurity Console). IAM invia al client il token ID contenente le informazioni sull'utente (cioè il profilo utente).
Token di accesso (access_token)	86400	Token di accesso utilizzato dal client OAuth 2.0 per accedere al server di risorse per conto del proprietario della risorsa identificato da IAM.
Token di aggiornamento (refresh_token)	172800	Il client OAuth 2.0 utilizza questo token per riemettere il token di identità e il token di accesso.

La tabella di seguito elenca i timeout per auth_code e login_consent_request.

Impostazioni di timeout dell'autorizzazione

Impostazione	Timeout predefinito (in secondi)	Descrizione
Codice di autorizzazione (auth_code)	3600	Timeout per lo scambio del codice con il token. Il client OAuth 2.0 invia questo codice al server di risorse e ottiene in cambio il token di accesso.
Timeout della richiesta di consenso per l'accesso (login_consent_request)	3600	Timeout per la delega dei diritti utente al client OAuth 2.0.

Per ulteriori informazioni sui token, vedere il sito Web OAuth.

Per configurare il timeout per i client senza attività di mouse o tastiera rilevate:

1. Nella cartella di installazione di Kaspersky Security Center Web Console, individuare e aprire il file config.json. Il file contiene i parametri per configurare il timeout per i client inattivi.

2. Utilizzare il parametro `clientIdleTimeout` per specificare l'ora, in millisecondi, dopo la quale un client inattivo mostra un pop-up di avviso.

3. Utilizzare il parametro `clientLogoutTimeout` per specificare l'ora, in millisecondi, dopo la quale l'autorizzazione IAM per il client inattivo viene terminata. `clientLogoutTimeout` esegue il conto alla rovescia in sequenza dopo `clientIdleTimeout`.

Download e distribuzione dei certificati IAM

Per impostazione predefinita, Identity and Access Manager utilizza i certificati generati da Administration Server per concedere ai browser l'accesso a Kaspersky Security Center Web Console. Tuttavia, se si desidera, è possibile utilizzare certificati personalizzati. Indipendentemente dal certificato utilizzato, è necessario assicurarsi che tutte le workstation da cui gli utenti di Kaspersky Security Center Web Console accedono a Kaspersky Security Center Web Console ritengano attendibile questo certificato.

Per scaricare e distribuire i certificati:

1. Nel menu principale, passare a **Impostazioni** → **Identity and Access Manager**.
2. Per ogni certificato, fare clic sul collegamento **Impostazioni** nel gruppo di impostazioni attinente, quindi eseguire una delle seguenti operazioni:
   - Se si desidera utilizzare il certificato generato da Administration Server durante l'installazione di Kaspersky Security Center Web Console:
     1. Selezionare **Certificato generato da Administration Server** nella finestra delle proprietà del certificato visualizzata.
     2. Fare clic sul pulsante **Scarica** per scaricare il certificato.
     3. Distribuire il certificato scaricato in tutte le workstation da cui gli utenti di Kaspersky Security Center Web Console accedono a Kaspersky Security Center Web Console.
   - Se si dispone di un certificato che si desidera utilizzare:
     1. Selezionare **Certificato TLS personalizzato** nella finestra delle proprietà del certificato visualizzata.
     2. Selezionare il file del certificato e la chiave privata.
     3. Fare clic sul pulsante **OK**.
     4. Distribuire il certificato a tutte le workstation da cui gli utenti accedono a Kaspersky Security Center Web Console o Kaspersky Industrial CyberSecurity Console.

I certificati concedono agli utenti l'accesso a Kaspersky Security Center Web Console e Kaspersky Industrial CyberSecurity Console.

È necessario riemettere tutti i certificati tempestivamente. I certificati generati da Administration Server devono essere rigenerati manualmente. I certificati generati dal programma di installazione di Kaspersky Security Center Web Console devono essere rigenerati utilizzando il programma di installazione.

Disabilitazione di Identity and Access Manager

Se si desidera, è possibile disabilitare Identity and Access Manager (noto anche come IAM).

Per disabilitare IAM,

1. Nel menu principale, passare a **Impostazioni** → **Integrazione**.
2. Nella sezione **Identity and Access Manager**, impostare l'interruttore **Identity and Access Manager** su disabilitato.

È possibile abilitare IAM successivamente in qualsiasi momento.

Se si aggiorna Kaspersky Security Center Web Console tramite il programma di installazione e si specifica che non si desidera installare IAM, verrà eseguito l'upgrade di Kaspersky Security Center Web Console e IAM non verrà installato. Tutte le informazioni sull'integrazione con Kaspersky Industrial CyberSecurity for Networks verranno eliminate dal dispositivo, così come i file di configurazione IAM e i file di registro.

Configurazione dell'autenticazione del dominio utilizzando i protocolli NTLM e Kerberos

Kaspersky Security Center 15.1 consente di utilizzare l'autenticazione del dominio in OpenAPI utilizzando i protocolli NTLM e Kerberos. L'utilizzo dell'autenticazione del dominio consente a un utente Windows di abilitare l'autenticazione sicura in Kaspersky Security Center Web Console senza dover reinserire la password nella rete aziendale (Single Sign-On).

L'autenticazione del dominio in OpenAPI tramite il protocollo Kerberos prevede le seguenti limitazioni:

- L'utente di Kaspersky Security Center Web Console deve essere autenticato in Active Directory utilizzando il protocollo Kerberos. L'utente deve disporre di un Ticket Granting Ticket (denominato anche TGT) Kerberos valido. Un TGT viene emesso automaticamente quando ti esegue l'autenticazione nel dominio.

- È necessario configurare l'autenticazione Kerberos nel browser. Per informazioni dettagliate, fare riferimento alla documentazione del browser in uso.

Se si desidera utilizzare l'autenticazione del dominio utilizzando i protocolli Kerberos, la rete deve soddisfare le seguenti condizioni:

- Administration Server deve essere eseguito con il nome dell'account di dominio.

- Il Kaspersky Security Center Web Console Server deve essere installato nello stesso dispositivo in cui è installato Administration Server.

- È necessario specificare i seguenti nomi dell'entità servizio per l'account di Administration Server:

  - "http/<server.fqnd.name>"

  - "http/<server>"

  Qui <server> sta per il nome di rete del dispositivo Administration Server e <server.fqnd.name> sta per il nome di dominio completo del dispositivo Administration Server.

- Quando ci si connette ad Administration Console o a Kaspersky Security Center Web Console, l'indirizzo di Administration Server deve essere specificato esattamente come l'indirizzo per il quale è registrato il nome dell'entità servizio. È possibile specificare sia <server.fqnd.name> che <server>.

- Per un accesso senza password, il processo del browser in cui Kaspersky Security Center Web Console è aperto come browser deve essere eseguito con un account di dominio.

I protocolli Kerberos e NTLM sono supportati solo in OpenAPI per Kaspersky Security Center 15.1. Non sono supportati in OpenAPI per Kaspersky Security Center Linux.

Configurazione di Administration Server

Questa sezione descrive il processo di configurazione e le proprietà di Kaspersky Security Center Administration Server.

Configurazione della connessione di Kaspersky Security Center Web Console ad Administration Server

Per impostare le porte di connessione di Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Porte di connessione**.

L'applicazione visualizzerà le impostazioni di connessione principali del server selezionato.

Kaspersky Security Center Web Console è connesso ad Administration Server tramite la porta SSL TCP 13299. La stessa porta può essere utilizzata dagli oggetti di automazione klakaut.

La porta TCP 14000 può essere utilizzata per connettere Kaspersky Security Center Web Console, punti di distribuzione, Administration Server secondari e oggetti di automazione klakaut, nonché per ricevere i dati dai dispositivi client.

In genere, la porta SSL TCP 13000 può essere utilizzata solo da Network Agent, un Administration Server secondario e dall'Administration Server primario nella rete DMZ. In alcuni casi può essere necessario connettere Kaspersky Security Center Web Console tramite la porta SSL 13000:

- Se è probabile che venga utilizzata una singola porta SSL sia per Kaspersky Security Center Web Console che per altre attività (ricezione dei dati dai dispositivi client, connessione di punti di distribuzione, connessione di Administration Server secondari).

- Se un oggetto di automazione klakaut non è connesso ad Administration Server direttamente, bensì tramite un punto di distribuzione nella rete perimetrale.

Configurazione della registrazione degli eventi di connessione ad Administration Server

È possibile salvare in un file di registro la cronologia delle connessioni e dei tentativi di connessione all'Administration Server durante l'esecuzione. Le informazioni nel file consentono di tenere traccia non solo delle connessioni all'interno dell'infrastruttura di rete, ma anche dei tentativi non autorizzati di accesso al server.

Per registrare gli eventi di connessione all'Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Porte di connessione**.

3. Abilitare l'opzione **Registra eventi di connessione ad Administration Server**.

Tutti gli ulteriori eventi di connessione in entrata all'Administration Server, i risultati di autenticazione e gli errori SSL verranno salvati nel file %ProgramData%\KasperskyLab\adminkit\logs\SC.syslog.

Configurazione delle impostazioni di accesso a Internet per Administration Server

È necessario configurare l'accesso a Internet per utilizzare Kaspersky Security Network e per scaricare gli aggiornamenti dei database anti-virus per Kaspersky Security Center e le applicazioni Kaspersky gestite.

Per specificare le impostazioni di accesso a Internet per Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Configurazione dell'accesso a Internet**.

3. Se si desidera utilizzare un server proxy durante la connessione a Internet, abilitare l'opzione **Usa server proxy**. Se questa opzione è abilitata, i campi sono disponibili per l'immissione delle impostazioni. Specificare le seguenti impostazioni per la connessione a un server proxy:

   - **Indirizzo**

     Indirizzo del server proxy utilizzato per la connessione di Kaspersky Security Center a Internet.

   - **Numero di porta**

     Numero della porta utilizzata per stabilire la connessione al proxy di Kaspersky Security Center.

   - **Ignora il server proxy per gli indirizzi locali**

     Non verrà utilizzato alcun server proxy per la connessione ai dispositivi dalla rete locale.

   - **Autenticazione server proxy**

     Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

     Questo campo di immissione è disponibile se la casella di controllo **Usa server proxy** è selezionata.

   - **Nome utente**

     Account utente con il quale è stata stabilita la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

   - **Password**

     Password impostata dall'utente di cui è stato utilizzato l'account per stabilire la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

     Per visualizzare la password immessa, tenere premuto il pulsante **Mostra** per il tempo necessario.

È inoltre possibile configurare l'accesso a Internet utilizzando l'Avvio rapido guidato.

Impostazione del numero massimo di eventi nell'archivio eventi

Nella sezione **Archivio eventi** della finestra delle proprietà di Administration Server è possibile modificare le impostazioni per l'archiviazione degli eventi nel database di Administration Server, limitando il numero di record degli eventi e il periodo di archiviazione dei record. Quando si specifica il numero massimo di eventi, l'applicazione calcola approssimativamente la quantità di spazio di archiviazione necessario per il numero specificato. È possibile utilizzare questo calcolo approssimativo per valutare se è necessario liberare spazio su disco per evitare l'overflow del database. La capacità predefinita del database di Administration Server è di 400.000 eventi. La capacità massima consigliata del database è di 45 milioni di eventi.

L'applicazione controlla il database ogni 10 minuti. Se il numero di eventi raggiunge il valore massimo specificato più 10.000, l'applicazione elimina gli eventi meno recenti in modo che rimanga solo il numero massimo di eventi specificato.

Quando l'Administration Server elimina gli eventi meno recenti, non può salvare i nuovi eventi nel database. Durante questo periodo di tempo, le informazioni sugli eventi rifiutati vengono scritte nel registro eventi Kaspersky. I nuovi eventi vengono accodati e quindi salvati nel database al termine dell'operazione di eliminazione.

Per limitare il numero di eventi che è possibile archiviare nell'archivio eventi di Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Archivio eventi**. Specificare il numero massimo di eventi archiviati nel database.

3. Fare clic sul pulsante **Salva**.

Inoltre, è possibile procedere come segue:

- Modificare le impostazioni di qualsiasi attività per salvare gli eventi relativi all'avanzamento dell'attività oppure salvare solo i risultati dell'esecuzione dell'attività.

- Ridurre o disabilitare il periodo di archiviazione per gli eventi delle applicazioni di Administration Server, Network Agent e Kaspersky installate nei dispositivi gestiti.

In tal modo si riduce il numero di eventi nel database, si aumenta la velocità di esecuzione degli scenari associati all'analisi della tabella degli eventi nel database e si limita il rischio che gli eventi critici vengano sovrascritti da un ampio numero di eventi.

Impostazioni di connessione dei dispositivi di protezione UEFI

Un *dispositivo di protezione UEFI* è un dispositivo con una soluzione Kaspersky per UEFI integrata al livello del BIOS. La protezione integrata garantisce la sicurezza del dispositivo fin dall'avvio del sistema, mentre la protezione nei dispositivi senza software integrato inizia solo dopo l'avvio dell'applicazione di protezione. Kaspersky Security Center supporta la gestione di tali dispositivi.

Per modificare le impostazioni di connessione dei dispositivi di protezione UEFI:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Porte aggiuntive**.

3. Modificare le impostazioni appropriate:

   - **Porta aperta per i dispositivi di protezione UEFI e i dispositivi KasperskyOS**

     I dispositivi di protezione UEFI possono connettersi all'Administration Server.

   - **Porta per i dispositivi di protezione UEFI e i dispositivi KasperskyOS**

     È possibile modificare il numero di porta se l'opzione **Porta aperta per i dispositivi di protezione UEFI e i dispositivi KasperskyOS** è abilitata. Il numero di porta predefinito è 13294.

4. Fare clic sul pulsante **Salva**.

I dispositivi di protezione UEFI ora possono connettersi all'Administration Server.

Creazione di una gerarchia di Administration Server: l'aggiunta un Administration Server secondario

Aggiunta di un Administration Server secondario (eseguita sul futuro Administration Server primario)

È possibile aggiungere un Administration Server come Administration Server secondario, configurando una gerarchia "primario/secondario".

Per aggiungere un Administration Server secondario disponibile per la connessione tramite Kaspersky Security Center Web Console:

1. Verificare che la porta 13000 del futuro Administration Server primario sia disponibile per la ricezione delle connessioni dagli Administration Server secondari.

2. Nel futuro Administration Server primario, fare clic sull'icona delle impostazioni ( ).

3. Nella pagina delle proprietà visualizzata, selezionare la scheda **Administration Server**.

4. Selezionare la casella di controllo accanto al nome del gruppo di amministrazione a cui si desidera aggiungere l'Administration Server.

5. Nella riga del menu fare clic su **Connetti Administration Server secondario**.

   Verrà avviata l'Aggiunta guidata Administration Server secondari. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

6. Compilare i seguenti campi:

- **Connetti l'Administration Server primario all'Administration Server secondario nella rete perimetrale**

  Selezionare questa opzione se l'Administration Server secondario si trova in una rete perimetrale (DMZ).

  Se questa opzione è selezionata, è necessario specificare il parametro **Indirizzo del server secondario**.

  Se questa opzione è selezionata, l'Administration Server primario avvia la connessione all'Administration Server secondario. In caso contrario, l'Administration Server secondario avvia una connessione con l'Administration Server primario.

- **Nome visualizzato dell'Administration Server secondario**

  Un nome con cui l'Administration Server secondario verrà visualizzato nella gerarchia. Se si desidera, è possibile immettere l'indirizzo IP come nome, oppure è possibile utilizzare un nome come "Server secondario per il gruppo 1".

- **Indirizzo dell'Administration Server secondario (facoltativo)**

  Specificare l'indirizzo IP o il nome di dominio dell'Administration Server secondario.

  Questo parametro è obbligatorio se l'opzione **Connetti l'Administration Server primario all'Administration Server secondario in DMZ** è abilitata.

- **Porta SSL Administration Server**

  Specificare il numero della porta SSL nell'Administration Server primario. Il numero di porta predefinito è 13000.

- **Porta API Administration Server**

  Specificare il numero della porta nell'Administration Server primario per la ricezione delle connessioni tramite OpenAPI. Il numero di porta predefinito è 13299.

7. Specificare il certificato dell'Administration Server secondario. Se è stato specificato il parametro **Indirizzo del server secondario**, è possibile fare clic sul pulsante **Ottieni da Administration Server secondario** per ottenere il certificato. In caso contrario, fare clic sul pulsante **Sfoglia il file del certificato** e individuare il file del certificato.

8. Specificare le impostazioni di connessione:

   - Immettere l'indirizzo del futuro Administration Server primario.

   - Se il futuro Administration Server secondario utilizza un server proxy, immettere l'indirizzo del server proxy e le credenziali dell'utente per connettersi al server proxy.

9. Immettere le credenziali dell'utente che dispone dei diritti di accesso sul futuro Administration Server secondario.

10. Se la verifica in due passaggi è abilitata e configurata, specificare il codice di sicurezza generato dall'app di autenticazione.

    Se la verifica in due passaggi è abilitata ma non configurata per l'account specificato, creare la gerarchia dal futuro server secondario (consultare le istruzioni di seguito).

Se le impostazioni di connessione sono corrette, viene stabilita la connessione con il futuro Administration Server secondario e viene costruita la gerarchia "primario/secondario". Se la connessione non è riuscita, verificare le impostazioni di connessione o specificare il certificato del futuro Administration Server secondario manualmente.

La connessione tra l'Administration Server primario e quello secondario viene stabilita tramite la porta 13000. Le attività e i criteri dall'Administration Server primario vengono ricevuti e applicati. L'Administration Server secondario viene visualizzato nell'Administration Server primario, nel gruppo di amministrazione a cui è stato aggiunto.

Aggiunta di un Administration Server secondario (eseguita sul futuro Administration Server secondario)

Se non è possibile connettersi al futuro Administration Server secondario (ad esempio, perché temporaneamente disconnesso o non disponibile), è comunque possibile aggiungere un Administration Server secondario.

Per aggiungere come secondario un Administration Server non disponibile per la connessione tramite Kaspersky Security Center Web Console:

1. Inviare il file del certificato del futuro Administration Server primario all'amministratore di sistema dell'ufficio in cui si trova il futuro Administration Server secondario. È ad esempio possibile scrivere il file su un dispositivo esterno, come un'unità flash, o inviarlo via e-mail.

   Il file di certificato è disponibile nel futuro Administration Server primario, in %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Richiedere all'amministratore di sistema responsabile del futuro Administration Server secondario di eseguire le seguenti operazioni:

   a. Fare clic sull'icona delle impostazioni ( ).

   b. Nella pagina delle proprietà visualizzata passare alla sezione **Gerarchia di Administration Server** della scheda **Generale**.

   c. Selezionare l'opzione **Questo Administration Server è secondario nella gerarchia**.

   d. Nel campo **Indirizzo Administration Server primario** immettere il nome della rete del futuro Administration Server primario.

   e. Selezionare il file precedentemente salvato con il certificato del futuro Administration Server primario facendo clic su **Sfoglia**.

   f. Se necessario, selezionare la casella di controllo **Connetti l'Administration Server primario all'Administration Server secondario nella rete perimetrale**.

   g. Se la connessione al futuro Administration Server secondario viene eseguita tramite un server proxy, selezionare l'opzione **Usa server proxy** e specificare le impostazioni di connessione.

   h. Fare clic su **Salva**.

Verrà creata la gerarchia "primario/secondario". L'Administration Server primario inizia a ricevere la connessione dall'Administration Server secondario tramite la porta 13000. Le attività e i criteri dall'Administration Server primario vengono ricevuti e applicati. L'Administration Server secondario viene visualizzato nell'Administration Server primario, nel gruppo di amministrazione a cui è stato aggiunto.

Visualizzazione dell'elenco degli Administration Server secondari

Per visualizzare l'elenco degli Administration Server secondari (inclusi quelli virtuali):

Nel menu principale, fare clic sul nome di Administration Server, accanto all'icona delle impostazioni ( ).

Viene visualizzato l'elenco a discesa degli Administration Server secondari (inclusi quelli virtuali).

È possibile passare a uno di questi Administration Server facendo clic sul relativo nome.

Vengono visualizzati anche i gruppi di amministrazione, che sono però disattivati e non disponibili per la gestione in questo menu.

Se si è connessi all'Administration Server primario in Kaspersky Security Center Web Console e non è possibile connettersi a un Administration Server virtuale gestito da un Administration Server secondario, è possibile utilizzare uno dei seguenti modi:

- **Modificare l'installazione esistente di Kaspersky Security Center Web Console per aggiungere il server secondario all'elenco degli Administration Server attendibili**. Sarà quindi possibile connettersi all'Administration Server virtuale in Kaspersky Security Center Web Console.

  1. Nel dispositivo in cui è installato Kaspersky Security Center Web Console, avviare il file di installazione ksc-web-console-<numero versione><numero build>.exe con un account con privilegi di amministratore.

     Verrà avviata l'Installazione guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

  2. Selezionare l'opzione **Upgrade**.

  3. Nel passaggio **Tipo di modifica** selezionare l'opzione **Modifica impostazioni di connessione**.

  4. Nel passaggio **Administration Server attendibili**, aggiungere l'Administration Server secondario richiesto.

  5. Nell'ultimo passaggio fare clic su **Modifica** per applicare le nuove impostazioni.

  6. Al termine della riconfigurazione dell'applicazione, fare clic sul pulsante **Fine**.

- Utilizzare Kaspersky Security Center Web Console per connettersi direttamente all'Administration Server secondario in cui è stato creato il server virtuale. Sarà quindi possibile passare all'Administration Server virtuale in Kaspersky Security Center Web Console.

- Utilizzare Administration Console basata su MMC per connettersi direttamente al server virtuale.

Eliminazione di una gerarchia di Administration Server

Se non si desidera più avere una gerarchia di Administration Server, è possibile disconnetterli da tale gerarchia.

Per eliminare una gerarchia di Administration Server:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server primario.

2. Nella pagina visualizzata passare alla scheda **Administration Server**.

3. Nel gruppo di amministrazione da cui si desidera eliminare l'Administration Server secondario selezionare l'Administration Server secondario.

4. Nella riga del menu fare clic su **Elimina**.

5. Nella finestra di dialogo visualizzata fare clic su **OK** per confermare che si desidera eliminare l'Administration Server secondario.

I precedenti Administration Server primario e secondario sono ora indipendenti l'uno dall'altro. La gerarchia non è più presente.

Manutenzione di Administration Server

La manutenzione di Administration Server consente di liberare spazio nella cartella di Administration Server e ridurre il volume del database eliminando gli oggetti non più necessari. Ciò consente di migliorare le prestazioni e l'affidabilità operativa dell'applicazione. È consigliabile eseguire la manutenzione di Administration Server almeno ogni settimana.

La manutenzione di Administration Server viene eseguita tramite un'attività specializzata. Durante la manutenzione di Administration Server, l'applicazione esegue le azioni seguenti:

- Elimina le cartelle e i file non necessari dalla cartella di archiviazione.
- Elimina i record non necessari dalle tabelle (noti anche come "puntatori pendenti").
- Cancella la cache.
- Esegue la manutenzione del database (se si utilizza SQL Server o PostgreSQL come DBMS):
  - Verifica la presenza di errori nel database (disponibile solo per SQL Server).
  - Riorganizza gli indici del database.
  - Aggiorna le statistiche del database.
  - Riduce le dimensioni del database (se necessario).

L'attività di Manutenzione di Administration Server viene creata automaticamente durante l'installazione di Kaspersky Security Center. Se l'attività di Manutenzione di Administration Server viene eliminata, è possibile crearla manualmente.

Per creare l'attività di Manutenzione di Administration Server:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nella finestra **Impostazioni nuova attività** della procedura guidata selezionare **Manutenzione di Administration Server** come tipo di attività e fare clic su **Avanti**.
4. Seguire le rimanenti istruzioni della procedura guidata.

La nuova attività creata verrà visualizzata nell'elenco delle attività. Una sola attività di Manutenzione di Administration Server può essere in esecuzione per un singolo Administration Server. Se è stata già creata l'attività di Manutenzione di Administration Server per un Administration Server, non può essere creata alcuna nuova attività di Manutenzione di Administration Server.

Configurazione dell'interfaccia

È possibile configurare l'interfaccia di Kaspersky Security Center Web Console in modo da visualizzare e nascondere sezioni ed elementi di interfaccia, a seconda delle funzionalità utilizzate.

Per configurare l'interfaccia di Kaspersky Security Center Web Console in base al set di funzionalità utilizzate al momento:

1. Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Opzioni di interfaccia**.
2. Nella finestra **Opzioni di interfaccia** visualizzata abilitare o disabilitare le opzioni richieste.
3. Fare clic su **Salva**.

Successivamente, la console visualizza le sezioni nel menu principale in base alle opzioni abilitate. Ad esempio, se si abilita **Mostra avvisi EDR**, nel menu principale viene visualizzata la sezione **Monitoraggio e generazione dei rapporti → Avvisi**.

Gestione di Administration Server virtuali

Questa sezione descrive le seguenti azioni per gestire Administration Server virtuali:

- Creare Administration Server virtuali
- Abilitare e disabilitare Administration Server virtuali
- Assegnare un amministratore per un Administration Server virtuale
- Modificare Administration Server per i dispositivi client
- Eliminare Administration Server virtuali

Creazione di un Administration Server virtuale

È possibile creare Administration Server virtuali e aggiungerli ai gruppi di amministrazione.

Quando si crea un Administration Server virtuale, eredita l'elenco di utenti e tutti i diritti utente dell'Administration Server primario. Se un utente dispone dei diritti di accesso al server primario, ha anche i diritti di accesso al server virtuale. Dopo la creazione, si configurano i diritti di accesso ai server in modo indipendente.

Per creare e aggiungere un Administration Server virtuale:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.
2. Nella pagina visualizzata passare alla scheda **Administration Server**.

3. Selezionare il gruppo di amministrazione a cui si desidera aggiungere un Administration Server virtuale. L'Administration Server virtuale gestirà i dispositivi del gruppo selezionato (compresi i sottogruppi).

4. Nella riga del menu fare clic su **Nuovo Administration Server virtuale**.

5. Nella pagina visualizzata definire le proprietà del nuovo Administration Server virtuale:

   - **Nome Administration Server virtuale**.
   - **Indirizzo connessione Administration Server**

     È possibile specificare il nome o l'indirizzo IP di Administration Server.

6. Nell'elenco degli utenti selezionare l'amministratore dell'Administration Server virtuale. Se si desidera, è possibile modificare uno degli account esistenti prima di assegnargli il ruolo di amministratore o creare un nuovo account utente.

7. Fare clic su **Salva**.

Il nuovo Administration Server virtuale verrà creato, aggiunto al gruppo di amministrazione e visualizzato nella scheda **Administration Server**.

Se si è connessi all'Administration Server primario in Kaspersky Security Center Web Console e non è possibile connettersi a un Administration Server virtuale gestito da un Administration Server secondario, è possibile utilizzare uno dei seguenti modi:

- Modificare l'installazione esistente di Kaspersky Security Center Web Console per aggiungere il server secondario all'elenco degli Administration Server attendibili. Sarà quindi possibile connettersi all'Administration Server virtuale in Kaspersky Security Center Web Console.

  1. Nel dispositivo in cui è installato Kaspersky Security Center Web Console, avviare il file di installazione ksc-web-console-<numero versione><numero build>.exe con un account con privilegi di amministratore.

     Verrà avviata l'Installazione guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

  2. Selezionare l'opzione **Upgrade**.

  3. Nel passaggio **Tipo di modifica** selezionare l'opzione **Modifica impostazioni di connessione**.

  4. Nel passaggio **Administration Server attendibili**, aggiungere l'Administration Server secondario richiesto.

  5. Nell'ultimo passaggio fare clic su **Modifica** per applicare le nuove impostazioni.

  6. Al termine della riconfigurazione dell'applicazione, fare clic sul pulsante **Fine**.

- Utilizzare Kaspersky Security Center Web Console per connettersi direttamente all'Administration Server secondario in cui è stato creato il server virtuale. Sarà quindi possibile passare all'Administration Server virtuale in Kaspersky Security Center Web Console.

- Utilizzare Administration Console basata su MMC per connettersi direttamente al server virtuale.

Abilitazione e disabilitazione di un Administration Server virtuale

Quando si crea un nuovo Administration Server virtuale, questo viene abilitato per impostazione predefinita. È possibile disabilitarlo o abilitarlo nuovamente in qualsiasi momento. La disabilitazione o l'abilitazione di un Administration Server virtuale equivale alla disattivazione o all'attivazione di un Administration Server fisico.

Per abilitare o disabilitare un Administration Server virtuale:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.
2. Nella pagina visualizzata passare alla scheda **Administration Server**.
3. Selezionare l'Administration Server virtuale che si desidera abilitare o disabilitare.
4. Nella riga del menu fare clic sul pulsante **Abilita/disabilita l'Administration Server virtuale**.

   Lo stato dell'Administration Server virtuale viene modificato in abilitato o disabilitato, a seconda del suo stato precedente. Viene visualizzato lo stato aggiornato accanto al nome dell'Administration Server.

Assegnazione di un amministratore per un Administration Server virtuale

Quando si utilizzano Administration Server virtuali nell'organizzazione, è consigliabile assegnare un amministratore dedicato per ciascun Administration Server virtuale. Questo potrebbe ad esempio essere utile quando si creano Administration Server virtuali per gestire uffici o reparti separati della propria organizzazione oppure se si è un provider MSP e si gestiscono i tenant tramite Administration Server virtuali.

Quando si crea un Administration Server virtuale, eredita l'elenco di utenti e tutti i diritti utente dell'Administration Server primario. Se un utente dispone dei diritti di accesso al server primario, ha anche i diritti di accesso al server virtuale. Dopo la creazione, si configurano i diritti di accesso ai server in modo indipendente. Se si desidera assegnare un amministratore solo per un Administration Server virtuale, accertarsi che l'amministratore non disponga dei diritti di accesso nell'Administration Server primario.

Si assegna un amministratore per un Administration Server virtuale concedendo all'amministratore i diritti di accesso all'Administration Server virtuale. È possibile concedere i diritti di accesso necessari in uno dei seguenti modi:

- Configurare manualmente i diritti di accesso per l'amministratore
- Assegnare uno o più ruoli utente per l'amministratore

Per accedere a Kaspersky Security Center Web Console, un amministratore di un Administration Server virtuale specifica il nome, il nome utente e la password dell'Administration Server virtuale. Kaspersky Security Center Web Console autentica l'amministratore e apre l'Administration Server virtuale per il quale l'amministratore dispone dei diritti di accesso. L'amministratore non può passare da un Administration Server all'altro.

Prerequisiti

Prima di iniziare, assicurarsi che vengano soddisfatte le seguenti condizioni:

- L'Administration Server virtuale è stato creato.
- Nell'Administration Server primario è stato creato un account per l'amministratore che si desidera assegnare per l'Administration Server virtuale.
- L'utente dispone del diritto **Modifica elenchi di controllo degli accessi agli oggetti** nell'area funzionale **Caratteristiche generali → Autorizzazioni utente**.

Configurazione manuale dei diritti di accesso

Per assegnare un amministratore per un Administration Server virtuale:

1. Nella menu principale, passare all'Administration Server virtuale desiderato:
   a. Fare clic sull'icona a forma di freccia di espansione (›) a destra del nome corrente dell'Administration Server.
   b. Selezionare l'Administration Server desiderato.
2. Nel menu principale, fare clic sull'icona delle impostazioni (⚙) accanto al nome di Administration Server.
   Verrà visualizzata la finestra delle proprietà di Administration Server.
3. Nella scheda **Diritti di accesso**, fare clic sul pulsante **Aggiungi**.
   Viene visualizzato un elenco unificato di utenti dell'Administration Server primario e dell'Administration Server virtuale corrente.
4. Nell'elenco di utenti selezionare l'account dell'amministratore che si desidera assegnare per l'Administration Server virtuale, quindi fare clic sul pulsante **OK**.
   L'applicazione aggiunge l'utente selezionato all'elenco utenti nella scheda **Diritti di accesso**.
5. Selezionare la casella di controllo accanto all'account aggiunto, quindi fare clic sul pulsante **Diritti di accesso**.
6. Configurare i diritti che l'amministratore avrà sull'Administration Server virtuale.
   Per fare in modo che l'autenticazione vada a buon fine, l'amministratore deve disporre almeno dei seguenti diritti:
   - Diritto **Lettura** nell'area funzionale **Caratteristiche generali → Funzionalità di base**
   - Diritto **Lettura** nell'area funzionale **Caratteristiche generali → Administration Server virtuali**

L'applicazione salva i diritti utente modificati nell'account amministratore.

Configurazione dei diritti di accesso assegnando ruoli utente

In alternativa, è possibile concedere i diritti di accesso a un amministratore dell'Administration Server virtuale tramite i ruoli utente. Questo potrebbe ad esempio essere utile se si desidera assegnare più amministratori nello stesso Administration Server virtuale. In tal caso, è possibile assegnare agli account degli amministratori gli stessi ruoli utente (uno o più di questi) anziché configurare gli stessi diritti utente per più amministratori.

Per assegnare un amministratore a un Administration Server virtuale assegnando ruoli utente:

1. Nell'Administration Server primario creare un nuovo ruolo utente, quindi specificare tutti i diritti di accesso necessari di cui un amministratore deve disporre nell'Administration Server virtuale. È possibile creare più ruoli, ad esempio, se si desidera separare l'accesso a diverse aree funzionali.

2. Nella menu principale, passare all'Administration Server virtuale desiderato:

   a. Fare clic sull'icona a forma di freccia di espansione (›) a destra del nome corrente dell'Administration Server.

   b. Selezionare l'Administration Server desiderato.

3. Assegnare il nuovo ruolo o diversi ruoli all'account amministratore.

L'applicazione assegna i ruoli all'account amministratore.

Configurazione dei diritti di accesso a livello di oggetto

Oltre ad assegnare diritti di accesso a livello di area funzionale, è possibile configurare l'accesso a oggetti specifici nell'Administration Server virtuale, ad esempio, a un gruppo di amministrazione specifico o a un'attività. A tale scopo, passare all'Administration Server virtuale, quindi configurare i diritti di accesso nelle proprietà dell'oggetto.

Modifica di Administration Server per i dispositivi client

È possibile sostituire l'Administration Server che gestisce i dispositivi client con un altro server mediante l'attività *Cambia Administration Server*. Dopo il completamento dell'attività, i dispositivi client selezionati passeranno sotto la gestione dell'Administration Server specificato.

> Non è possibile utilizzare l'attività *Cambia Administration Server* per i dispositivi client connessi ad Administration Server tramite gateway di connessione. Per tali dispositivi è necessario riconfigurare Network Agent o reinstallarlo e specificare il gateway di connessione.

Per sostituire l'Administration Server che gestisce i dispositivi client con un altro server:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nel passaggio **Impostazioni nuova attività**, specificare le seguenti impostazioni:

   a. Nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Security Center**.

   b. Nel campo **Tipo di attività**, selezionare **Cambia Administration Server**.

   c. Nel campo **Nome attività**, specificare il nome dell'attività che si intende creare.

      Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

   d. Selezionare i dispositivi a cui assegnare l'attività:

   - **Assegna attività a un gruppo di amministrazione**

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

     Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

   - **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**

     È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

   - **Assegna attività a una selezione dispositivi**

     L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

4. Nel passaggio **Ambito dell'attività** della procedura guidata, specificare un gruppo di amministrazione, dispositivi con indirizzi specifici o una selezione di dispositivi.

5. In questo passaggio della procedura guidata, confermare di accettare i termini di modifica di Administration Server per i dispositivi client.

6. In questo passaggio della procedura guidata, selezionare l'Administration Server che si desidera utilizzare per gestire i dispositivi selezionati:

- **Passa a un altro Administration Server primario**

  Per spostare i dispositivi client su un altro Administration Server primario, specificare le seguenti impostazioni di connessione dell'Administration Server:

  1. Nel campo **Indirizzo di Administration Server**, specificare l'indirizzo del nuovo Administration Server primario.
  2. Nel campo **Numero di porta**, specificare il numero di porta per connettersi all'Administration Server.

     Il numero di porta predefinito è 14000.
  3. Nel campo **Porta SSL**, specificare il numero della porta SSL nell'Administration Server primario.

     Il numero di porta predefinito è 13000.
  4. Se necessario, abilitare l'opzione **Usa server proxy**.

     Se questa opzione è disabilitata, viene utilizzata la connessione diretta per connettere il dispositivo all'Administration Server.

     Se questa opzione è abilitata, specificare i parametri del server proxy:

     - **Indirizzo server proxy**
     - **Porta server proxy**

     Se il server proxy richiede l'autenticazione, nei campi **Nome utente** e **Password** specificare le credenziali dell'account con cui viene stabilita la connessione al server proxy. È consigliabile specificare le credenziali di un account con i privilegi minimi richiesti solo per l'autenticazione del server proxy.
  5. Se necessario, caricare un nuovo certificato di Administration Server.

- **Passa a un altro server virtuale in questo server primario**

  Selezionare questa opzione per spostare i dispositivi client sull'Administration Server virtuale sull'Administration Server primario corrente. A tale scopo, nell'elenco a discesa **Nome Administration Server virtuale**, selezionare l'Administration Server virtuale necessario.

7. Nel passaggio **Selezione di un account per l'esecuzione dell'attività** della procedura guidata, specificare le impostazioni dell'account:

   - **Account predefinito**

     L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Specifica account**

     Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

     - **Account**

       Account tramite il quale viene eseguita l'attività.

     - **Password**

       Password dell'account con cui verrà eseguita l'attività.

8. Se si desidera modificare le impostazioni predefinite dell'attività, nella fase **Completare la creazione dell'attività** della procedura guidata, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione**.

   Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

9. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.

10. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

11. Se si desidera modificare le impostazioni predefinite dell'attività, nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

12. Fare clic sul pulsante **Salva**.

    L'attività verrà creata e configurata.

13. Eseguire l'attività creata.

Dopo il completamento dell'attività, i dispositivi client per cui è stata creata passano sotto la gestione dell'Administration Server specificato nelle impostazioni dell'attività.

Eliminazione di un Administration Server virtuale

Quando si elimina un Administration Server virtuale, verranno eliminati anche tutti gli oggetti creati nell'Administration Server, inclusi criteri e attività. I dispositivi gestiti dei gruppi di amministrazione che erano gestiti dall'Administration Server virtuale verranno rimossi dai gruppi di amministrazione. Per far tornare i dispositivi sotto la gestione di Kaspersky Security Center, eseguire il polling di rete, quindi spostare i dispositivi rilevati dal gruppo Dispositivi non assegnati ai gruppi di amministrazione.

Per eliminare un Administration Server virtuale:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome di Administration Server.
2. Nella pagina visualizzata passare alla scheda **Administration Server**.
3. Selezionare l'Administration Server virtuale che si desidera eliminare.
4. Nella riga del menu fare clic sul pulsante **Elimina**.

L'Administration Server virtuale viene eliminato.

Abilitazione della protezione dell'account dalle modifiche non autorizzate

È possibile abilitare un'opzione aggiuntiva per proteggere un account utente dalle modifiche non autorizzate. Se questa opzione è abilitata, la modifica delle impostazioni dell'account utente richiede l'autorizzazione dell'utente con i diritti di modifica.

Per abilitare o disabilitare la protezione dell'account dalle modifiche non autorizzate:

1. Nel menu principale accedere a **Utenti e ruoli** → **Utenti**.
2. Fare clic sul nome dell'account utente interno per cui specificare la protezione dell'account dalle modifiche non autorizzate.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Protezione account**.
4. Nella scheda **Protezione account** selezionare l'opzione **Richiedi l'autenticazione per verificare l'autorizzazione di modifica degli account utente** se si desidera richiedere le credenziali ogni volta che le impostazioni dell'account vengono modificate. In caso contrario, selezionare l'opzione **Consentire agli utenti di modificare questo account senza autenticazione aggiuntiva**.
5. Fare clic sul pulsante **Salva**.

La protezione dell'account da modifiche non autorizzate è abilitata per un account utente.

Backup e ripristino dei dati di Administration Server

Il backup dei dati consente di spostare un Administration Server da un dispositivo all'altro senza perdite di dati. Tramite il backup, è possibile ripristinare i dati quando si sposta il database di Administration Server su un altro dispositivo o quando si esegue l'aggiornamento a una versione più recente di Kaspersky Security Center. Inoltre, è possibile utilizzare il backup dei dati per spostare i dati di Administration Server da Kaspersky Security Center Windows sotto la gestione di Kaspersky Security Center Linux (lo spostamento dei dati da Kaspersky Security Center Linux a Kaspersky Security Center Windows non è supportato).

Non viene eseguito il backup dei plug-in di gestione installati. Dopo aver ripristinato i dati di Administration Server da una copia di backup, è necessario scaricare e reinstallare i plug-in per le applicazioni gestite.

Prima di eseguire il backup dei dati di Administration Server, verificare se al gruppo di amministrazione è stato aggiunto un Administration Server virtuale. Se viene aggiunto un Administration Server virtuale, assicurarsi che a questo Administration Server virtuale sia assegnato un amministratore prima del backup. Non è possibile concedere all'amministratore i diritti di accesso all'Administration Server virtuale dopo il backup. Tenere presente che se le credenziali dell'account amministratore vengono smarrite, non sarà possibile assegnare un nuovo amministratore all'Administration Server virtuale.

Per eseguire il backup o il ripristino di un cluster di failover di Kaspersky Security Center, è necessario arrestare l'intero cluster per la manutenzione e quindi riavviarlo al termine del backup o del ripristino.

È possibile creare una copia di backup dei dati di Administration Server in uno dei seguenti modi:

- Creando ed eseguendo un'attività di backup dei dati tramite Administration Console.
- Eseguendo l'utilità klbackup nel dispositivo in cui è installato Administration Server. Questa utilità è inclusa nel kit di distribuzione di Kaspersky Security Center. Dopo l'installazione di Administration Server, l'utilità è disponibile nella radice della cartella di destinazione specificata durante l'installazione dell'applicazione.

I seguenti dati vengono salvati nella copia di backup di Administration Server:

- Database di Administration Server (criteri, attività, impostazioni delle applicazioni, eventi salvati in Administration Server).
- Dettagli sulla configurazione della struttura dei gruppi di amministrazione e dei dispositivi client.
- Archivio dei pacchetti di distribuzione delle applicazioni per l'installazione remota.
- Certificato di Administration Server.
- Contenuto della cartella *Updates*.

  Per impostazione predefinita, il percorso della cartella è C:\ProgramData\KasperskyLab\adminkit\1093\.working\share\Updates\

Il ripristino dei dati di Administration Server è possibile solo tramite l'utilità klbackup. È necessario eseguire Il ripristino di un'istanza funzionante di Administration Server che è stata appena installata e con la stessa versione (o una versione successiva) di quella per cui è stata creata la copia di backup.

Creazione di un'attività di backup dei dati

Le attività di backup sono attività di Administration Server, create tramite l'Avvio rapido guidato. Se un'attività di backup creata dall'Avvio rapido guidato è stata eliminata, è possibile crearne una manualmente.

Per creare un'attività di backup dei dati di Administration Server:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nella finestra **Impostazioni nuova attività** della procedura guidata selezionare il tipo di attività **Backup dei dati di Administration Server**.
4. Seguire le rimanenti istruzioni della procedura guidata.

L'attività **Backup dei dati di Administration Server** può essere creata solo in una singola copia. Se l'attività di backup dei dati di Administration Server è stata già creata per l'Administration Server, non viene visualizzata nella finestra di selezione del tipo di attività della Creazione guidata attività di backup di Administration Server.

Per configurare l'attività Backup dei dati di Administration Server:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Attività** e selezionare l'attività **Backup dei dati di Administration Server**.
2. Fare clic sull'attività **Backup dei dati di Administration Server**.

   Verrà visualizzata la finestra delle proprietà dell'attività.
3. Se necessario, specificare le impostazioni generali dell'attività in base alle proprie esigenze.

4. Nella sezione **Impostazioni applicazione**, specificare il percorso della cartella per l'archiviazione delle copie di backup dei dati di Administration Server, impostare la password di protezione del backup e il numero di copie di backup, se necessario.

5. Fare clic su **Salva** per applicare le modifiche.

L'attività *Backup dei dati di Administration Server* è configurata.

Spostamento di Administration Server in un altro dispositivo

Se è necessario utilizzare Administration Server in un nuovo dispositivo, è possibile spostarlo in uno dei seguenti modi:

- Spostare Administration Server e il server di database in un nuovo dispositivo (il server di database può essere installato nel nuovo dispositivo insieme ad Administration Server o in un altro dispositivo).
- Mantenere il server di database nel dispositivo precedente e spostare solo Administration Server in un nuovo dispositivo.

Per spostare Administration Server e il server di database in un nuovo dispositivo:

1. Nel dispositivo precedente creare un backup dei dati di Administration Server.

   A tale scopo è possibile eseguire l'attività di backup dei dati tramite Kaspersky Security Center Web Console o eseguire l'utilità klbackup.

   Se si utilizza SQL Server come DBMS per Administration Server, è possibile migrare i dati da SQL Server al DBMS di MySQL o MariaDB. A tale scopo, eseguire l'utilità klbackup in modalità interattiva per creare un backup dei dati. Abilitare l'opzione **Esegui la migrazione al formato MySQL/MariaDB** nella finestra **Impostazioni backup** della procedura guidata di backup e ripristino. Kaspersky Security Center creerà un backup compatibile con MySQL e MariaDB. Successivamente, è possibile ripristinare i dati dal backup in MySQL o MariaDB.

   È inoltre possibile abilitare l'opzione **Esegui la migrazione al formato Azure** se si desidera migrare i dati da SQL Server al DBMS di Azure SQL.

2. Nel dispositivo precedente, disconnettere Administration Server dalla rete.

3. Selezionare un nuovo dispositivo in cui installare Administration Server. Assicurarsi che l'hardware e il software nel dispositivo selezionato soddisfino i requisiti per Administration Server, Kaspersky Security Center Web Console e Network Agent. Controllare inoltre che le porte utilizzate in Administration Server siano disponibili.

4. Assegnare lo stesso indirizzo al nuovo dispositivo.

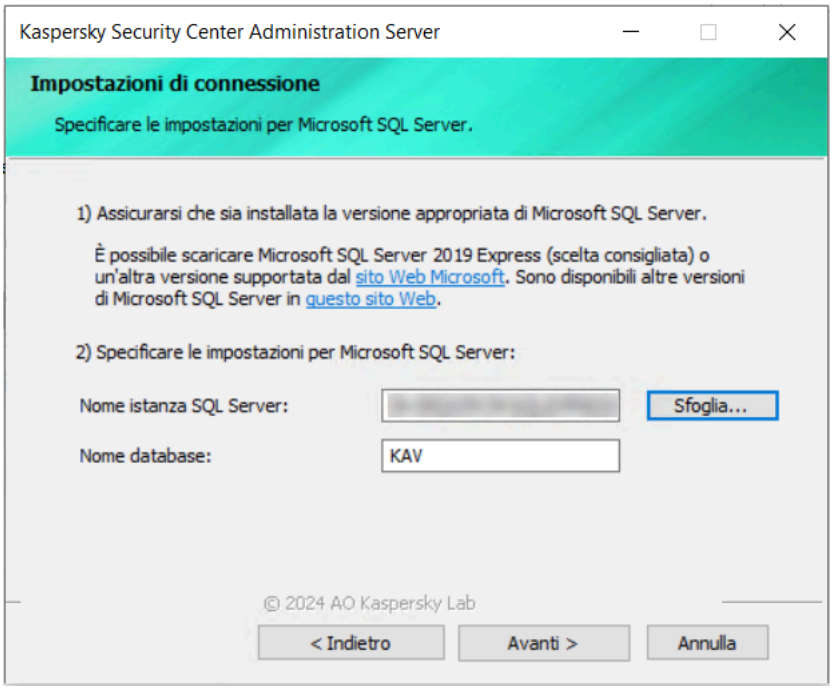
   È possibile assegnare al nuovo Administration Server il nome NetBIOS, l'FQDN e l'indirizzo IP statico. Dipende dall'indirizzo di Administration Server impostato nel pacchetto di installazione di Network Agent al momento della distribuzione dei Network Agent. In alternativa, è possibile utilizzare l'indirizzo di connessione che determina l'Administration Server a cui Network Agent si connette (è possibile ottenere questo indirizzo nei dispositivi gestiti utilizzando l'utilità klnagchk).

5. Se nececessario, in un altro dispositivo installare il sistema di gestione database (DBMS) che verrà utilizzato da Administration Server.

   Il database può essere installato nel nuovo dispositivo insieme ad Administration Server o in un altro dispositivo. Verificare che questo dispositivo soddisfi i requisiti hardware e software. Quando si seleziona un DBMS, tenere in considerazione il numero di dispositivi coperti da Administration Server.

6. Eseguire l'installazione dell'Administration Server nel nuovo dispositivo.

7. Durante l'installazione dell'Administration Server, configurare le impostazioni di connessione al server di database.



Esempio della finestra Impostazioni di connessione per Microsoft SQL Server

A seconda di dove è necessario individuare il server del database, eseguire una delle seguenti operazioni:

- Mantenimento del server del database nel dispositivo precedente

  1. Fare clic sul pulsante **Sfoglia** accanto al campo **Nome istanza SQL Server**, quindi selezionare il nome del dispositivo precedente nell'elenco visualizzato.

     Si noti che il dispositivo precedente deve essere disponibile per la connessione con il nuovo Administration Server.

  2. Immettere il nome del database precedente nel campo **Nome database**.

- Spostare il server del database in un altro dispositivo

  1. Fare clic sul pulsante **Sfoglia** accanto al campo **Nome istanza SQL Server**, quindi selezionare il nome del dispositivo nell'elenco visualizzato.

  2. Immettere il nuovo nome nel campo **Nome database**.

     Si noti che il nuovo nome del database deve corrispondere al nome del database del dispositivo precedente. I nomi dei database devono essere identici, in modo da poter utilizzare il backup di Administration Server. Il nome predefinito del database è *KAV*.

8. Al termine dell'installazione ripristinare i dati di Administration Server nel nuovo dispositivo utilizzando l'utilità klbackup.

   Se si utilizza SQL Server come DBMS nei dispositivi precedenti e nuovi, tenere presente che la versione di SQL Server installata nel nuovo dispositivo deve essere uguale o successiva alla versione di SQL Server installata nel dispositivo precedente. In caso contrario non è possibile recuperare i dati di Administration Server nel nuovo dispositivo.

9. Aprire Kaspersky Security Center Web Console e connettersi ad Administration Server.
10. Verificare che tutti i dispositivi gestiti vengano collegati ad Administration Server.
11. Disinstallare Administration Server e il server del database dal dispositivo precedente.

È inoltre possibile utilizzare Administration Console per spostare Administration Server e il server di un database in un altro dispositivo.

Controllo dell'integrità dei moduli mediante le utilità klscmodchk e integrity_checker

Kaspersky Security Center contiene più moduli binari sotto forma di librerie collegate dinamicamente, file eseguibili, file di configurazione e file di interfaccia. Gli intrusi possono sostituire uno o più moduli eseguibili o file applicativi con altri file contenenti codice dannoso. Per impedire la sostituzione di moduli e file, Kaspersky Security Center esegue un controllo dell'integrità dei componenti utilizzando le utilità klscmodchk e integrity_checker. Queste utilità controllano i moduli e i file per individuare eventuali modifiche non autorizzate o danni. Se un modulo o un file applicativo ha un checksum errato, viene considerato danneggiato.

L'utilità klscmodchk esegue controlli di integrità per i seguenti componenti di Kaspersky Security Center:

- Administration Server
- Network Agent
- Plug-in di gestione per l'Administration Console con file manifest

L'utilità integrity_checker esegue controlli di integrità per i seguenti componenti di Kaspersky Security Center:

- Administration Server
- Network Agent
- Kaspersky Security Center Web Console

Entrambe le utilità verificano l'integrità del modulo in base al file manifest kl_file_integrity_manifest.xml, che fa parte della build di Kaspersky Security Center e si trova nella cartella di installazione. Il file manifest del componente contiene file la cui integrità è importante per il corretto funzionamento del contenitore Kaspersky Security Center. Viene verificata anche l'integrità dei file manifest stessi.

Si sconsiglia vivamente di modificare il file manifest kl_file_integrity_manifest.xml, poiché ciò invaliderebbe la firma digitale e causerebbe la mancata riuscita del controllo di integrità.

Per verificare l'integrità del componente Kaspersky Security Center, eseguire uno dei seguenti comandi:

- `$ klscmodchk [ parametri ]`

  L'utilità klscmodchk avvia l'utilità integrity_checker con il parametro `--verbose` e controlla l'integrità dei moduli.

  Parametri per l'utilità klscmodchk:

  - `-logfile <log_file_path>`: specifica il percorso di un file sul disco per la registrazione. Per impostazione predefinita, le informazioni vengono inviate alla console.
  - `-chkplugins`: controlla l'integrità dei moduli plug-in di gestione installati per Administration Console che includono i file manifest. Per impostazione predefinita, i plug-in di gestione non sono selezionati.
  - `-verbose`: fornisce informazioni estese durante il controllo di integrità.

- `$ integrity_checker [ parametri ] percorso_file_manifest>`

  Parametri per l'utilità integrity_checker:

  - `--help`: mostra la guida dell'utilità integrity_checker.
  - `--version`: mostra la versione dell'utilità integrity_checker.
  - `--verbose`: mostra informazioni sul funzionamento dell'operatore dell'utilità. Quando si esegue un controllo di integrità, è sufficiente utilizzare questo parametro nel comando.

Il risultato del controllo di ogni file manifest viene visualizzato accanto al nome del file manifest nel seguente formato:

- RIUSCITO: integrità del file confermata (codice di ritorno 0).
- NON RIUSCITO: integrità del file non confermata (codice di ritorno diverso da zero).

È inoltre possibile configurare i controlli di integrità per l'avvio automatico all'avvio dell'applicazione. Per impostazione predefinita, il controllo automatico dell'integrità è disabilitato.

Per abilitare il controllo automatico dell'integrità:

1. Sul dispositivo in cui è installato l'Administration Server, al prompt dei comandi di Windows, immettere il seguente comando:

   ```
   klscflag.exe -fset -pv klserver -n KLMODCHK_ENABLE_CHECKING -t d -v 1
   ```

2. Riavvia il dispositivo.

Il controllo automatico dell'integrità viene abilitato.

Al successivo avvio di Kaspersky Security Center, l'utilità klscmodchk verrà eseguita insieme ad Administration Server e avvierà il controllo dell'integrità dei moduli. Il risultato dei controlli di integrità viene scritto nel Registro eventi Kaspersky.

Configurazione iniziale di Kaspersky Security Center Web Console

Questa sezione descrive le operazioni che è necessario eseguire dopo l'installazione di Kaspersky Security Center Web Console per eseguire la configurazione iniziale.

Avvio rapido guidato (Kaspersky Security Center Web Console)

Questa sezione fornisce informazioni su Avvio rapido guidato di Administration Server.

> La procedura guidata richiede l'accesso a Internet. Se Administration Server non dispone dell'accesso a Internet, è consigliabile eseguire manualmente tutti i passaggi della procedura guidata tramite l'interfaccia di Kaspersky Security Center Web Console.

Kaspersky Security Center consente di regolare una selezione minima di impostazioni necessarie per creare un sistema centralizzato di gestione per la protezione della rete dalle minacce per la sicurezza. Questa configurazione viene eseguita tramite l'Avvio rapido guidato. Quando la procedura guidata è in esecuzione, è possibile apportare le seguenti modifiche all'applicazione:

- Aggiungere file chiave o immettere codici di attivazione che è possibile distribuire automaticamente ai dispositivi nei gruppi di amministrazione.
- Configurare l'interazione con Kaspersky Security Network (KSN). Se è stato consentito l'utilizzo di KSN, la procedura guidata abilita il servizio del server proxy KSN, che assicura la connessione tra KSN e i dispositivi.
- Impostare l'invio di notifiche tramite e-mail per informare degli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni gestite (per il corretto invio delle notifiche, il servizio Messenger deve essere in esecuzione in Administration Server e in tutti i dispositivi dei destinatari).
- Creare un criterio di protezione per workstation e server, nonché attività di scansione malware, attività di download degli aggiornamenti e attività di backup dei dati, per il livello superiore della gerarchia dei dispositivi gestiti.

  > L'Avvio rapido guidato crea criteri soltanto per le applicazioni per cui non sono presenti criteri nella cartella **Dispositivi gestiti**. L'Avvio rapido guidato non crea attività se sono già state create attività con lo stesso nome per il livello superiore della gerarchia dei dispositivi gestiti.

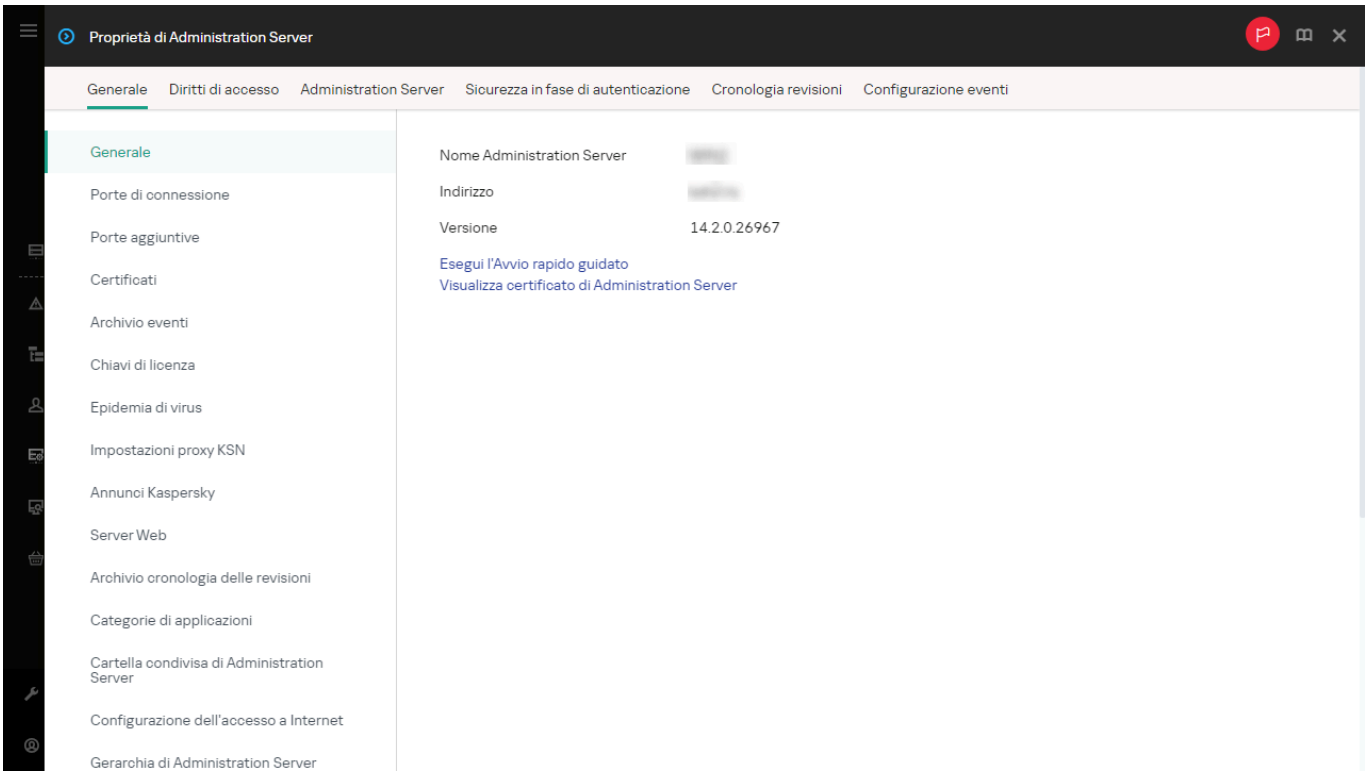
L'applicazione richiede automaticamente di eseguire l'Avvio rapido guidato dopo l'installazione di Administration Server, al momento della prima connessione. È anche possibile avviare manualmente l'avvio rapido guidato in qualsiasi momento.

Per avviare manualmente l'avvio rapido guidato:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome di Administration Server.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Generale**.



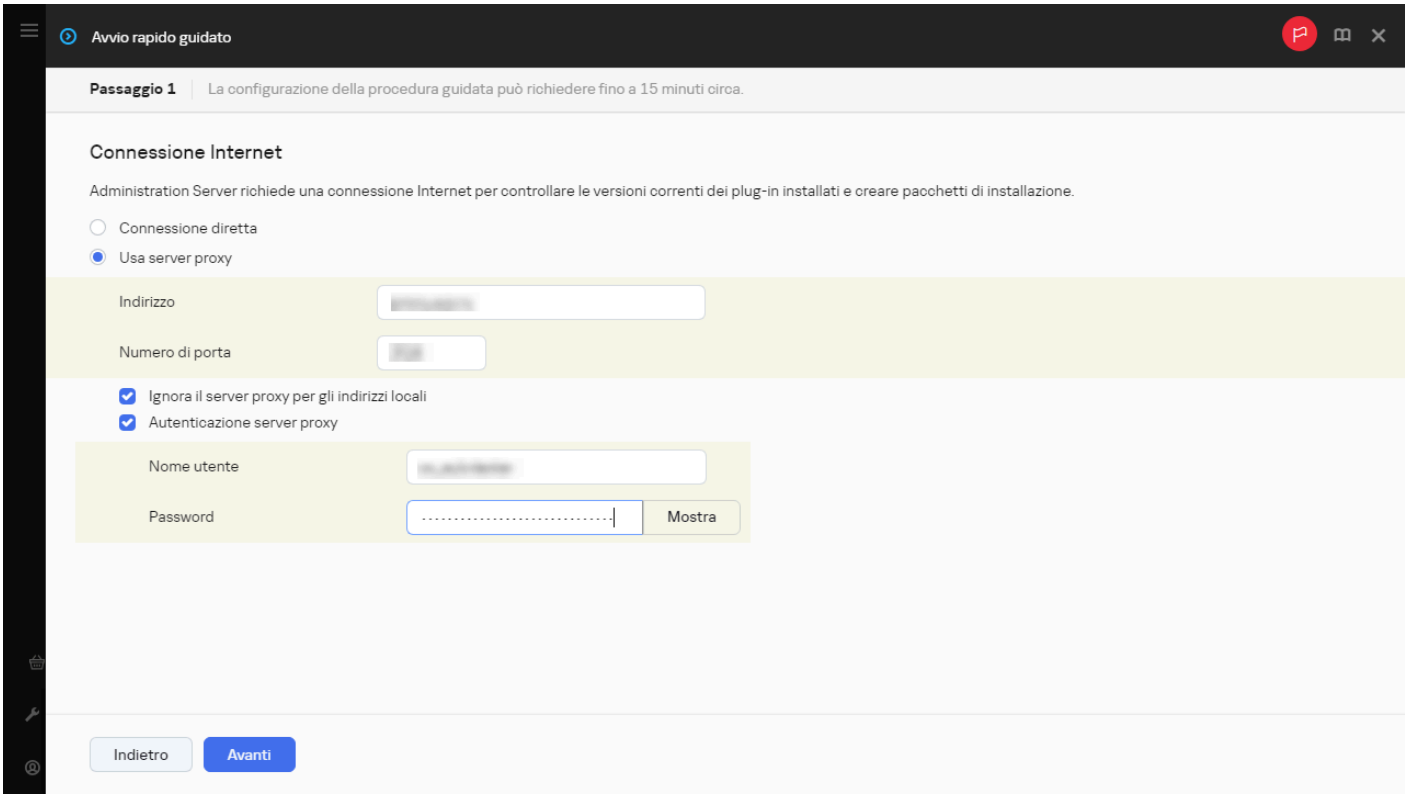
Finestra delle proprietà di Administration Server

3. Fare clic su **Esegui l'Avvio rapido guidato**.

Verrà offerta la possibilità di eseguire la configurazione iniziale di Administration Server. Seguire le istruzioni della procedura guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

Passaggio 1. Definizione delle impostazioni della connessione Internet

Specificare le impostazioni di accesso a Internet per Administration Server. È necessario configurare l'accesso a Internet per utilizzare Kaspersky Security Network e per scaricare gli aggiornamenti dei database anti-virus per Kaspersky Security Center e le applicazioni Kaspersky gestite.



Impostazioni della connessione Internet

Se si desidera utilizzare un server proxy durante la connessione a Internet, abilitare l'opzione **Usa server proxy**. Se questa opzione è abilitata, i campi sono disponibili per l'immissione delle impostazioni. Specificare le seguenti impostazioni per la connessione a un server proxy:

- Indirizzo

  Indirizzo del server proxy utilizzato per la connessione di Kaspersky Security Center a Internet.

- Numero di porta

  Numero della porta utilizzata per stabilire la connessione al proxy di Kaspersky Security Center.

- Ignora il server proxy per gli indirizzi locali

  Non verrà utilizzato alcun server proxy per la connessione ai dispositivi dalla rete locale.

- **Autenticazione server proxy**

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  Questo campo di immissione è disponibile se la casella di controllo **Usa server proxy** è selezionata.

- **Nome utente**

  Account utente con il quale è stata stabilita la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

- **Password**

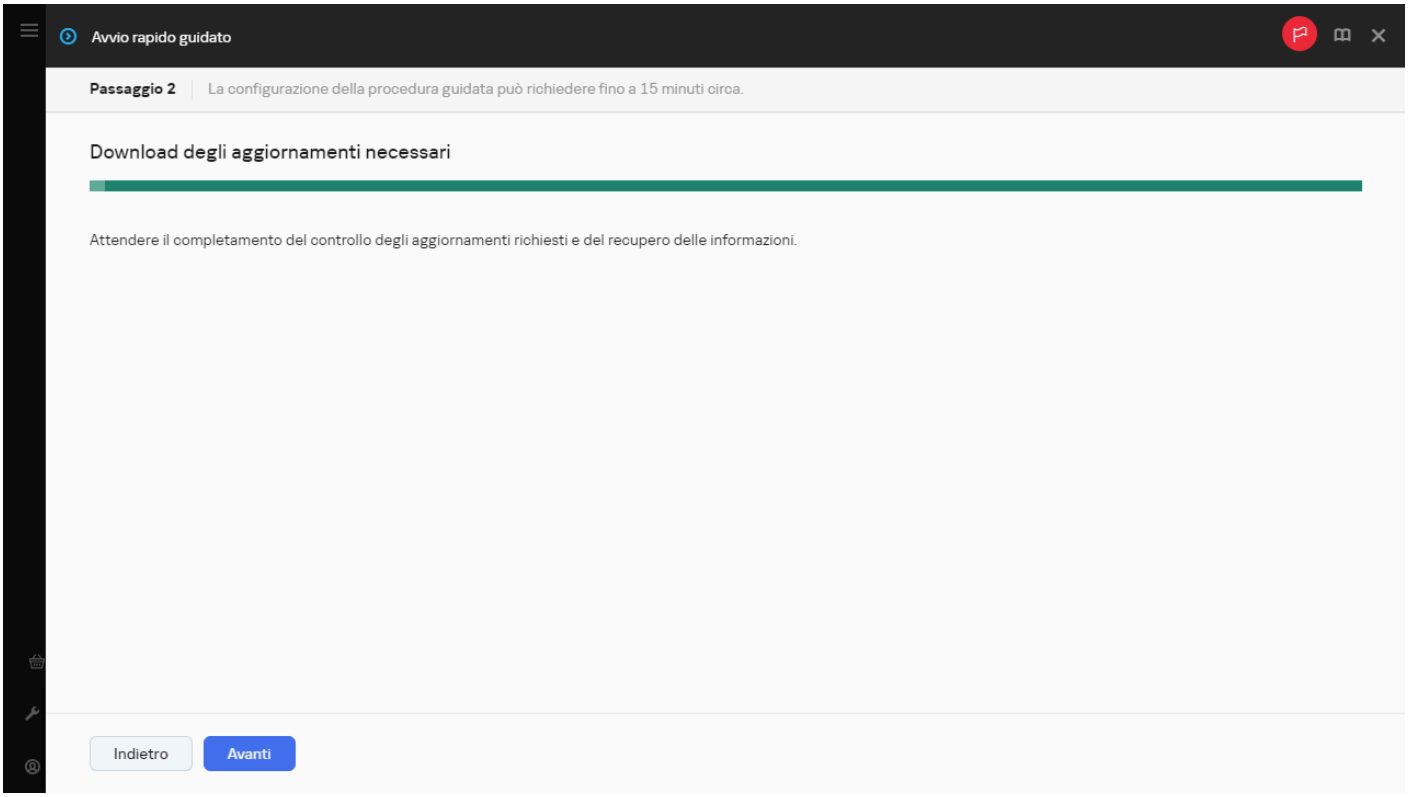
  Password impostata dall'utente di cui è stato utilizzato l'account per stabilire la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

  Per visualizzare la password immessa, tenere premuto il pulsante **Mostra** per il tempo necessario.

È possibile configurare l'accesso a Internet in un secondo momento, separatamente dall'Avvio rapido guidato.

Passaggio 2. Download degli aggiornamenti necessari

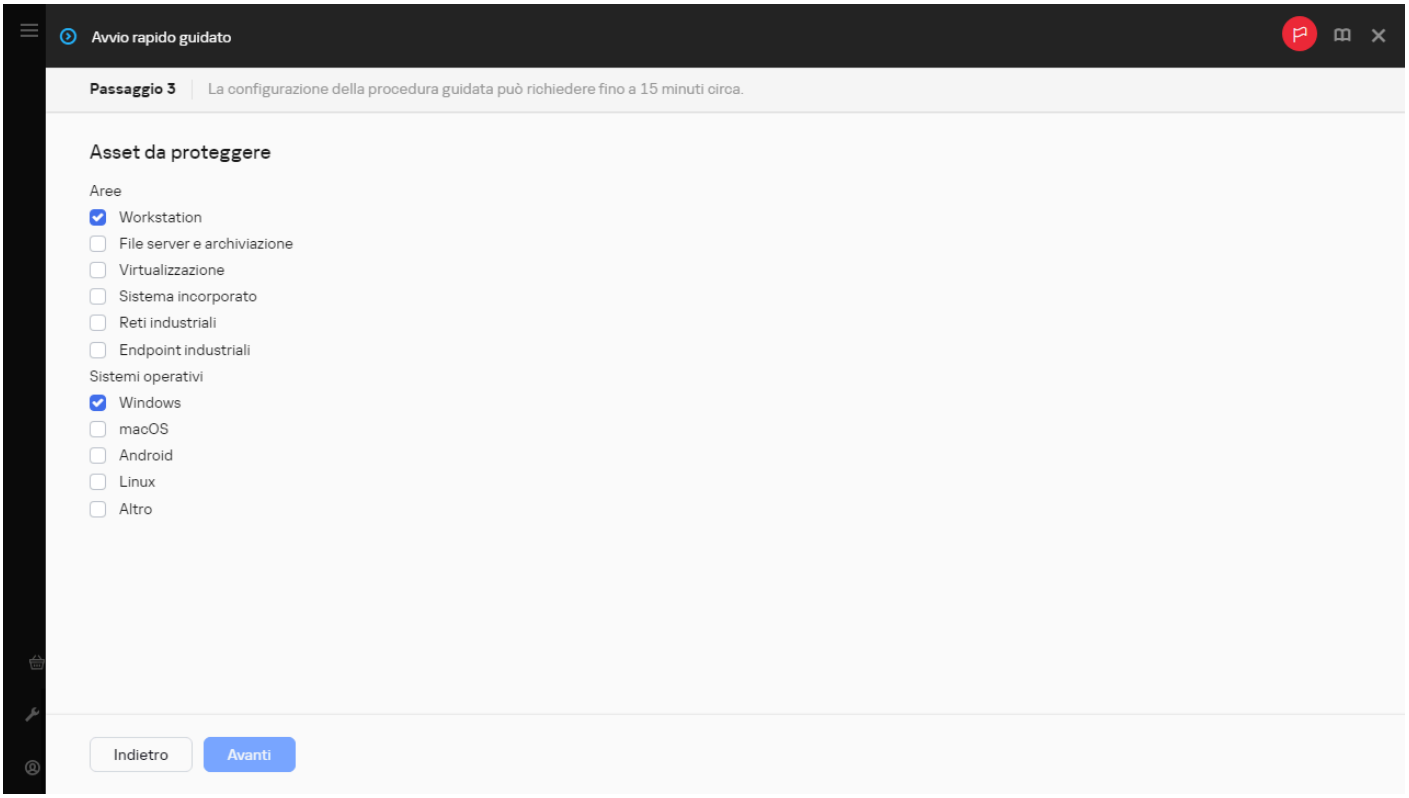
Gli aggiornamenti richiesti vengono scaricati automaticamente dai server Kaspersky.



Download degli aggiornamenti necessari

Passaggio 3. Selezione delle risorse da proteggere

Selezionare le aree di protezione e i sistemi operativi in uso nella rete. Quando si selezionano queste opzioni, si specificano i filtri per i plug-in di gestione delle applicazioni e i pacchetti di distribuzione nei server Kaspersky che è possibile scaricare per installarli nei dispositivi client nella rete.



Selezione delle risorse da proteggere

Selezionare le opzioni:

- **Aree**

  È possibile selezionare le seguenti aree di protezione:

  - **Workstation**. Selezionare questa opzione se si desidera proteggere le workstation nella rete. Per impostazione predefinita, l'opzione Workstation è selezionata.
  - **File server e archiviazione**. Selezionare questa opzione se si desidera proteggere i file server nella rete.
  - **Dispositivi mobili**. Selezionare questa opzione se si desidera proteggere i dispositivi mobili di proprietà dell'azienda o dei dipendenti aziendali. Se si seleziona questa opzione ma non è stata fornita una licenza con la funzionalità Mobile Device Management, viene visualizzato un messaggio che informa l'utente della necessità di fornire una licenza con la funzionalità Mobile Device Management. Se non viene fornita una licenza, non è possibile utilizzare la funzionalità per i dispositivi mobili.
  - **Virtualizzazione**. Selezionare questa opzione se si desidera proteggere le macchine virtuali nella rete.
  - **Kaspersky Anti-Spam**. Selezionare questa opzione se si desidera proteggere i server di posta aziendali dall'invio di spam, frodi e malware.
  - **Sistema incorporato**. Selezionare questa opzione se si desidera proteggere i sistemi integrati basati su Windows, come gli sportelli automatici (ATM).
  - **Reti industriali**. Selezionare questa opzione se si desidera monitorare i dati di sicurezza nella rete industriale e dagli endpoint di rete protetti dalle applicazioni Kaspersky.
  - **Endpoint industriali**. Selezionare questa opzione se si desidera proteggere i singoli nodi in una rete industriale.

- **Sistemi operativi**

  È possibile selezionare le seguenti piattaforme:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Altro

  Per ulteriori informazioni sui sistemi operativi supportati, vedere Requisiti hardware e software per Kaspersky Security Center Web Console.

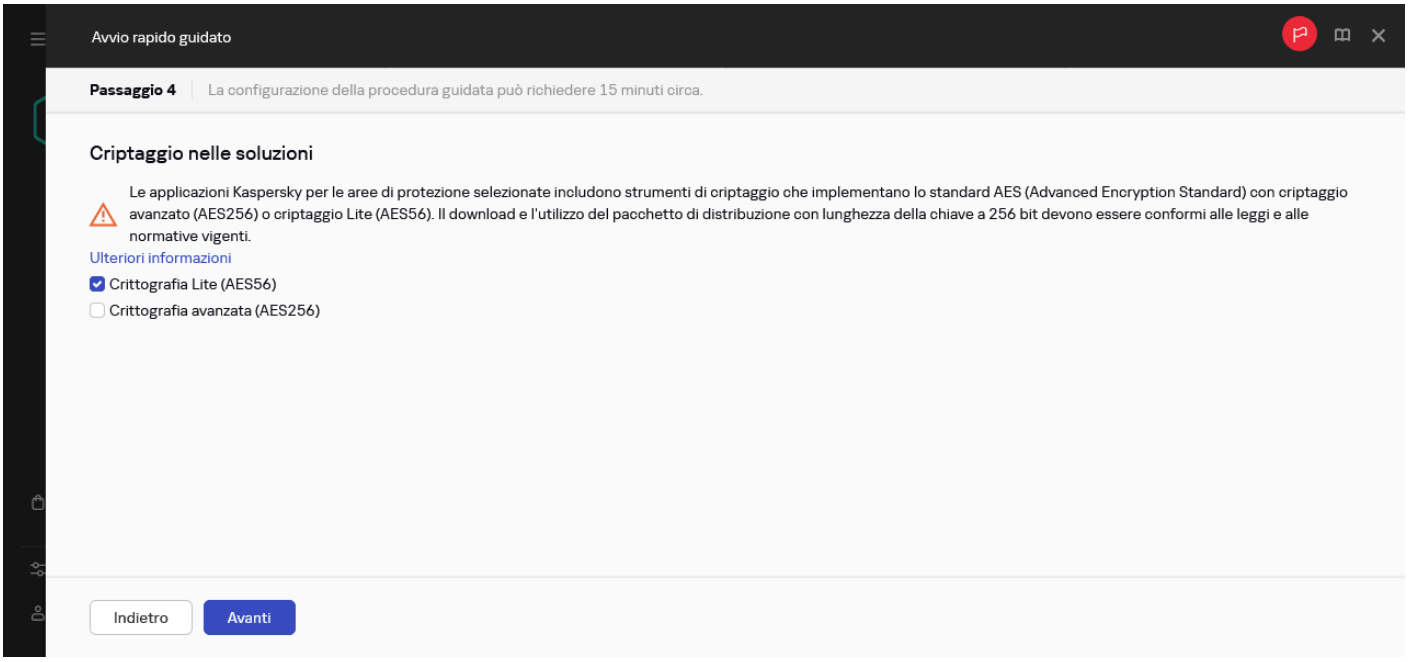
È possibile selezionare i pacchetti dell'applicazione Kaspersky nell'elenco dei pacchetti disponibili in un secondo momento, separatamente dall'Avvio rapido guidato. Per semplificare la ricerca dei pacchetti richiesti, è possibile filtrare l'elenco dei pacchetti disponibili in base a vari criteri.

Passaggio 4. Selezione del criptaggio nelle soluzioni

La finestra **Criptaggio nelle soluzioni** viene visualizzata solo se è stato selezionato **Workstation** come ambito della protezione.

Kaspersky Endpoint Security for Windows include strumenti di criptaggio per le informazioni archiviate nei dispositivi client basati su Windows. In tali strumenti di criptaggio, è implementato AES (Advanced Encryption Standard), con una lunghezza della chiave di 256 o 56 bit.

Il download e l'utilizzo del pacchetto di distribuzione con una lunghezza della chiave di 256 bit devono essere eseguiti in conformità con le leggi e le normative applicabili. Per scaricare un pacchetto di distribuzione di Kaspersky Endpoint Security for Windows valido per le esigenze aziendali, consultare le normative del paese in cui si trovano i dispositivi client dell'organizzazione.



Selezione del criptaggio nelle soluzioni

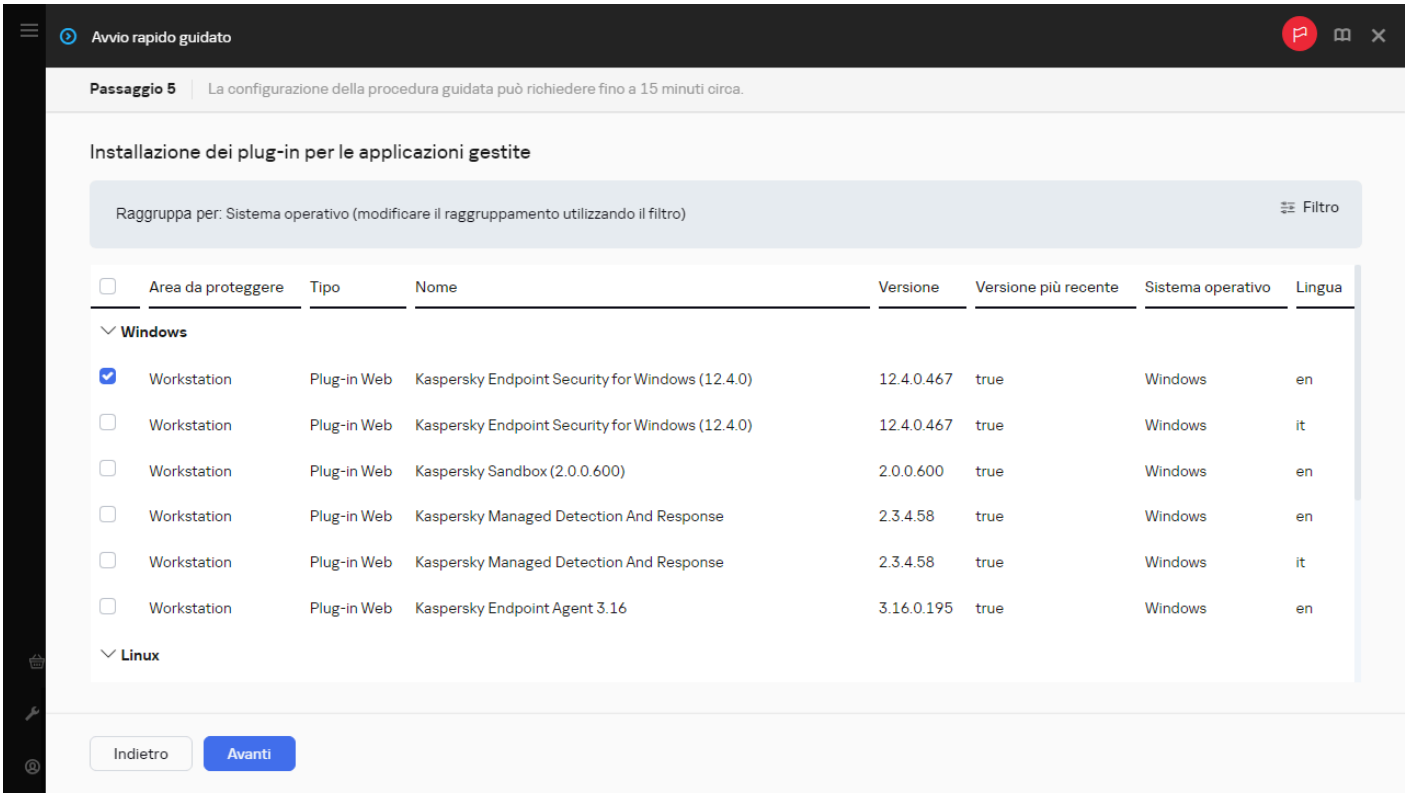
Nella finestra **Criptaggio nelle soluzioni** selezionare uno dei seguenti tipi di criptaggio:

- Crittografia Lite. Questo tipo di criptaggio utilizza una lunghezza della chiave di 56 bit.
- Crittografia avanzata. Questo tipo di criptaggio utilizza una lunghezza della chiave di 256 bit.

È possibile selezionare il pacchetto di distribuzione per Kaspersky Endpoint Security for Windows con il tipo di criptaggio richiesto in un secondo momento, separatamente dall'Avvio rapido guidato.

Passaggio 5. Configurazione dell'installazione dei plug-in per le applicazioni gestite

Selezionare i plug-in per le applicazioni gestite da installare. Viene visualizzato un elenco dei plug-in che si trovano nei server Kaspersky. L'elenco viene filtrato in base alle opzioni selezionate nel passaggio precedente della procedura guidata. Per impostazione predefinita, un elenco completo include i plug-in di tutte le lingue. Per visualizzare solo i plug-in di una lingua specifica, utilizzare il filtro.



Installazione dei plug-in per le applicazioni gestite

L'elenco dei plug-in include le seguenti colonne:

- **Area da proteggere**

  Le aree selezionate da proteggere sono visualizzate in questa colonna.

- **Tipo**

  I tipi di plug-in vengono visualizzati in questa colonna.

- **Nome**

  I plug-in sono selezionati in base alle aree di protezione e alle piattaforme, selezionati nel passaggio precedente.

- **Versione**

  L'elenco include i plug-in di tutte le versioni che si trovano nei server Kaspersky. Per impostazione predefinita, sono selezionati i plug-in delle versioni più recenti.

- **Versione più recente**

  Questa colonna indica se una versione del plug-in è l'ultima. Se viene visualizzato il valore **true**, il plug-in corrispondente è della versione più recente. Se viene visualizzato un valore **false**, il plug-in corrispondente ha una versione successiva.

- **Sistema operativo**

  Questa colonna mostra i sistemi operativi dei plug-in.

- **Lingua**

  Per impostazione predefinita, la lingua di localizzazione di un plug-in è determinata dalla lingua di Kaspersky Security Center selezionata al momento dell'installazione. È possibile specificare altre lingue nell'elenco a discesa **Mostra lingua di localizzazione di Administration Console oppure**.

Dopo aver selezionato i plug-in, fare clic su **Avanti** per avviare l'installazione.

È possibile installare i plug-in di gestione per le applicazioni Kaspersky manualmente, separatamente dall'Avvio rapido guidato.

L'Avvio rapido guidato installa automaticamente i plug-in selezionati. Per installare alcuni plug-in è necessario accettare le condizioni del Contratto di licenza con l'utente finale. Leggere il testo del Contratto di licenza con l'utente finale visualizzato, selezionare la casella di controllo **Accetto di utilizzare Kaspersky Security Network** e fare clic sul pulsante **Installa**. Se non si accettano le condizioni del Contratto di licenza con l'utente finale, il plug-in non viene installato.

Quando tutti i plug-in selezionati sono installati, l'Avvio rapido guidato porta automaticamente al passaggio successivo.

Passaggio 6. Installazione dei plug-in selezionati

L'Avvio rapido guidato installa automaticamente i plug-in selezionati nel passaggio precedente. Per installare alcuni plug-in è necessario accettare le condizioni del Contratto di licenza con l'utente finale. Leggere il testo del Contratto di licenza con l'utente finale visualizzato, selezionare la casella di controllo **Accetto di utilizzare Kaspersky Security Network** e fare clic sul pulsante **Installa**. Se non si accettano le condizioni del Contratto di licenza con l'utente finale, il plug-in non viene installato.

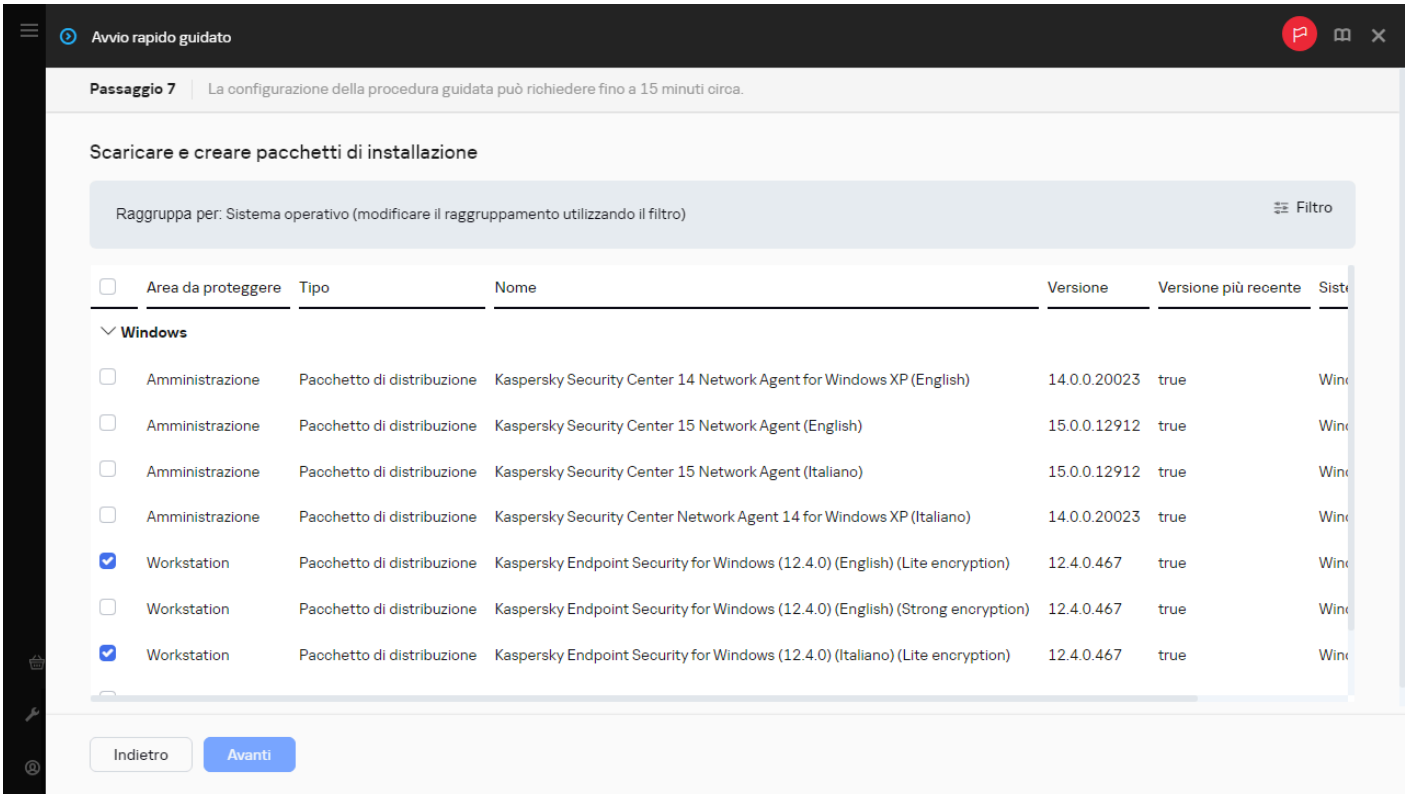
Quando tutti i plug-in selezionati sono installati, l'Avvio rapido guidato porta automaticamente al passaggio successivo.

Passaggio 7. Download dei pacchetti di distribuzione e creazione dei pacchetti di installazione

Selezionare i pacchetti di distribuzione da scaricare.

Le distribuzioni delle applicazioni gestite potrebbero richiedere l'installazione di una versione minima specifica di Kaspersky Security Center.

Dopo aver selezionato un tipo di criptaggio per Kaspersky Endpoint Security for Windows, viene visualizzato un elenco dei pacchetti di distribuzione di entrambi i tipi di criptaggio. Nell'elenco viene selezionato un pacchetto di distribuzione con il tipo di criptaggio selezionato. È possibile selezionare i pacchetti di distribuzione di qualsiasi tipo di criptaggio. La lingua del pacchetto di distribuzione corrisponde alla lingua di Kaspersky Security Center. Se non esiste un pacchetto di distribuzione di Kaspersky Endpoint Security for Windows per la lingua di Kaspersky Security Center, viene selezionato il pacchetto di distribuzione in inglese.



Download dei pacchetti di distribuzione e creazione dei pacchetti di installazione

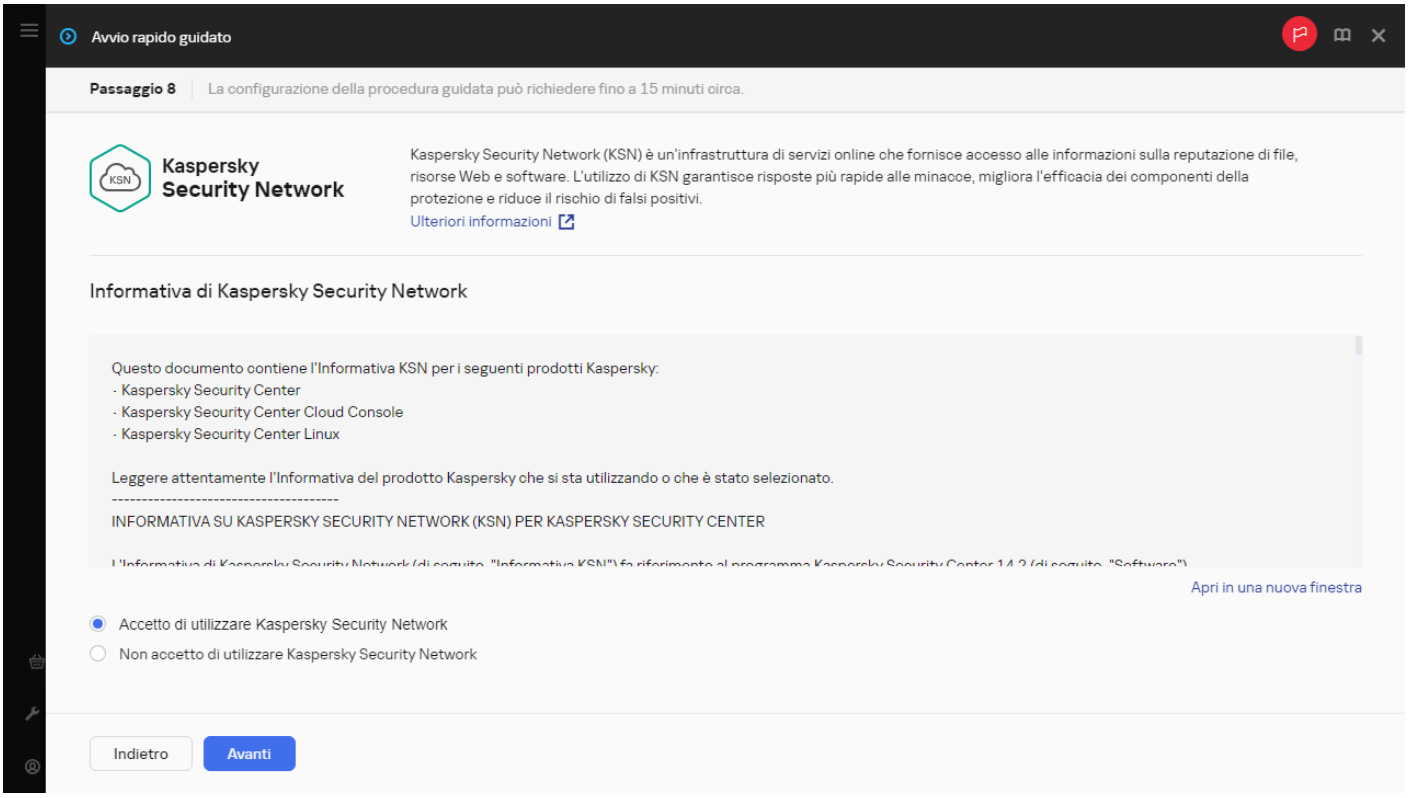
Per terminare il download di alcuni pacchetti di distribuzione è necessario accettare il Contratto di licenza con l'utente finale. Quando si fa clic sul pulsante **Accetta**, viene visualizzato il testo del Contratto di licenza con l'utente finale. Per procedere al passaggio successivo della procedura guidata, è necessario accettare i termini e le condizioni del Contratto di licenza con l'utente finale e i termini e le condizioni dell'Informativa sulla privacy di Kaspersky. Se non si accettano i termini e le condizioni, il download del pacchetto viene annullato.

Dopo aver accettato i termini e le condizioni del Contratto di licenza con l'utente finale e i termini e le condizioni dell'Informativa sulla privacy di Kaspersky, il download dei pacchetti di distribuzione prosegue. Successivamente è possibile utilizzare i pacchetti di installazione per distribuire le applicazioni Kaspersky nei dispositivi client.

È possibile scaricare i pacchetti di distribuzione e creare i pacchetti di installazione successivamente, separatamente dall'Avvio rapido guidato.

Passaggio 8. Configurazione di Kaspersky Security Network

Specificare le impostazioni per la trasmissione delle informazioni sulle operazioni di Kaspersky Security Center alla Knowledge Base di Kaspersky Security Network.



Configurazione di Kaspersky Security Network

Selezionare una delle seguenti opzioni:

- **Accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center e le applicazioni gestite installate nei dispositivi client trasferiranno automaticamente i dettagli sull'esecuzione a Kaspersky Security Network. La partecipazione a Kaspersky Security Network garantisce aggiornamenti più rapidi dei database contenenti le informazioni sui virus e sulle altre minacce, assicurando una risposta più rapida alle minacce per la sicurezza emergenti.

- **Non accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center e le applicazioni gestite non forniranno informazioni a Kaspersky Security Network.

  Se si seleziona questa opzione, l'utilizzo di Kaspersky Security Network sarà disabilitato.

È possibile configurare l'accesso a Kaspersky Security Network (KSN) successivamente, separatamente dall'Avvio rapido guidato.

Passaggio 9. Selezione del metodo di attivazione dell'applicazione

Selezionare una delle seguenti opzioni di attivazione di Kaspersky Security Center:

- **Immettendo il codice di attivazione**

  Codice di attivazione è una sequenza univoca di 20 caratteri alfanumerici. Il codice di attivazione viene inserito per aggiungere una chiave che consente di attivare Kaspersky Security Center. Si riceve il codice di attivazione tramite l'indirizzo e-mail specificato dopo l'acquisto di Kaspersky Security Center.

  Per attivare l'applicazione utilizzando un codice di attivazione, è necessario l'accesso a Internet per stabilire la connessione con i server di attivazione Kaspersky.

  Se è stata selezionata questa opzione di attivazione, è possibile abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

  Se questa opzione è abilitata, la chiave di licenza verrà distribuita automaticamente ai dispositivi gestiti.

  Se questa opzione è disabilitata, è possibile distribuire la chiave di licenza ai dispositivi gestiti in un secondo momento, nel nodo **Licenze di Kaspersky** della struttura di Administration Console.

- **Specificando un file chiave**

  File chiave: si tratta di un file con estensione key fornito all'utente da Kaspersky. Un file chiave consente di aggiungere una chiave per l'attivazione dell'applicazione.

  I metodi per ottenere il file chiave sono descritti nella sezione seguente: Informazioni sul file chiave.

  Per attivare l'applicazione utilizzando il file chiave, non è necessario connettersi ai server di attivazione di Kaspersky.

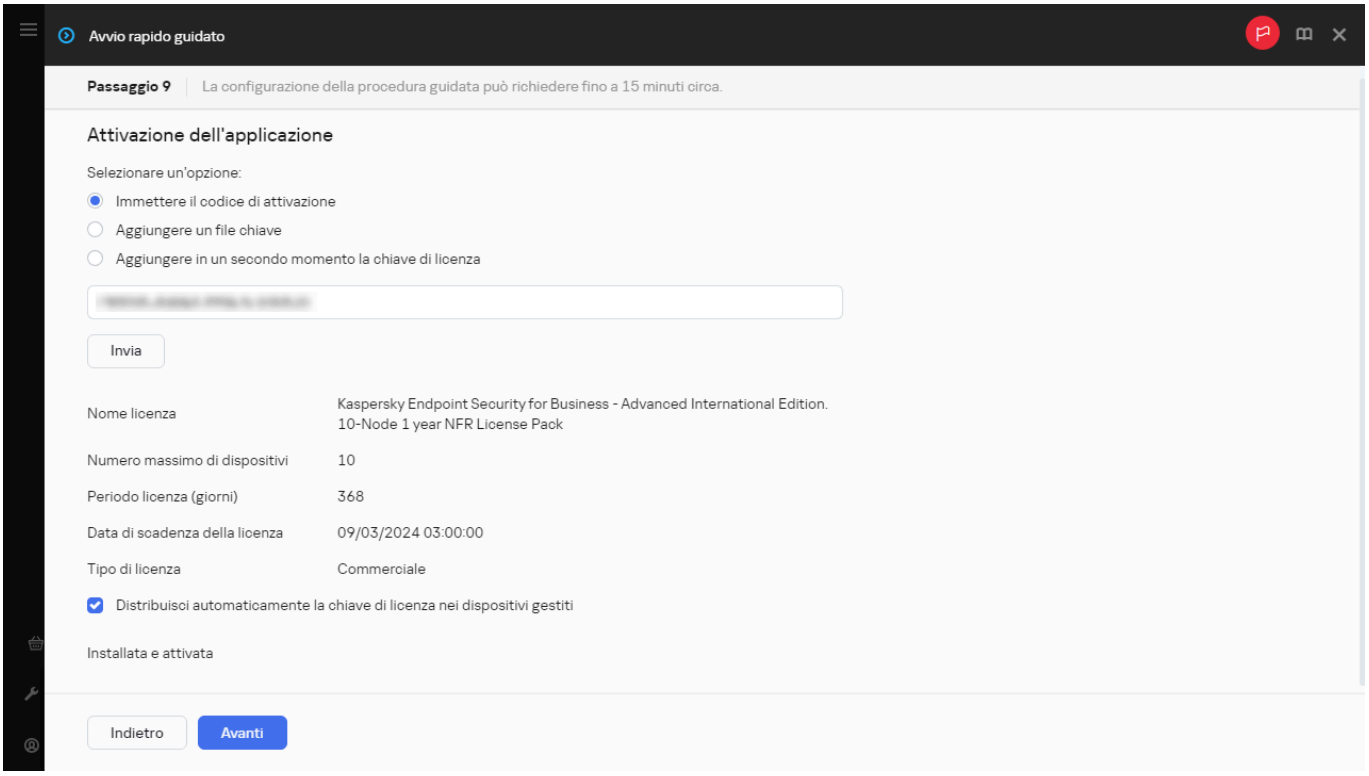
  Se è stata selezionata questa opzione di attivazione, è possibile abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

  Se questa opzione è abilitata, la chiave di licenza verrà distribuita automaticamente ai dispositivi gestiti.

  Se questa opzione è disabilitata, è possibile distribuire la chiave di licenza ai dispositivi gestiti in un secondo momento, nel nodo **Licenze di Kaspersky** della struttura di Administration Console.

- **Rimandando l'attivazione dell'applicazione**

L'applicazione verrà eseguita con la funzionalità di base, senza Mobile Device Management e senza Vulnerability e patch management.



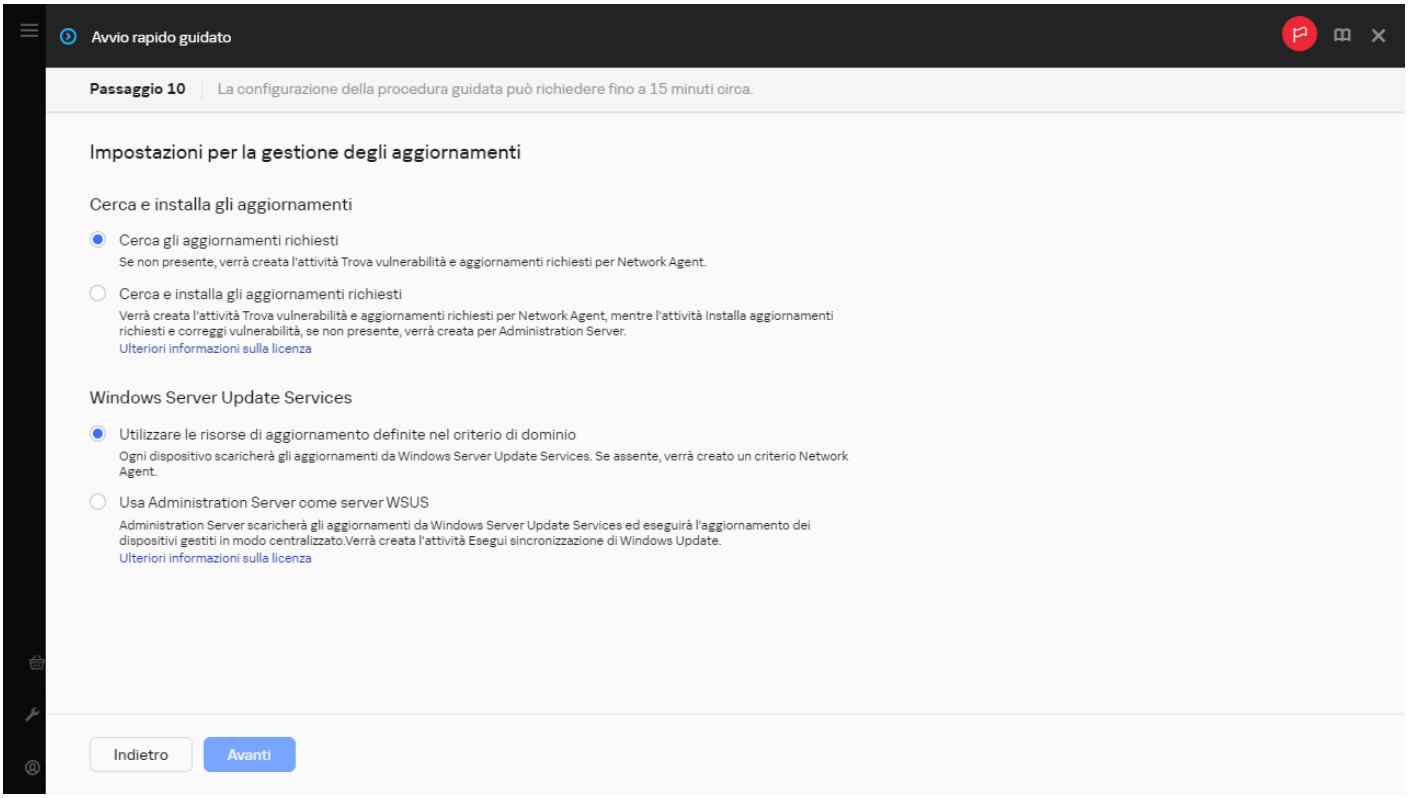
Selezione del metodo di attivazione dell'applicazione

Se si sceglie di rimandare l'attivazione dell'applicazione, è possibile aggiungere una chiave di licenza in qualsiasi momento selezionando **Operazioni** → **Licensing**.

Se si utilizza Kaspersky Security Center distribuito da un'AMI a pagamento o per uno SKU con fatturazione mensile basato sull'utilizzo, non è possibile specificare un file chiave o immettere un codice.

Passaggio 10. Definizione delle impostazioni di gestione degli aggiornamenti di terze parti

Questo passaggio non viene visualizzato se non si dispone della licenza Vulnerability e Patch Management e l'attività *Trova vulnerabilità e aggiornamenti richiesti* esiste già.



Impostazioni di gestione degli aggiornamenti di terze parti

Per gli aggiornamenti software di terze parti, selezionare una delle seguenti opzioni:

- **Cerca gli aggiornamenti richiesti**

  L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente, se non ne è presente una.

  Questa opzione è selezionata per impostazione predefinita.

- **Cerca e installa gli aggiornamenti richiesti**

  Se non sono già esistenti, le attività *Trova vulnerabilità e aggiornamenti richiesti* e *Installa aggiornamenti richiesti e correggi vulnerabilità* vengono create automaticamente.

  Questa opzione è disponibile solo con la licenza Vulnerability e patch management.

Per gli aggiornamenti di Windows Update, selezionare una delle seguenti opzioni:

- **Utilizzare le risorse di aggiornamento definite nel criterio di dominio**

  I dispositivi client scaricheranno gli aggiornamenti Windows Update in base alle impostazioni del criterio di dominio. Se non è già esistente, il criterio di Network Agent viene creato automaticamente.

- **Usa Administration Server come server WSUS**

  I dispositivi client scaricheranno gli aggiornamenti Windows Update da Administration Server. Se non sono già esistenti, l'attività *Esegui sincronizzazione di Windows Update* e il criterio di Network Agent vengono creati automaticamente.

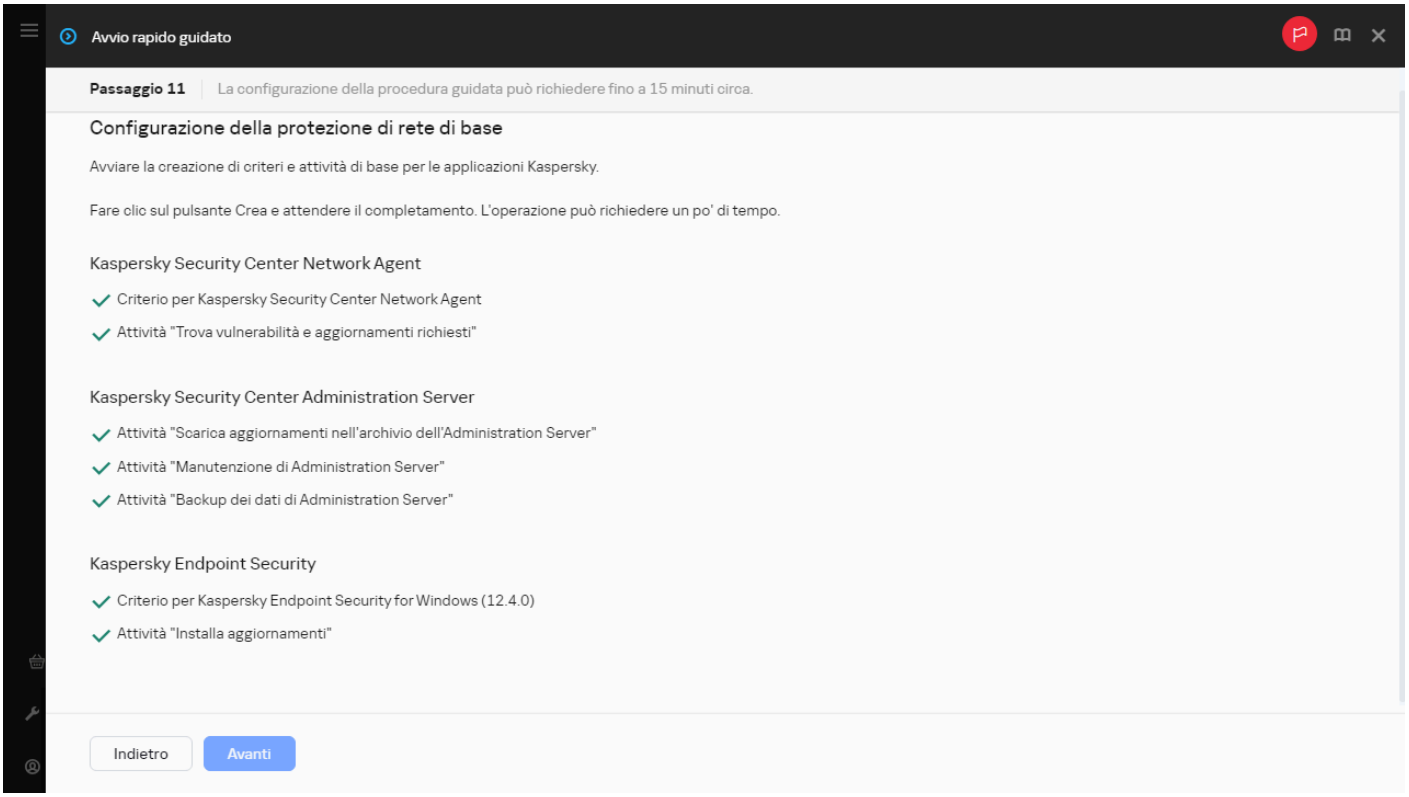
  Questa opzione è disponibile solo con la licenza Vulnerability e patch management.

È possibile creare le attività *Trova vulnerabilità e aggiornamenti richiesti* e *Installa gli aggiornamenti richiesti e correggi vulnerabilità* separatamente dall'Avvio rapido guidato. Per utilizzare Administration Server come server WSUS, creare l'attività *Perform Windows Update synchronization* e selezionare l'opzione **Usa Administration Server come server WSUS** nel criterio di Network Agent.

Passaggio 11. Creazione di una configurazione della protezione di rete di base

È possibile esaminare un elenco dei criteri e delle attività creati.

Attendere il completamento della creazione di criteri e attività prima di procedere al passaggio successivo della procedura guidata.

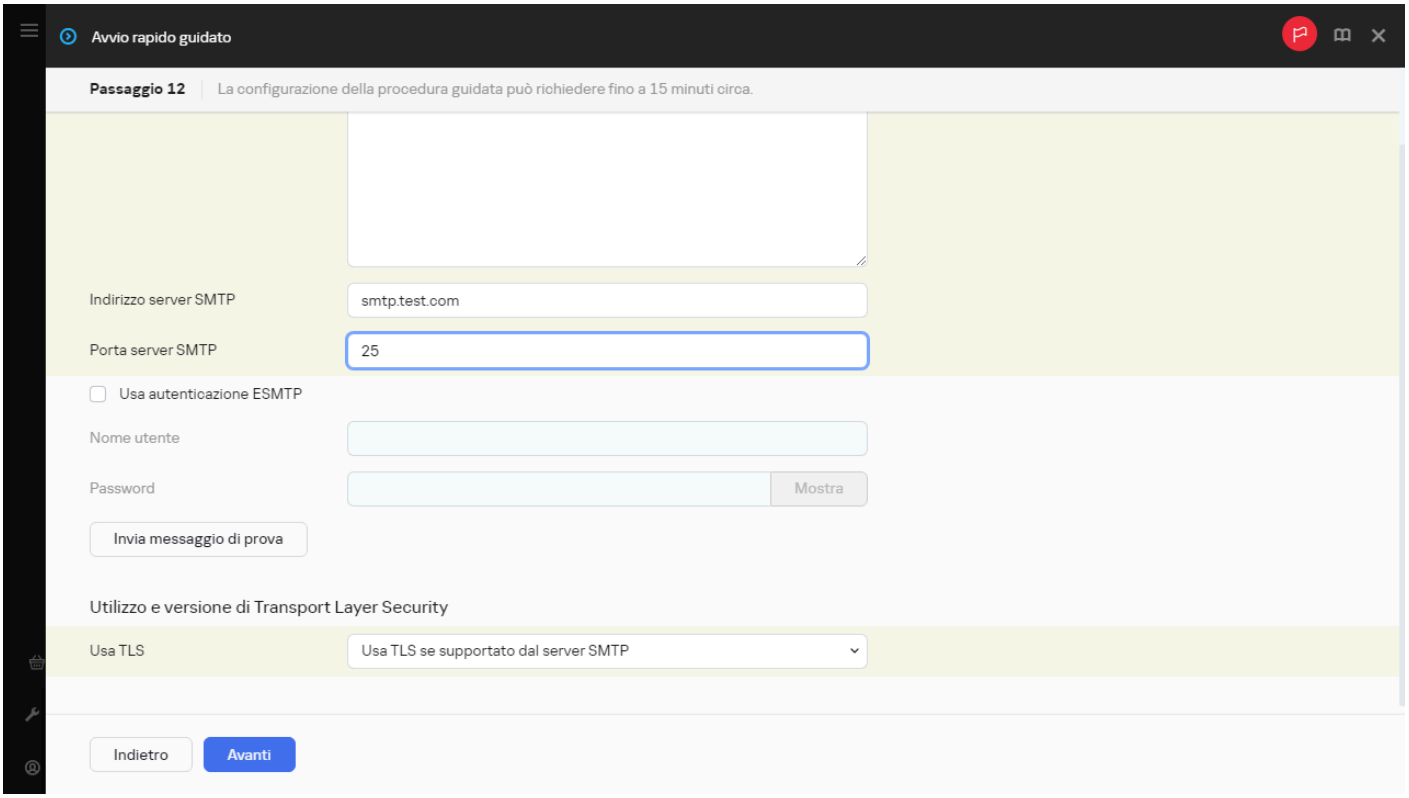


Creazione di una configurazione della protezione di rete di base

È possibile creare le attività e i criteri richiesti in un secondo momento, separatamente dall'Avvio rapido guidato.

Passaggio 12. Configurazione delle notifiche e-mail

Configurare l'invio di notifiche relative agli eventi registrati durante l'esecuzione delle applicazioni Kaspersky nei dispositivi client. Queste impostazioni verranno utilizzate come impostazioni predefinite per i criteri dell'applicazione.



Configurazione delle notifiche e-mail

Per configurare l'invio di notifiche relative agli eventi che si verificano nelle applicazioni Kaspersky, utilizzare le seguenti impostazioni:

- **Destinatari (indirizzi e-mail)**

  Gli indirizzi e-mail degli utenti a cui l'applicazione invierà le notifiche. È possibile immettere uno o più indirizzi; se si immette più di un indirizzo, separarli con un punto e virgola.

- **Indirizzo server SMTP**

  L'indirizzo o gli indirizzi dei server di posta dell'organizzazione.

  Se si immette più di un indirizzo, separarli con un punto e virgola. È possibile utilizzare i seguenti valori:

  - Indirizzo IPv4 o IPv6
  - Nome di rete Windows (nome NetBIOS) del dispositivo
  - Nome DNS del server SMTP

- Porta server SMTP

  Numero di porta di comunicazione del server SMTP. Se si utilizzano più server SMTP, la connessione a questi viene stabilita tramite la porta di comunicazione specificata. Il numero di porta predefinito è 25.

- Usa autenticazione ESMTP

  Abilita il supporto dell'autenticazione ESMTP. Quando la casella di controllo è selezionata, nei campi **Nome utente** e **Password** è possibile specificare le impostazioni per l'autenticazione ESMTP. Per impostazione predefinita, questa casella di controllo è deselezionata.

- Usa TLS

È possibile specificare le impostazioni di connessione TLS con un server SMTP:

- **Non utilizzare TLS**

  È possibile selezionare questa opzione se si desidera disabilitare il criptaggio dei messaggi e-mail.

- **Usa TLS se supportato dal server SMTP**

  È possibile selezionare questa opzione se si desidera utilizzare una connessione TLS in un server SMTP. Se il server SMTP non supporta TLS, Administration Server si connette al server SMTP senza utilizzare TLS.

- **Usa sempre TLS, controlla la validità del certificato del server**

  È possibile selezionare questa opzione se si desidera utilizzare le impostazioni di autenticazione TLS. Se il server SMTP non supporta TLS, Administration Server non può connettersi al server SMTP.

  È consigliabile utilizzare questa opzione per una protezione più efficace della connessione con un server SMTP. Se si seleziona questa opzione, è possibile configurare le impostazioni di autenticazione per una connessione TLS.

  Se si seleziona il valore **Usa sempre TLS, controlla la validità del certificato del server**, è possibile specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. È inoltre possibile specificare un certificato per l'autenticazione del client nel server SMTP.

È possibile specificare i certificati per una connessione TLS facendo clic sul collegamento **Specifica certificati**:

- Cercare un file di certificato del server SMTP:

  È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Administration Server. Kaspersky Security Center verifica se anche il certificato di un server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center non può connettersi a un server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

- Cercare un file di certificato del client:

  È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. È necessario specificare il certificato e la relativa chiave privata utilizzando uno dei seguenti tipi di certificato:

  - Certificato X-509:

    È necessario specificare un file con il certificato e un file con la chiave privata. Entrambi i file non dipendono l'uno dall'altro e l'ordine di caricamento dei file non è significativo. Quando entrambi i file vengono caricati, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

  - Contenitore pkcs12:

    È necessario caricare un singolo file che contenga il certificato e la relativa chiave privata. Quando il file viene caricato, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

È possibile verificare le nuove impostazioni di notifica e-mail facendo clic sul pulsante **Invia messaggio di test**.

È possibile configurare le notifiche degli eventi in un secondo momento, separatamente rispetto all'Avvio rapido guidato.

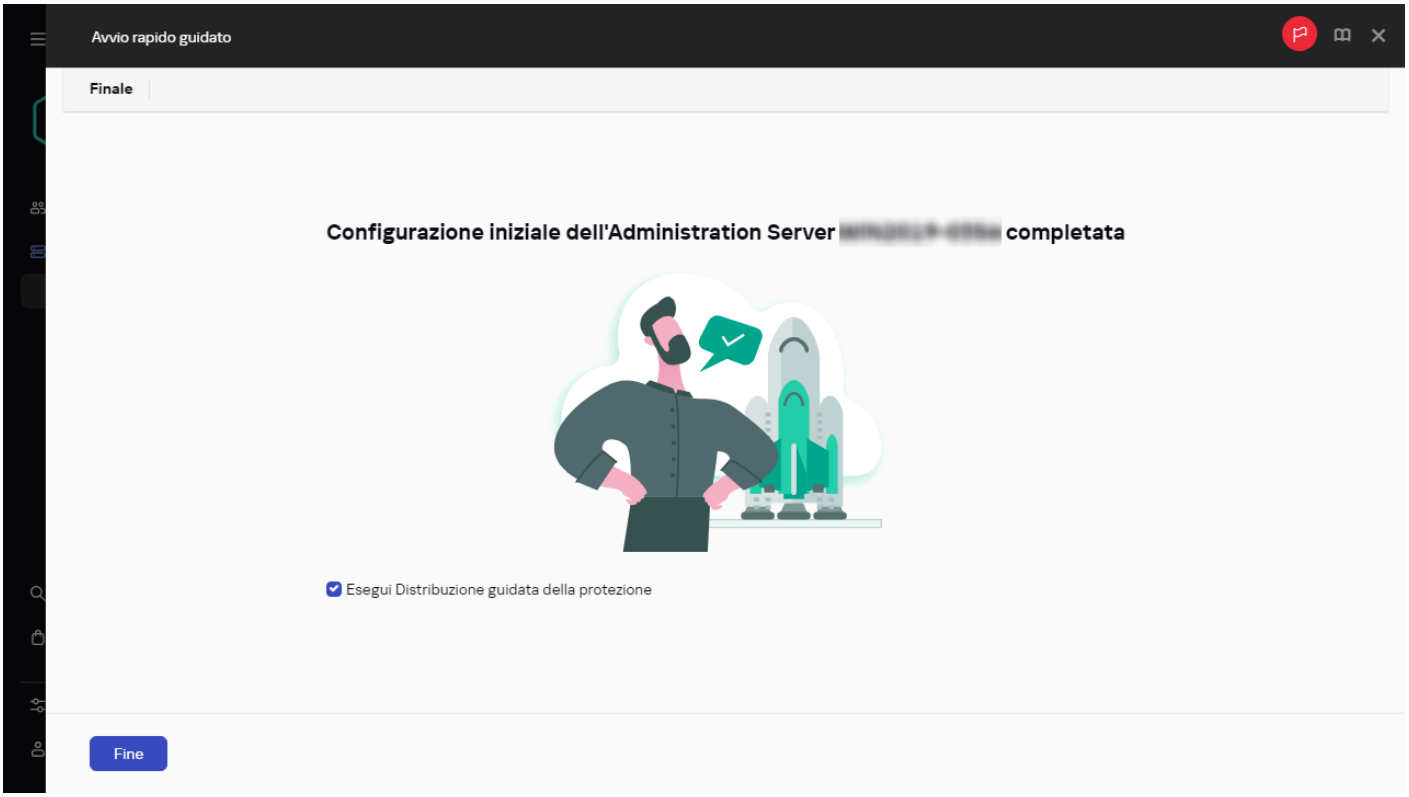
Passaggio 13. Esecuzione di un polling della rete

Administration Server esegue un polling iniziale. Durante il polling, viene visualizzata una barra di avanzamento. Al termine del polling, il collegamento **Visualizza dispositivi rilevati** diventa disponibile. È possibile fare clic su questo collegamento per visualizzare i dispositivi della rete rilevati da Administration Server. Per tornare all'Avvio rapido guidato, premere il tasto **ESC**.

È possibile eseguire il polling della rete in un secondo momento, separatamente dall'Avvio rapido guidato. Utilizzare Kaspersky Security Center Web Console per configurare il polling di un controller di dominio, dei domini di Windows, degli intervalli IP e delle reti IPv6.

Passaggio 14. Chiusura dell'Avvio rapido guidato

Nella pagina di completamento dell'Avvio rapido guidato selezionare la casella di controllo **Esegui Distribuzione guidata della protezione** se si desidera avviare l'installazione automatica delle applicazioni anti-virus o di Network Agent nei dispositivi della rete.



Passaggio finale dell'avvio rapido guidato

Per chiudere la procedura guidata, fare clic sul pulsante **Fine**.

Connessione dei dispositivi fuori sede

Questa sezione descrive come connettere i dispositivi fuori sede (cioè i dispositivi gestiti che si trovano all'esterno della rete principale) ad Administration Server.

Scenario: Connessione dei dispositivi fuori sede tramite un gateway di connessione

Questo scenario descrive come connettere i dispositivi gestiti che si trovano all'esterno della rete principale ad Administration Server.

Prerequisiti

Lo scenario prevede i seguenti prerequisiti:

- Una rete perimetrale deve essere organizzata nella rete dell'organizzazione.
- Kaspersky Security Center Administration Server deve essere distribuito nella rete aziendale.

Passaggi

Questo scenario procede per fasi:

1. **Selezione di un dispositivo client nella rete perimetrale**

   Questo dispositivo verrà utilizzato come gateway di connessione. Il dispositivo selezionato deve soddisfare i requisiti per i gateway di connessione.

2. **Installazione di Network Agent nel ruolo di gateway di connessione**

   È consigliabile utilizzare un'installazione locale per installare Network Agent nel dispositivo selezionato.

   Per impostazione predefinita, il file di installazione si trova in: \\<nome server>\KLSHARE\PkgInst\NetAgent_<numero versione>

   Nella finestra **Gateway di connessione** dell'Installazione guidata di Network Agent selezionare **Utilizzare Network Agent come gateway di connessione nella rete perimetrale**. Questa modalità attiva contemporaneamente il ruolo del gateway di connessione e indica a Network Agent di attendere le connessioni da Administration Server anziché stabilire connessioni ad Administration Server.

   In alternativa, è possibile installare Network Agent in un dispositivo Linux e configurare Network Agent in modo che funga da gateway di connessione, ma è necessario prestare attenzione all'elenco delle limitazioni di Network Agent in esecuzione nei dispositivi Linux.

3. **Autorizzazione delle connessioni nei firewall sul gateway di connessione**

   Per assicurarsi che Administration Server sia effettivamente in grado di connettersi al gateway di connessione nella rete perimetrale, consentire le connessioni alla porta TCP 13000 in tutti i firewall tra Administration Server e il gateway di connessione.

   Se il gateway di connessione non dispone di un indirizzo IP reale in Internet ma si trova invece dietro una configurazione NAT (Network Address Translation), configurare una regola per inoltrare le connessioni tramite NAT.

4. **Creazione di un gruppo di amministrazione per i dispositivi esterni**

   Creare un nuovo gruppo nel gruppo **Dispositivi gestiti**. Questo nuovo gruppo conterrà dispositivi gestiti esterni.

5. **Connessione del gateway di connessione ad Administration Server**

Il gateway di connessione configurato è in attesa di una connessione da Administration Server. Tuttavia, Administration Server non elenca il dispositivo con il gateway di connessione tra i dispositivi gestiti. Questo è dovuto al fatto che il gateway di connessione non ha tentato di stabilire una connessione ad Administration Server. È pertanto necessaria una procedura speciale per garantire che Administration Server avvii una connessione al gateway di connessione.

Procedere come segue:

1. Aggiungere il gateway di connessione come punto di distribuzione.
2. Spostare il gateway di connessione dal gruppo **Dispositivi non assegnati** al gruppo creato per i dispositivi esterni.

Il gateway di connessione è stato connesso e configurato.

6 **Connessione dei dispositivi desktop esterni ad Administration Server**

Solitamente i dispositivi desktop esterni non vengono spostati all'interno del perimetro. Pertanto è necessario configurarli per eseguire la connessione ad Administration Server tramite il gateway durante l'installazione di Network Agent.

7 **Configurazione degli aggiornamenti per i computer dispositivi esterni**

Se gli aggiornamenti delle applicazioni di protezione sono configurati per il download da Administration Server, i dispositivi esterni scaricano gli aggiornamenti tramite il gateway di connessione. Questo comporta due svantaggi:

- Si tratta di traffico non necessario che occupa la larghezza di banda del canale di comunicazione Internet aziendale.
- Questo non è necessariamente il modo più rapido per ottenere aggiornamenti. È molto probabile che per i dispositivi esterni sarebbe più economico e veloce ricevere gli aggiornamenti dai server di aggiornamento Kaspersky.

Procedere come segue:

1. Spostare tutti i dispositivi esterni nel gruppo di amministrazione separato creato in precedenza.
2. Escludere il gruppo con i dispositivi esterni dall'attività di aggiornamento.
3. Creare un'attività di aggiornamento separata per il gruppo con i dispositivi esterni.

8 **Connessione dei laptop mobili ad Administration Server**

I laptop mobili a volte sono all'interno della rete e altre volte all'esterno della rete. Per una gestione efficace, è necessario che questi si connettano ad Administration Server in modo diverso a seconda della posizione. Per un utilizzo efficiente del traffico, è inoltre necessario che ricevano gli aggiornamenti da origini diverse a seconda della posizione.

È necessario configurare le regole per gli utenti fuori sede: profili di connessione e descrizioni dei percorsi di rete. Ciascuna regola definisce l'istanza di Administration Server a cui i laptop mobili devono connettersi a seconda della posizione e l'istanza di Administration Server da cui devono ricevere gli aggiornamenti.

Scenario: connessione di dispositivi fuori sede tramite un Administration Server secondario in DMZ

Se si desidera connettere i dispositivi gestiti che si trovano all'esterno della rete principale ad Administration Server, è possibile utilizzare un Administration Server secondario situato nella rete perimetrale (DMZ).

Prerequisiti

Prima di iniziare, verificare di avere:

- Una rete perimetrale deve essere organizzata nella rete dell'organizzazione.
- Kaspersky Security Center Administration Server è distribuito nella rete interna dell'organizzazione.

Passaggi

Questo scenario procede per fasi:

1. **Selezione di un dispositivo client nella rete perimetrale**

   Nella DMZ, selezionare un dispositivo client che verrà utilizzato come Administration Server secondario.

2. **Installazione di Kaspersky Security Center Administration Server**

   Installare Kaspersky Security Center Administration Server in questo dispositivo client.

3. **Creazione di una gerarchia di Administration Server**

   Se si posiziona un Administration Server secondario in DMZ, l'Administration Server secondario deve ricevere una connessione dall'Administration Server primario. A tale scopo, aggiungere un nuovo Administration Server come secondario in modo che l'Administration Server primario si connetta all'Administration Server secondario tramite la porta 13000. Quando si combinano due Administration Server in una gerarchia, verificare che la porta 13299 sia accessibile in entrambi gli Administration Server. Kaspersky Security Center Web Console si connette a un Administration Server tramite la porta 13299.

4. **Connessione dei dispositivi gestiti fuori sede all'Administration Server secondario**

   È possibile connettere i dispositivi fuori sede ad Administration Server in DMZ nello stesso modo in cui viene stabilita la connessione tra Administration Server e i dispositivi gestiti che si trovano nella rete principale. I dispositivi gestiti fuori sede avviano la connessione tramite la porta 13000.

Informazioni sulla connessione dei dispositivi fuori sede

Alcuni dispositivi gestiti si trovano sempre all'esterno della rete principale (ad esempio dispositivi nelle filiali dell'azienda; chioschi, bancomat e terminali installati in vari punti vendita; dispositivi negli uffici domestici dei dipendenti). Alcuni dispositivi si spostano di tanto in tanto al di fuori del perimetro (ad esempio i laptop degli utenti che visitano le filiali regionali o l'ufficio di un cliente).

È comunque necessario monitorare e gestire la protezione dei dispositivi fuori sede: ricevere informazioni effettive sul relativo stato della protezione e mantenere aggiornate le applicazioni di protezione in essi installate. Questa prassi è necessaria perché se ad esempio uno di questi dispositivi viene compromesso mentre è all'esterno della rete principale, potrebbe diventare una piattaforma per la propagazione delle minacce non appena si connette alla rete principale. Per connettere i dispositivi fuori sede ad Administration Server è possibile utilizzare due metodi:

- Gateway di connessione nella rete perimetrale

  Visualizzare lo schema del traffico dati: Administration Server nella LAN, dispositivi gestiti in Internet, gateway di connessione in uso

- Administration Server nella rete perimetrale

  Visualizzare lo schema del traffico dati: Administration Server nella rete perimetrale, dispositivi gestiti in Internet

Un gateway di connessione nella rete perimetrale

Un metodo consigliato per connettere i dispositivi fuori sede ad Administration Server è quello di organizzare una rete perimetrale nella rete dell'organizzazione e di installare un gateway di connessione nella rete perimetrale. I dispositivi esterni si connetteranno al gateway di connessione e Administration Server all'interno della rete avvierà una connessione ai dispositivi tramite il gateway di connessione.

Rispetto all'altro metodo, questo è più sicuro:

- Non è necessario aprire l'accesso ad Administration Server dall'esterno della rete.
- Un gateway di connessione compromesso non rappresenta un rischio elevato per la sicurezza dei dispositivi di rete. Un gateway di connessione in realtà non gestisce nulla autonomamente e non stabilisce alcuna connessione.

Inoltre, un gateway di connessione non richiede molte risorse hardware.

Tuttavia, questo metodo ha un processo di configurazione più complicato:

- Per fare in modo che un dispositivo funga da gateway di connessione nella rete perimetrale, è necessario installare Network Agent e connetterlo ad Administration Server in un modo specifico.
- Non sarà possibile utilizzare lo stesso indirizzo per la connessione ad Administration Server per tutte le situazioni. Dall'esterno del perimetro sarà necessario utilizzare non solo un indirizzo diverso (indirizzo del gateway di connessione), ma anche una modalità di connessione diversa: tramite un gateway di connessione.
- È inoltre necessario definire impostazioni di connessione diverse per i laptop in posizioni diverse.

Per aggiungere un gateway di connessione a una rete configurata in precedenza:

1. Installare Network Agent in modalità gateway di connessione.
2. Reinstallare Network Agent nei dispositivi che si desidera connettere al gateway di connessione appena aggiunto.

Administration Server nella rete perimetrale

Un altro metodo consiste nell'installare un singolo Administration Server nella rete perimetrale.

Questa configurazione è meno sicura rispetto all'altro metodo. Per gestire laptop esterni in questo caso, Administration Server deve accettare connessioni da qualsiasi indirizzo in Internet. Gestirà comunque tutti i dispositivi nella rete interna, ma dalla rete perimetrale. Pertanto, un server compromesso potrebbe causare un'ingente quantità di danni, nonostante la bassa probabilità che tale evento si verifichi.

Il rischio si riduce notevolmente se Administration Server nella rete perimetrale non gestisce i dispositivi nella rete interna. Tale configurazione può essere utilizzata ad esempio da un fornitore di servizi per gestire i dispositivi dei clienti.

Potrebbe essere opportuno utilizzare questo metodo nei seguenti casi:

- Se si ha familiarità con l'installazione e la configurazione di Administration Server e non si desidera eseguire un'altra procedura per installare e configurare un gateway di connessione.
- Se è necessario gestire più dispositivi. La capacità massima di Administration Server è di 100.000 dispositivi, mentre un gateway di connessione può supportare fino a 10.000 dispositivi.

Questa soluzione presenta anche possibili difficoltà:

- Administration Server richiede più risorse hardware e un altro database.
- Le informazioni sui dispositivi verranno archiviate in due database non correlati (per Administration Server all'interno della rete e un altro nella rete perimetrale), il che complica il monitoraggio.
- Per gestire tutti i dispositivi, Administration Server deve trovarsi in una gerarchia, il che complica non solo il monitoraggio ma anche la gestione. Un'istanza dell'Administration Server secondario impone limitazioni alle possibili strutture dei gruppi di amministrazione. È necessario decidere come e quali attività e criteri distribuire a un'istanza dell'Administration Server secondario.
- La configurazione di dispositivi esterni per l'utilizzo di Administration Server nella rete perimetrale dall'esterno e per l'utilizzo dell'Administration Server primario dall'interno non è più semplice della configurazione per l'utilizzo di una connessione condizionale tramite un gateway.
- Elevati rischi per la sicurezza. Un'istanza di Administration Server compromessa semplifica la compromissione dei laptop gestiti. In tal caso, gli hacker devono solo attendere che uno dei laptop torni nella rete aziendale in modo da poter proseguire l'attacco nella LAN.

Connessione dei dispositivi desktop esterni ad Administration Server

I dispositivi desktop che si trovano sempre all'esterno della rete principale (ad esempio dispositivi nelle filiali dell'azienda; chioschi, bancomat e terminali installati in vari punti vendita; dispositivi negli uffici domestici dei dipendenti) non possono essere collegati direttamente ad Administration Server. Devono essere collegati ad Administration Server tramite un gateway di connessione installato nella rete perimetrale. Questa configurazione viene eseguita durante l'installazione di Network Agent in tali dispositivi.

Per connettere dispositivi desktop esterni ad Administration Server:

1. Creare un nuovo pacchetto di installazione per Network Agent.
2. Aprire le proprietà del pacchetto di installazione creato e passare alla sezione **Impostazioni** → **Avanzate**, quindi selezionare l'opzione **Esegui la connessione ad Administration Server utilizzando un gateway di connessione**.

   L'impostazione **Esegui la connessione ad Administration Server utilizzando un gateway di connessione** non è compatibile con l'impostazione **Utilizzare Network Agent come gateway di connessione nella rete perimetrale**. Non è possibile abilitare entrambe queste impostazioni contemporaneamente.

3. Nel campo **Indirizzo gateway connessione**, specificare l'indirizzo pubblico del gateway di connessione.

   Se il gateway di connessione si trova dietro una configurazione NAT (Network Address Translation) e non dispone di un proprio indirizzo pubblico, configurare una regola del gateway NAT per inoltrare le connessioni dall'indirizzo pubblico all'indirizzo interno del gateway di connessione.

4. Creare un pacchetto di installazione indipendente basato sul pacchetto di installazione creato.

5. Distribuire il pacchetto di installazione indipendente ai dispositivi di destinazione in formato elettronico o tramite un'unità rimovibile.

6. Installare Network Agent dal pacchetto indipendente.

I dispositivi desktop esterni sono connessi ad Administration Server.

Informazioni sui profili di connessione per gli utenti fuori sede

Gli utenti fuori sede con computer portatili (di seguito denominati anche "dispositivi") possono aver bisogno di modificare il metodo di connessione a un Administration Server o passare da un Administration Server all'altro a seconda della posizione corrente del dispositivo nella rete aziendale.

I profili di connessione sono supportati solo per i dispositivi che eseguono Windows e macOS.

Utilizzo di differenti indirizzi di un singolo Administration Server

I dispositivi con Network Agent installato possono connettersi all'Administration Server dalla rete Intranet dell'organizzazione o da Internet. Questa situazione può richiedere l'utilizzo da parte di Network Agent di differenti indirizzi per la connessione ad Administration Server: l'indirizzo esterno dell'Administration Server per la connessione Internet e l'indirizzo interno dell'Administration Server per la connessione dalla rete interna.

A tale scopo, aggiungere un profilo per la connessione ad Administration Server da Internet nelle proprietà del criterio di Network Agent (nella sezione **Impostazioni applicazione → Connettività → Profili connessione → Profili connessione di Administration Server**). Nella finestra di creazione del profilo, disabilitare l'opzione **Usa per ricevere solo aggiornamenti** e accertarsi che l'opzione **Sincronizza le impostazioni di connessione con le impostazioni di Administration Server specificate nel profilo** sia selezionata. Se si utilizza un gateway di connessione per accedere ad Administration Server (ad esempio, in una configurazione di Kaspersky Security Center come quella descritta in Accesso a Internet: Network Agent come gateway nella rete perimetrale), è necessario specificare l'indirizzo del gateway di connessione nel campo corrispondente del profilo di connessione.

Passaggio da un Administration Server all'altro a seconda della rete corrente

Se l'organizzazione ha più sedi con diversi Administration Server e alcuni dispositivi con Network Agent installato si spostano tra di esse, è necessario che Network Agent si connetta all'Administration Server della rete locale nella sede in cui si trova attualmente il dispositivo.

In questo caso, creare un profilo per la connessione ad Administration Server nelle proprietà del criterio di Network Agent per ciascuna delle sedi, tranne che per la sede principale in cui si trova l'Administration Server principale originale. Specificare gli indirizzi di Administration Server nei profili di connessione e abilitare o disabilitare l'opzione **Usa per ricevere solo aggiornamenti**:

- Selezionare l'opzione se è necessario sincronizzare Network Agent con l'Administration Server principale e utilizzare il server locale solo per scaricare gli aggiornamenti.

- Disabilitare questa opzione se è necessario che Network Agent sia completamente gestito dall'Administration Server locale.

Sarà quindi necessario impostare le condizioni per il passaggio ai nuovi profili creati: almeno una condizione per ciascuna delle sedi, tranne che per la sede principale. Lo scopo di ogni condizione consiste nel rilevamento degli elementi che sono specifici per l'ambiente di rete di una sede. Se una condizione è vera, il profilo corrispondente viene attivato. Se nessuna delle condizioni è vera, Network Agent passa all'Administration Server principale.

Creazione di un profilo di connessione per gli utenti fuori sede

Un profilo di connessione di Administration Server è disponibile solo nei dispositivi che eseguono Windows e macOS.

Per creare un profilo per la connessione di Network Agent ad Administration Server per gli utenti fuori sede:

1. Se si desidera creare un profilo di connessione per un gruppo di dispositivi gestiti, aprire il criterio di Network Agent di questo gruppo. A tale scopo, procedere come segue:
   a. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
   b. Fare clic sul collegamento del percorso corrente.
   c. Nella finestra visualizzata selezionare il gruppo di amministrazione desiderato.
      Successivamente, il percorso corrente viene modificato.
   d. Aggiungere il criterio di Network Agent per il gruppo di dispositivi gestiti. Se è già stato creato, fare clic sul nome del criterio di Network Agent per aprire le proprietà del criterio.
2. Se si desidera creare un profilo di connessione per un dispositivo gestito specifico, procedere come segue:
   a. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
   b. Fare clic sul nome del dispositivo gestito.
   c. Nella finestra delle proprietà del dispositivo gestito visualizzata, passare alla scheda **Applicazioni**.
   d. Fare clic sul nome del criterio di Network Agent a cui si applica solo il dispositivo gestito selezionato.
3. Nella finestra delle proprietà visualizzata passare a **Impostazioni applicazione** → **Connettività** → **Profili connessione.**

4. Nella sezione **Profili connessione di Administration Server** fare clic sul pulsante **Aggiungi**.

   Per impostazione predefinita, l'elenco dei profili di connessione contiene i profili <Modalità offline> e <Administration Server principale>. I profili non possono essere modificati o rimossi.

   Il profilo <Modalità offline> non specifica alcun server per la connessione. Di conseguenza, quando viene eseguito il passaggio a questo profilo, Network Agent non tenta di connettersi ad alcun Administration Server, mentre le applicazioni installate nei dispositivi client sono eseguite con i criteri fuori sede. Il profilo <Modalità offline> può essere utilizzato se i dispositivi sono disconnessi dalla rete.

   Il profilo <Administration Server principale> specifica per la connessione l'Administration Server che è stato selezionato durante l'installazione di Network Agent. Il profilo <Administration Server principale> viene applicato quando un dispositivo si riconnette all'Administration Server principale dopo l'esecuzione in una rete esterna per un determinato periodo.

5. Nella finestra **Configurare il profilo** visualizzata configurare il profilo di connessione:

   - Nome profilo

     Nel campo di immissione è possibile visualizzare o modificare il nome del profilo di connessione.

   - Indirizzo di Administration Server

     Indirizzo di Administration Server a cui il dispositivo client deve connettersi durante l'attivazione del profilo.

   - Numero di porta

     Il numero di porta utilizzato per la connessione.

   - Porta SSL

     Il numero della porta per la connessione tramite il protocollo SSL.

   - Usa connessione SSL

     Se questa opzione è abilitata, la connessione viene stabilita tramite una porta sicura utilizzando il protocollo SSL.

     Per impostazione predefinita, questa opzione è abilitata. È consigliabile non disabilitare questa opzione in modo che la connessione rimanga protetta.

   - Se si desidera utilizzare un server proxy durante la connessione a Internet, selezionare l'opzione **Usa server proxy**. Se questa opzione è selezionata, i campi sono disponibili per l'immissione delle impostazioni. Specificare le seguenti impostazioni per la connessione a un server proxy:

     - Indirizzo

       Indirizzo del server proxy utilizzato per la connessione di Kaspersky Security Center a Internet.

     - Numero di porta

Numero della porta utilizzata per stabilire la connessione al proxy di Kaspersky Security Center.

- **Autenticazione server proxy**

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

- **Nome utente**

  Account utente con il quale è stata stabilita la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

- **Password**

  Password impostata dall'utente di cui è stato utilizzato l'account per stabilire la connessione al server proxy (questo campo è disponibile se la casella di controllo **Autenticazione server proxy** è selezionata).

  Per visualizzare la password immessa, tenere premuto il pulsante **Mostra** per il tempo necessario.

- **Indirizzo gateway connessione**

  Indirizzo del gateway attraverso cui i dispositivi client si connettono ad Administration Server.

- **Abilita la modalità fuori sede quando Administration Server non è disponibile**

  Selezionare questa casella di controllo per consentire alle applicazioni installate in un dispositivo client di utilizzare i profili criterio per i dispositivi in modalità fuori sede, nonché i criteri fuori sede, per qualsiasi tentativo di connessione se Administration Server non è disponibile. Se non è definito alcun criterio fuori sede per l'applicazione, verrà utilizzato il criterio attivo.

  Se questa opzione è disabilitata, le applicazioni utilizzeranno i criteri attivi.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Usa per ricevere solo aggiornamenti**

  Se questa opzione è abilitata, il profilo verrà utilizzato solo per il download degli aggiornamenti da parte delle applicazioni installate nel dispositivo client. Per le altre operazioni verrà stabilita la connessione ad Administration Server con le impostazioni di connessione iniziali definite durante l'installazione di Network Agent.

  Per impostazione predefinita, questa opzione è abilitata.

- **Sincronizza le impostazioni di connessione con le impostazioni di Administration Server specificate nel profilo**

Se questa opzione è abilitata, Network Agent si connette ad Administration Server utilizzando le impostazioni specificate nelle proprietà del profilo.

Se questa opzione è disabilitata, Network Agent si connette ad Administration Server utilizzando le impostazioni originali specificate durante l'installazione.

Questa opzione è disponibile se l'opzione **Usa per ricevere solo aggiornamenti** è disabilitata.

Per impostazione predefinita, questa opzione è disabilitata.

Verrà creato un profilo per la connessione di Network Agent ad Administration Server per gli utenti mobili. Quando Network Agent si connette ad Administration Server con questo profilo, le applicazioni installate in un dispositivo client utilizzeranno i criteri per i dispositivi in modalità fuori sede o i criteri fuori sede.

Informazioni sul passaggio di Network Agent ad altri Administration Server

Kaspersky Security Center offre un'opzione per effettuare il passaggio Network Agent di un dispositivo client ad altri Administration Server se cambiano le seguenti impostazioni di rete:

- **Condizione per l'indirizzo server DHCP**- L'indirizzo IP del server DHCP della rete è stato modificato.
- **Condizione per indirizzo gateway di connessione predefinito**- L'indirizzo del gateway principale della rete è stato modificato.
- **Condizione per dominio DNS**- Il suffisso DNS della subnet è stato modificato.
- **Condizione per l'indirizzo server DNS** - L'indirizzo IP del server DNS della rete è stato modificato.
- **Condizione per l'indirizzo del server WINS**- L'indirizzo IP del server WINS della rete è stato modificato. Questa impostazione è disponibile solo per i dispositivi che eseguono Windows.
- **Condizione per la risolvibilità del nome**- Il nome DNS o NetBIOS del dispositivo client è cambiato.
- **Condizione per subnet**- Modifica dell'indirizzo e della subnet mask.
- **Condizione per l'accessibilità dominio Windows**- Modifica dello stato del dominio Windows a cui il dispositivo client è connesso. Questa impostazione è disponibile solo per i dispositivi che eseguono Windows.
- **Condizione per l'accessibilità dell'indirizzo di connessione SSL**- Il dispositivo client può o non può (a seconda dell'opzione selezionata) stabilire una connessione SSL con un server specificato (nome: porta). È necessario utilizzare un server dedicato con software in grado di gestire un carico elevato e richieste di connessione frequenti di Network Agent. Non specificare la porta dell'Administration Server. Per ogni server è inoltre possibile specificare un certificato SSL. In questo caso, Network Agent verifica il certificato del server oltre a controllare la capacità di una connessione SSL. Se il certificato non corrisponde, la connessione non va a buon fine.

Questa funzionalità è supportata solo per i Network Agent installati nei dispositivi che eseguono Windows o macOS.

Le impostazioni iniziali della connessione di Network Agent ad Administration Server vengono definite durante l'installazione di Network Agent. Se sono state create regole per il passaggio del Network Agent ad altri Administration Server, Network Agent risponde alle modifiche delle impostazioni di rete nel modo seguente:

- Se le impostazioni di rete sono conformi a una delle regole create, Network Agent si connette all'Administration Server specificato in questa regola. Le applicazioni installate nei dispositivi client passano ai criteri fuori sede, a condizione che tale comportamento sia abilitato da una regola.
- Se non è applicabile alcuna regola, Network Agent ripristina le impostazioni predefinite della connessione all'Administration Server specificato durante l'installazione. Per le applicazioni installate nei dispositivi client vengono ripristinati i criteri attivi.
- Se l'Administration Server non è accessibile, Network Agent utilizzerà i criteri fuori sede.

Network Agent passa al criterio fuori sede solo se l'opzione **Abilita la modalità fuori sede quando Administration Server non è disponibile** è abilitata nelle impostazioni del criterio di Network Agent.

Le impostazioni della connessione di Network Agent all'Administration Server vengono salvate in un profilo. Nel profilo di connessione è possibile creare regole per il passaggio dei dispositivi client ai criteri fuori sede, nonché configurare il profilo in modo da utilizzarlo solo per il download degli aggiornamenti.

Creazione di una regola per il passaggio di Network Agent in base al percorso di rete

Il passaggio di Network Agent in base al percorso di rete è disponibile solo nei dispositivi che eseguono Windows e macOS.

Per creare una regola per il passaggio di Network Agent da un Administration Server all'altro in caso di modifiche delle impostazioni di rete:

1. Se si desidera creare una regola per un gruppo di dispositivi gestiti, aprire il criterio di Network Agent di questo gruppo. A tale scopo, procedere come segue:

   a. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

   b. Fare clic sul collegamento del percorso corrente.

   c. Nella finestra visualizzata selezionare il gruppo di amministrazione desiderato.

   Successivamente, il percorso corrente viene modificato.

   d. Aggiungere il criterio di Network Agent per il gruppo di dispositivi gestiti. Se è già stato creato, fare clic sul nome del criterio di Network Agent per aprire le proprietà del criterio.

2. Se si desidera creare una regola per un dispositivo gestito specifico, procedere come segue:

   a. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   b. Fare clic sul nome del dispositivo gestito.

   c. Nella finestra delle proprietà del dispositivo gestito visualizzata, passare alla scheda **Applicazioni**.

   d. Fare clic sul nome del criterio di Network Agent a cui si applica solo il dispositivo gestito selezionato.

3. Nella finestra delle proprietà visualizzata passare a **Impostazioni applicazione** → **Connettività** → **Profili connessione.**

4. Nella sezione **Impostazioni percorso di rete** fare clic sul pulsante **Aggiungi**.

5. Nella finestra delle proprietà visualizzata configurare la descrizione del percorso di rete e la regola per il passaggio. Specificare le seguenti impostazioni della descrizione del percorso di rete:

   - **Descrizione**

     Il nome della descrizione del percorso di rete non può essere superiore a 255 caratteri, né contenere simboli speciali come ("*<>?\/:|).

   - **Usa profilo connessione**

     Nell'elenco a discesa è possibile specificare il profilo di connessione utilizzato da Network Agent per connettersi ad Administration Server. Questo profilo verrà utilizzato quando sono soddisfatte le condizioni della descrizione del percorso di rete. Il profilo di connessione contiene le impostazioni per la connessione di Network Agent all'Administration Server e definisce in quali casi i dispositivi client devono passare ai criteri fuori sede. Il profilo viene utilizzato solo per scaricare gli aggiornamenti.

   - **Descrizione abilitata**

     Selezionare questa casella di controllo per abilitare l'utilizzo della nuova descrizione del percorso di rete.

6. Selezionare le condizioni per la regola per il passaggio di Network Agent:

   - **Condizione per l'indirizzo server DHCP**- L'indirizzo IP del server DHCP della rete è stato modificato.
   - **Condizione per indirizzo gateway di connessione predefinito**- L'indirizzo del gateway principale della rete è stato modificato.
   - **Condizione per dominio DNS**- Il suffisso DNS della subnet è stato modificato.
   - **Condizione per l'indirizzo server DNS** - L'indirizzo IP del server DNS della rete è stato modificato.
   - **Condizione per l'indirizzo del server WINS**- L'indirizzo IP del server WINS della rete è stato modificato. Questa impostazione è disponibile solo per i dispositivi che eseguono Windows.
   - **Condizione per la risolvibilità del nome**- Il nome DNS o NetBIOS del dispositivo client è cambiato.
   - **Condizione per subnet**- Modifica dell'indirizzo e della subnet mask.
   - **Condizione per l'accessibilità dominio Windows**- Modifica dello stato del dominio Windows a cui il dispositivo client è connesso. Questa impostazione è disponibile solo per i dispositivi che eseguono Windows.
   - **Condizione per l'accessibilità dell'indirizzo di connessione SSL**- Il dispositivo client può o non può (a seconda dell'opzione selezionata) stabilire una connessione SSL con un server specificato (nome: porta). Per ogni server è inoltre possibile specificare un certificato SSL. In questo caso, Network Agent verifica il certificato del server oltre a controllare la capacità di una connessione SSL. Se il certificato non corrisponde, la connessione non va a buon fine.

   Le condizioni in una regola vengono combinate utilizzando l'operatore logico AND. Per attivare una regola di passaggio in base alla descrizione del percorso di rete, devono essere soddisfatte tutte le condizioni della regola.

7. Nella sezione delle condizioni specificare quando è necessario che Network Agent passi a un altro Administration Server. A tale scopo, fare clic sul pulsante **Aggiungi**, quindi impostare il valore della condizione.

   Inoltre, l'opzione **Corrisponde ad almeno un valore dell'elenco** è abilitata per impostazione predefinita. È possibile disabilitare questa opzione se si desidera che la condizione venga soddisfatta con tutti i valori specificati.

8. Salvare le modifiche.

Verrà creata una nuova regola di passaggio in base alla descrizione del percorso di rete. Quando le condizioni della regola sono soddisfatte, Network Agent utilizza il profilo di connessione specificato nella regola per connettersi ad Administration Server.

Distribuzione guidata della protezione

Per installare le applicazioni Kaspersky, è possibile utilizzare la Distribuzione guidata della protezione. La Distribuzione guidata della protezione consente l'installazione remota delle applicazioni con pacchetti di installazione creati appositamente o direttamente da un pacchetto di distribuzione.

La Distribuzione guidata della protezione esegue le seguenti operazioni:

- Download di un pacchetto di installazione per l'installazione dell'applicazione (se non è già stato creato). Il pacchetto di installazione è disponibile in **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**. È possibile utilizzare questo pacchetto di installazione per l'installazione dell'applicazione in futuro.

- Creazione ed esecuzione di un'attività di installazione remota per dispositivi specifici o per un gruppo di amministrazione. La nuova attività di installazione remota creata viene archiviata nella sezione **Attività**. È possibile avviare manualmente questa attività in un secondo momento. Il tipo di attività è **Installa l'applicazione in remoto**.

Se si desidera installare Network Agent nei dispositivi con sistema operativo SUSE Linux Enterprise Server 15, installare il pacchetto insserv-compat prima di configurare Network Agent.

Passaggio 1. Avvio della Distribuzione guidata della protezione

Per avviare manualmente la Distribuzione guidata della protezione:

Nella finestra principale dell'applicazione, passare a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Distribuzione guidata della protezione**.

Verrà avviata la Distribuzione guidata della protezione. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

Passaggio 2. Selezione del pacchetto di installazione

Selezionare il pacchetto di installazione dell'applicazione che si desidera installare.

Se il pacchetto di installazione dell'applicazione desiderata non è elencato, fare clic sul pulsante **Aggiungi** e quindi selezionare l'applicazione dall'elenco.

Passaggio 3. Selezione di un metodo per la distribuzione del file chiave o del codice di attivazione

Selezionare un metodo per la distribuzione del file chiave o del codice di attivazione:

- **Non aggiungere la chiave di licenza al pacchetto di installazione**

  La chiave viene distribuita automaticamente a tutti i dispositivi con cui è compatibile:
  - Se la distribuzione automatica è stata abilitata nelle proprietà della chiave.
  - Se l'attività **Aggiungi chiave** è stata creata.

- **Aggiungi la chiave di licenza al pacchetto di installazione**

  La chiave verrà distribuita ai dispositivi insieme al pacchetto di installazione.

  Non è consigliabile distribuire la chiave utilizzando questo metodo poiché i diritti di accesso condiviso in lettura sono abilitati nell'archivio dei pacchetti di installazione.

Se il pacchetto di installazione include già un file chiave o un codice di attivazione, questa finestra viene visualizzata, ma contiene solo le informazioni della chiave di licenza.

Passaggio 4. Selezione della versione di Network Agent

Se è stato selezionato il pacchetto di installazione di un'applicazione diversa da Network Agent, è necessario installare anche Network Agent, che connette l'applicazione con Kaspersky Security Center Administration Server.

Selezionare la versione più recente di Network Agent.

Passaggio 5. Selezione dei dispositivi

Specificare un elenco di dispositivi in cui verrà installata l'applicazione:

- **Installa nei dispositivi gestiti**

  Se questa opzione è selezionata, l'attività di installazione remota viene creata per un gruppo di dispositivi.

- **Selezionare i dispositivi per l'installazione**

  L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

Passaggio 6. Specificazione delle impostazioni dell'attività di installazione remota

Nella pagina **Impostazioni dell'attività di installazione remota** specificare le impostazioni per l'installazione remota dell'applicazione.

Nel gruppo di impostazioni **Forza il download del pacchetto di installazione** specificare la modalità di distribuzione dei file necessari per l'installazione dell'applicazione ai dispositivi client:

- **Utilizzando Network Agent**

  Se questa opzione è abilitata, i pacchetti di installazione vengono distribuiti ai dispositivi client da Network Agent installato nei dispositivi client.

  Se questa opzione è disabilitata, i pacchetti di installazione vengono distribuiti utilizzando gli strumenti del sistema operativo dei dispositivi client.

  È consigliabile abilitare questa opzione se l'attività è stata assegnata a dispositivi in cui sono installati Network Agent.

  Per impostazione predefinita, questa opzione è abilitata.

- **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**

  Se questa opzione è abilitata, i pacchetti di installazione verranno trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo tramite i punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete.

  Se l'opzione **Utilizzo di Network Agent** è abilitata, i file vengono inviati tramite gli strumenti del sistema operativo solo se gli strumenti di Network Agent non sono disponibili.

  Per impostazione predefinita, questa opzione è abilitata per le attività di installazione remota create in un Administration Server virtuale.

- **Utilizzando le risorse del sistema operativo tramite Administration Server**

  Se questa opzione è selezionata, i file vengono trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo dei dispositivi client tramite l'Administration Server. È possibile abilitare questa opzione se Network Agent non è installato nel dispositivo client, ma il dispositivo client si trova nella stessa rete di Administration Server.

  Per impostazione predefinita, questa opzione è abilitata.

Definire le impostazioni aggiuntive:

- **Non reinstallare l'applicazione se è già installata**

  Se questa opzione è abilitata, l'applicazione selezionata non verrà reinstallata se è già stata installata nel dispositivo client.

  Se questa opzione è disabilitata, l'applicazione verrà installata in ogni caso.

  Per impostazione predefinita, questa opzione è abilitata.

- **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory**

  Se questa opzione è abilitata, un pacchetto di installazione viene installato utilizzando i criteri di gruppo di Active Directory.

  Questa opzione è disponibile se il pacchetto di installazione di Network Agent è selezionato.

  Per impostazione predefinita, questa opzione è disabilitata.

Passaggio 7. Gestione riavvio

Specificare l'azione da eseguire se il sistema operativo deve essere riavviato durante l'installazione dell'applicazione:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

  L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

  Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

  Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

  Per impostazione predefinita, questa opzione è disabilitata.

Passaggio 8. Rimozione delle applicazioni incompatibili prima dell'installazione

Questo passaggio è presente solo se l'applicazione da distribuire risulta incompatibile con alcune altre applicazioni.

Selezionare l'opzione se si desidera che Kaspersky Security Center rimuova automaticamente le applicazioni incompatibili con l'applicazione distribuita.

Viene visualizzato anche l'elenco delle applicazioni incompatibili.

Se non si seleziona questa opzione, l'applicazione verrà installata solo nei dispositivi in cui non sono presenti applicazioni incompatibili.

Passaggio 9. Spostamento dei dispositivi in Dispositivi gestiti

Specificare se i dispositivi devono essere spostati in un gruppo di amministrazione dopo l'installazione di Network Agent.

- **Non spostare i dispositivi**

  I dispositivi rimangono nei gruppi in cui si trovano attualmente. I dispositivi che non sono stati inseriti in alcun gruppo rimangono non assegnati.

- **Sposta i dispositivi non assegnati nel gruppo**

  I dispositivi vengono spostati nel gruppo di amministrazione selezionato.

L'opzione **Non spostare i dispositivi** è selezionata per impostazione predefinita. Per motivi di sicurezza, è consigliabile spostare i dispositivi manualmente.

Passaggio 10. Selezione degli account per l'accesso ai dispositivi

Se necessario, aggiungere gli account che verranno utilizzati per avviare l'attività di installazione remota:

- **Nessun account richiesto (Network Agent installato)**

  Se questa opzione è selezionata, non è necessario specificare un account con cui verrà eseguito il programma di installazione dell'applicazione. L'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

  Se Network Agent non è stato installato nei dispositivi client, questa opzione non è disponibile.

- **Account richiesto (Network Agent non utilizzato)**

Selezionare questa opzione se Network Agent non è installato nei dispositivi a cui si assegna l'attività di installazione remota. In questo caso, è possibile specificare un account utente o un certificato SSH per installare l'applicazione.

- **Account locale**. Se questa opzione è selezionata, specificare l'account utente con cui verrà eseguito il programma di installazione dell'applicazione. Fare clic sul pulsante **Aggiungi**, selezionare **Account locale** e quindi specificare le credenziali dell'account utente.

  È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi per cui si assegna l'attività. In questo caso, tutti gli account aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

- **Certificato SSH**. Se si desidera installare un'applicazione in un dispositivo client basato su Linux, è possibile specificare un certificato SSH anziché un account utente. Fare clic sul pulsante **Aggiungi**, selezionare **Certificato SSH**, quindi specificare la chiave privata e quella pubblica del certificato.

  Per generare una chiave privata, è possibile utilizzare l'utilità ssh-keygen. Si noti che Kaspersky Security Center supporta il formato PEM delle chiavi private, ma l'utilità ssh-keygen genera chiavi SSH nel formato OPENSSH per impostazione predefinita. Il formato OPENSSH non è supportato da Kaspersky Security Center. Per creare una chiave privata nel formato PEM supportato, aggiungere l'opzione -m PEM nel comando ssh-keygen. Ad esempio:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail dell'utente>"
  ```

Passaggio 11. Avvio dell'installazione

Questo è il passaggio finale della procedura guidata. A questo punto, l'**Attività di installazione remota** è stata creata e configurata correttamente.

Per impostazione predefinita, l'opzione **Esegui l'attività al termine della procedura guidata** non è selezionata. Se si seleziona questa opzione, l'**Attività di installazione remota** verrà avviata immediatamente dopo il completamento della procedura guidata. Se non si seleziona questa opzione, l'**Attività di installazione remota** non verrà avviata. È possibile avviare manualmente questa attività in un secondo momento.

Fare clic su **OK** per completare il passaggio finale della Distribuzione guidata della protezione.

Distribuzione delle applicazioni Kaspersky tramite Kaspersky Security Center Web Console

In questa sezione viene descritta la distribuzione delle applicazioni Kaspersky nei dispositivi client dell'organizzazione tramite Kaspersky Security Center Web Console.

Scenario: Distribuzione delle applicazioni Kaspersky tramite Kaspersky Security Center Web Console

In questo scenario viene descritto come distribuire le applicazioni Kaspersky tramite Kaspersky Security Center Web Console. È possibile utilizzare l'Avvio rapido guidato e la Distribuzione guidata della protezione oppure completare manualmente tutti i passaggi necessari.

Le seguenti applicazioni sono disponibili per la distribuzione tramite Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

Passaggi

La distribuzione delle applicazioni Kaspersky prevede diversi passaggi:

1. **Download del plug-in di gestione per l'applicazione**

   Questo passaggio viene gestito dall'Avvio rapido guidato. Se si sceglie di non eseguire la procedura guidata, scaricare manualmente il plug-in per Kaspersky Endpoint Security for Windows.

   Se si intende gestire i dispositivi mobili aziendali, seguire le istruzioni fornite nella Guida di Kaspersky Security for Mobile per scaricare e installare i plug-in di gestione per Kaspersky Endpoint Security for Android.

2. **Download e creazione dei pacchetti di installazione**

   Questo passaggio viene gestito dall'Avvio rapido guidato.

   L'Avvio rapido guidato consente di scaricare il pacchetto di installazione con il plug-in di gestione. Se non è stata selezionata questa opzione durante l'esecuzione della procedura guidata o se la procedura guidata non è stata eseguita affatto, è necessario scaricare il pacchetto manualmente.

   Se non è possibile installare le applicazioni Kaspersky tramite Kaspersky Security Center in alcuni dispositivi, ad esempio nei dispositivi dei dipendenti remoti, è possibile creare pacchetti di installazione indipendenti per le applicazioni. Se si utilizzano pacchetti indipendenti per installare le applicazioni Kaspersky, non è necessario creare ed eseguire un'attività di installazione remota, né creare e configurare attività per Kaspersky Endpoint Security for Windows.

3. **Creazione, configurazione ed esecuzione dell'attività di installazione remota**

   Per Kaspersky Endpoint Security for Windows, questo passaggio fa parte della Distribuzione guidata della protezione, che viene avviata automaticamente al termine dell'Avvio rapido guidato. Se si sceglie di non eseguire la Distribuzione guidata della protezione, è necessario creare questa attività manualmente e configurarla manualmente.

   È inoltre possibile creare manualmente diverse attività di installazione remota per diversi gruppi di amministrazione o diverse selezioni dispositivi. È possibile distribuire versioni differenti di un'applicazione in queste attività.

   Assicurarsi che vengano rilevati tutti i dispositivi nella rete, quindi eseguire l'attività (o le attività) di installazione remota.

   > Installare il programma di installazione dell'utilità nmap sulle risorse basate su Linux. Questa utilità è necessaria per abilitare la funzionalità Network Location Awareness.

Se si desidera installare Network Agent nei dispositivi con sistema operativo SUSE Linux Enterprise Server 15, installare il pacchetto insserv-compat prima di configurare Network Agent.

Se si desidera installare Network Agent nei dispositivi con il sistema operativo RED OS 7.3.4 o versione successiva o MSVSPHERE 9.2 o versione successiva, installare il pacchetto libxcrypt-compat per il corretto funzionamento di Network Agent.

4. **Creazione e configurazione delle attività per l'applicazione gestita**

   È necessario configurare l'attività *Installa aggiornamento* di Kaspersky Endpoint Security for Windows.

   Questo passaggio fa parte dell'Avvio rapido guidato: l'attività verrà creata e configurata automaticamente con le impostazioni predefinite. Se la procedura guidata non è stata eseguita, è necessario creare questa attività manualmente e configurarla manualmente. Se si utilizza l'Avvio rapido guidato, assicurarsi che la pianificazione dell'attività soddisfi i requisiti. Per impostazione predefinita, l'avvio pianificato dell'attività è impostato su **Manualmente**, ma è consigliabile scegliere un'altra opzione.

   Altre applicazioni Kaspersky potrebbero avere altre attività predefinite. Fare riferimento alla documentazione delle applicazioni corrispondenti per informazioni dettagliate.

   Assicurarsi che la pianificazione per ciascuna attività creata soddisfi i requisiti.

5. **Installazione di Kaspersky Security for Mobile (opzionale)**

   Se si intende gestire i dispositivi mobili aziendali, seguire le istruzioni fornite nella Guida di Kaspersky Security for Mobile per informazioni sulla distribuzione di Kaspersky Endpoint Security for Android.

6. **Creazione dei criteri in corso**

   Creare il criterio per ciascuna applicazione manualmente o (nel caso di Kaspersky Endpoint Security for Windows) tramite l'Avvio rapido guidato. È possibile utilizzare le impostazioni predefinite del criterio, nonché modificare le impostazioni predefinite del criterio in base alle esigenze in qualsiasi momento.

7. **Verifica dei risultati**

   Assicurarsi che la distribuzione sia stata completata correttamente: sono disponibili criteri e attività per ciascuna applicazione e tali applicazioni sono installate nei dispositivi gestiti.

Risultati

Il completamento dello scenario dà i seguenti risultati:

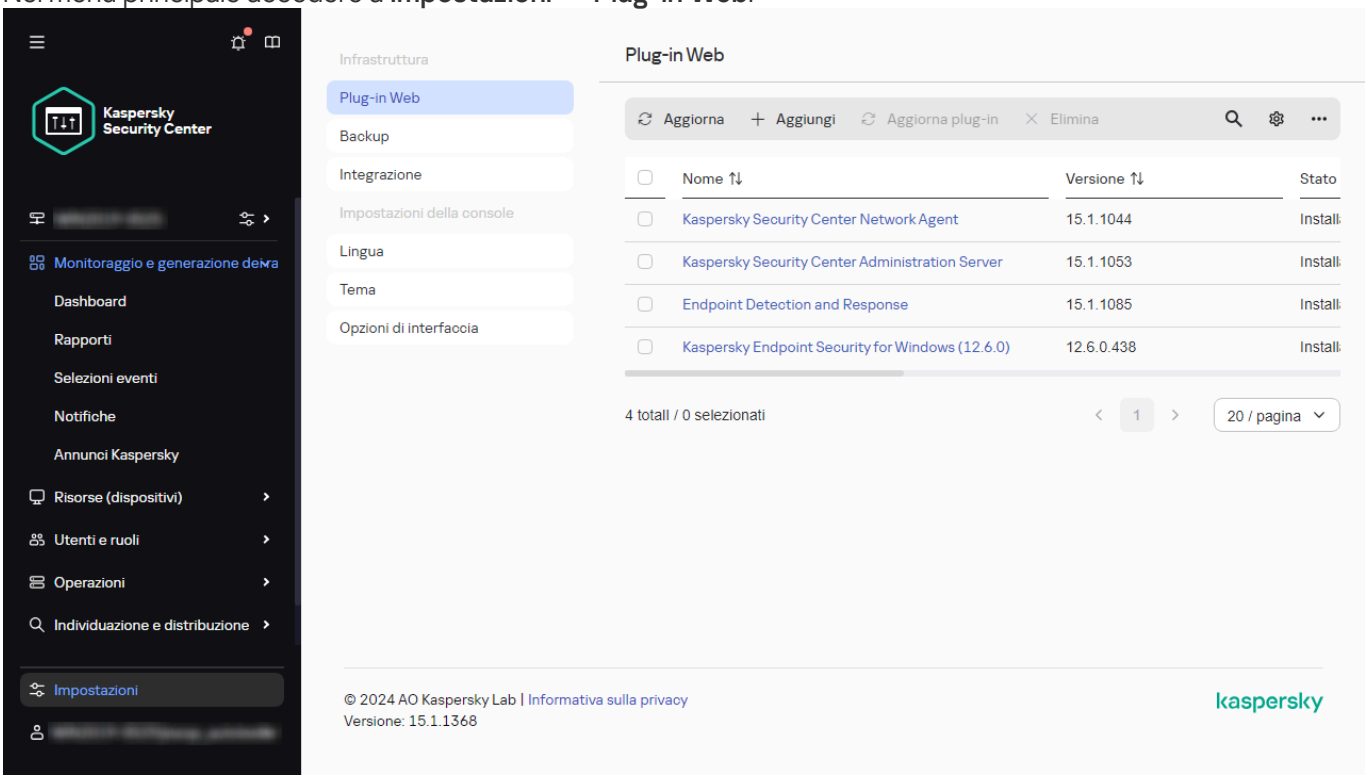
- Vengono creati tutti i criteri e le attività richiesti per le applicazioni selezionate.
- Le pianificazioni delle attività sono configurate in base alle esigenze.
- Le applicazioni selezionate sono distribuite, o pianificate per essere distribuite, nei dispositivi client selezionati.

Recupero dei plug-in per le applicazioni Kaspersky

Per distribuire un'applicazione Kaspersky, come Kaspersky Endpoint Security for Windows, è necessario scaricare il plug-in di gestione per l'applicazione.

Per scaricare un plug-in di gestione per un'applicazione Kaspersky:

1. Nel menu principale accedere a **Impostazioni** → **Plug-in Web**.



Elenco dei plug-in Web installati

2. Nella finestra visualizzata fare clic sul pulsante **Aggiungi**.

   Verrà visualizzato l'elenco dei plug-in disponibili.

3. Nell'elenco dei plug-in disponibili selezionare il plug-in che si desidera scaricare (ad esempio, Kaspersky Endpoint Security 11 for Windows) facendo clic sul relativo nome.

   Verrà visualizzata una pagina di descrizione del plug-in.

4. Nella pagina di descrizione del plug-in fare clic su **Installa plug-in**.

5. Al termine dell'installazione, fare clic su **OK**.

Il plug-in di gestione verrà scaricato con la configurazione predefinita e visualizzato nell'elenco dei plug-in di gestione.

È possibile aggiungere plug-in e aggiornare i plug-in scaricati da un file. È possibile scaricare i plug-in di gestione e i plug-in di gestione Web dalla pagina Web del Servizio di assistenza tecnica Kaspersky.

Per scaricare o aggiornare il plug-in da un file:

1. Nel menu principale accedere a **Impostazioni** → **Plug-in Web**.

2. Eseguire una delle seguenti operazioni:

   - Fare clic su **Aggiungi da file** per scaricare un plug-in da un file.
   - Fare clic su **Aggiorna da file** per scaricare l'aggiornamento di un plug-in da un file.

3. Specificare il file e la firma del file.

4. Scaricare i file specificati.

Il plug-in di gestione verrà scaricato dal file e visualizzato nell'elenco dei plug-in di gestione.

Download e creazione dei pacchetti di installazione per le applicazioni Kaspersky

È possibile creare pacchetti di installazione per le applicazioni Kaspersky dai server Web di Kaspersky se l'Administration Server dispone di accesso a Internet.

Per scaricare e creare il pacchetto di installazione per l'applicazione Kaspersky:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   È anche possibile visualizzare le notifiche relative ai nuovi pacchetti per le applicazioni Kaspersky nell'elenco delle notifiche sullo schermo. Se sono presenti notifiche relative a un nuovo pacchetto, è possibile fare clic sul collegamento accanto alla notifica e passare all'elenco dei pacchetti di installazione disponibili.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Fare clic su **Aggiungi**.

   Viene avviata la Creazione guidata nuovo pacchetto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Selezionare **Crea pacchetto di installazione per un'applicazione Kaspersky**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili sui server Web di Kaspersky. L'elenco contiene i pacchetti di installazione solo per le applicazioni compatibili con la versione corrente di Kaspersky Security Center.

4. Fare clic sul nome di un pacchetto di installazione, ad esempio Kaspersky Endpoint Security for Windows (11.1.0).

   Verrà visualizzata una finestra con le informazioni sul pacchetto di installazione.

   È possibile scaricare e utilizzare un pacchetto di installazione che includa strumenti di criptaggio che implementano la crittografia avanzata, se conforme alle leggi e ai regolamenti vigenti. Per scaricare il pacchetto di installazione di Kaspersky Endpoint Security for Windows valido per le esigenze aziendali, consultare le normative del paese in cui si trovano i dispositivi client dell'organizzazione.

5. Leggere le informazioni e fare clic sul pulsante **Scarica e crea pacchetto di installazione**.

   Se un pacchetto di distribuzione non può essere convertito in un pacchetto di installazione, viene visualizzato il pulsante **Scarica pacchetto di distribuzione** anziché **Scarica e crea pacchetto di installazione**.

   Verrà avviato il download del pacchetto di installazione in Administration Server. È possibile chiudere la finestra della procedura guidata o procedere al passaggio successivo della procedura. Se si chiude la finestra della procedura guidata, il processo di download continuerà in background.

   Se si desidera tenere traccia del processo di download di un pacchetto di installazione:

   a. Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione** → **In corso ()**.

   b. Tenere traccia dello stato di avanzamento dell'operazione nella colonna **Stato di avanzamento del download** e nella colonna **Stato del download** della tabella.

   Al termine del processo, il pacchetto di installazione viene aggiunto all'elenco nella scheda **Download eseguito**. Se il processo di download si interrompe e lo stato del download passa a **Accetta Contratto di licenza con l'utente finale**, fare clic sul nome del pacchetto di installazione, quindi procedere al passaggio successivo della procedura.

   > Se la dimensione dei dati contenuti nel pacchetto di distribuzione selezionato supera il limite corrente, viene visualizzato un messaggio di errore. È possibile modificare il valore limite, quindi procedere con la creazione del pacchetto di installazione.

6. Per alcune applicazioni Kaspersky, durante il processo di download viene visualizzato il pulsante **Mostra Contratto di licenza con l'utente finale**. Se viene visualizzato, procedere come segue:

   a. Fare clic sul pulsante **Mostra Contratto di licenza con l'utente finale** per leggere il Contratto di licenza con l'utente finale (EULA).

   b. Leggere il Contratto di licenza con l'utente finale visualizzato, quindi fare clic su **Accetta**.

      Dopo aver accettato il Contratto di licenza con l'utente finale, il download prosegue. Se si fa clic su **Rifiuta**, il download viene interrotto.

7. Al termine del download, fare clic sul pulsante **Chiudi**.

Il pacchetto di installazione selezionato verrà scaricato nella cartella condivisa di Administration Server, nella sottocartella Pacchetti. Dopo il download, il pacchetto di installazione viene visualizzato nell'elenco dei pacchetti di installazione.

Modifica del limite relativo alle dimensioni dei dati del pacchetto di installazione personalizzato

Le dimensioni totali dei dati decompressi durante la creazione di un pacchetto di installazione personalizzato sono limitate. Il limite predefinito è 1 GB.

Se si tenta di caricare un file di archivio contenente dati che superano il limite corrente, viene visualizzato un messaggio di errore. Potrebbe essere necessario aumentare questo valore limite durante la creazione dei pacchetti di installazione a partire da pacchetti di distribuzione di grandi dimensioni.

Per modificare il valore limite per le dimensioni del pacchetto di installazione personalizzato:

1. Nel dispositivo Administration Server, eseguire il prompt dei comandi con l'account utilizzato per installare Administration Server.

2. Sostituire la directory corrente con la cartella di installazione di Kaspersky Security Center (in genere, <Disco>:\Programmi (x86)\Kaspersky Lab\Kaspersky Security Center).

3. A seconda del tipo di installazione di Administration Server, immettere uno dei seguenti comandi, utilizzando i diritti di amministratore:

   - Installazione locale normale:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <numero di byte>
     ```

   - Installazione nel cluster di failover Kaspersky Security Center:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <numero di byte> --stp klfoc
     ```

   - Installazione in un cluster di failover di Windows Server:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <numero di byte> --stp cluster
     ```

   Dove <numero di byte> è un numero di byte in formato esadecimale o decimale.

   Ad esempio, se il limite richiesto è 2 GB, è possibile specificare il valore decimale 2147483648 o il valore esadecimale 0x80000000. In questo caso, per un'installazione locale di Administration Server, è possibile utilizzare il seguente comando:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

Il limite relativo alle dimensioni dei dati del pacchetto di installazione personalizzato è stato modificato.

Download dei pacchetti di distribuzione per le applicazioni Kaspersky

In Kaspersky Security Center Web Console è possibile scaricare e salvare i pacchetti di distribuzione per le applicazioni Kaspersky. È possibile utilizzare i pacchetti di distribuzione per installare le applicazioni manualmente, senza utilizzare Kaspersky Security Center.

Per scaricare e salvare i pacchetti di distribuzione per le applicazioni Kaspersky:

1. Nel menu principale, passare a **Operazioni** → **Applicazioni Kaspersky** → **Versioni correnti delle applicazioni**.

   Verrà visualizzato un elenco dei pacchetti di distribuzione, dei plug-in e delle patch disponibili. Kaspersky Security Center visualizza solo gli elementi compatibili con la versione corrente.

2. Nell'elenco fare clic sul nome del pacchetto che si desidera scaricare.

   Verrà visualizzata la descrizione del pacchetto.

3. Leggere la descrizione e fare clic sul pulsante **Scarica e crea pacchetto di installazione**.

   Se un pacchetto di distribuzione non può essere convertito in un pacchetto di installazione, viene visualizzato il pulsante **Scarica pacchetto di distribuzione** anziché **Scarica e crea pacchetto di installazione**.

   Verrà avviato il download del pacchetto di installazione in Administration Server.

Il pacchetto di installazione o di distribuzione selezionato verrà scaricato nella cartella condivisa di Administration Server, nella sottocartella **Pacchetti**. Dopo il download, il pacchetto di installazione viene visualizzato nell'elenco dei pacchetti di installazione.

Controllo della corretta distribuzione di Kaspersky Endpoint Security

Per verificare di avere distribuito correttamente le applicazioni Kaspersky, come Kaspersky Endpoint Security:

1. Utilizzando Kaspersky Security Center Web Console, assicurarsi di disporre dei seguenti elementi:
   - Un criterio per Kaspersky Endpoint Security e/o le altre applicazioni di protezione utilizzate.
   - Attività per Kaspersky Endpoint Security for Windows: attività *Scansione rapida* e attività *Installa aggiornamento* (se si utilizza Kaspersky Endpoint Security for Windows).
   - Attività per le altre applicazioni di protezione utilizzate.
2. In uno dei dispositivi gestiti, selezionato per l'installazione, verificare quanto segue:
   - Kaspersky Endpoint Security o un'altra applicazione di protezione Kaspersky è installata.
   - In Kaspersky Endpoint Security, le impostazioni di Protezione minacce file, Protezione minacce Web e Protezione minacce di posta corrispondono ai criteri creati per il dispositivo.
   - Il servizio Kaspersky Endpoint Security può essere arrestato e avviato manualmente.
   - Le attività di gruppo possono essere arrestate e avviate manualmente.

Creazione di pacchetti di installazione indipendenti

Gli utenti dei dispositivi nell'organizzazione possono utilizzare pacchetti di installazione indipendenti per installare manualmente le applicazioni nei dispositivi.

Un pacchetto di installazione indipendente è un file eseguibile (installer.exe) che può essere archiviato nel server Web, in una cartella condivisa, inviato per e-mail oppure trasferito a un dispositivo client utilizzando un altro metodo. Nel dispositivo client l'utente può eseguire il file ricevuto in locale per installare un'applicazione senza coinvolgere Kaspersky Security Center. È possibile creare pacchetti di installazione indipendenti per le applicazioni Kaspersky e per applicazioni di terze parti per piattaforme Windows, macOS e Linux. Per creare un pacchetto di installazione indipendente per un'applicazione di terze parti, è necessario creare un pacchetto di installazione personalizzato.

Assicurarsi che il pacchetto di installazione indipendente non sia disponibile per persone non autorizzate.

Per creare un pacchetto di installazione indipendente:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Nell'elenco dei pacchetti di installazione selezionare un pacchetto di installazione e, sopra l'elenco, fare clic sul pulsante **Distribuisci**.

3. Selezionare l'opzione **Utilizzo di un pacchetto indipendente**.

   Verrà avviata la Creazione guidata pacchetto di installazione indipendente. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Assicurarsi che l'opzione **Installa Network Agent con questa applicazione**, se si desidera installare Network Agent insieme all'applicazione selezionata.

   L'opzione viene visualizzata a seconda dell'applicazione per la quale si crea un pacchetto di installazione indipendente.

   Per impostazione predefinita, questa opzione è abilitata. È consigliabile abilitare questa opzione se non si è sicuri che Network Agent sia installato nel dispositivo. Se Network Agent è già installato nel dispositivo, dopo l'installazione del pacchetto di installazione indipendente con Network Agent, Network Agent verrà aggiornato alla versione più recente.

   Se si disabilita questa opzione, Network Agent non verrà installato nel dispositivo e il dispositivo non sarà gestito.

   Se un pacchetto di installazione indipendente per l'applicazione selezionata esiste già in Administration Server, la procedura guidata informa l'utente. In questo caso, è necessario selezionare una delle seguenti azioni:

   - **Crea pacchetto di installazione indipendente**. Selezionare questa opzione se, ad esempio, si desidera creare un pacchetto di installazione indipendente per una nuova versione dell'applicazione e si desidera mantenere anche un pacchetto di installazione indipendente creato per una versione precedente dell'applicazione. Il nuovo pacchetto di installazione indipendente viene inserito in un'altra cartella.
   - **Usa pacchetto di installazione indipendente esistente**. Selezionare questa opzione se si desidera utilizzare un pacchetto di installazione indipendente esistente. Il processo di creazione del pacchetto non verrà avviato.
   - **Ricrea pacchetto di installazione indipendente esistente**. Selezionare questa opzione se si desidera creare nuovamente un pacchetto di installazione indipendente per la stessa applicazione. Il pacchetto di installazione indipendente viene inserito nella stessa cartella.

5. Nel passaggio **Sposta nell'elenco dei dispositivi gestiti**, l'opzione **Non spostare i dispositivi** è abilitata per impostazione predefinita. Se non si desidera spostare il dispositivo client in un gruppo di amministrazione dopo l'installazione di Network Agent, lasciare l'opzione abilitata.

   Se si desidera spostare il dispositivo client dopo l'installazione di Network Agent, selezionare l'opzione **Sposta i dispositivi non assegnati in questo gruppo** e specificare un gruppo di amministrazione in cui spostare il dispositivo client. Per impostazione predefinita, il dispositivo viene spostato nel gruppo **Dispositivi gestiti**.

6. Al termine del processo di creazione del pacchetto di installazione indipendente, fare clic sul pulsante **FINE**.

   La Creazione guidata pacchetto di installazione indipendente verrà chiusa.

Il pacchetto di installazione indipendente viene creato e inserito nella sottocartella PkgInst della cartella condivisa di Administration Server. È possibile visualizzare l'elenco dei pacchetti indipendenti facendo clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti** sopra l'elenco dei pacchetti di installazione.

Visualizzazione dell'elenco dei pacchetti di installazione indipendenti

È possibile visualizzare l'elenco dei pacchetti di installazione indipendenti e le proprietà di ciascun pacchetto di installazione indipendente.

Per visualizzare l'elenco dei pacchetti di installazione indipendenti per tutti i pacchetti di installazione:

Sopra l'elenco, fare clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti**.

Nell'elenco dei pacchetti di installazione indipendenti le relative proprietà vengono visualizzate come segue:

- **Nome pacchetto**. Nome del pacchetto di installazione indipendente, formato automaticamente dal nome dell'applicazione incluso nel pacchetto e dalla versione dell'applicazione.
- **Nome applicazione**. Nome dell'applicazione incluso nel pacchetto di installazione indipendente.
- **Versione applicazione**.
- **Nome pacchetto di installazione di Network Agent**. La proprietà viene visualizzata solo se Network Agent è incluso nel pacchetto di installazione indipendente.
- **Versione di Network Agent**. La proprietà viene visualizzata solo se Network Agent è incluso nel pacchetto di installazione indipendente.
- **Dimensione**. Dimensione del file in MB.
- **Gruppo**. Nome del gruppo in cui viene spostato il dispositivo client dopo l'installazione di Network Agent.
- **Data creazione**. Data e ora di creazione del pacchetto di installazione indipendente.
- **Ultima modifica**. Data e ora di modifica del pacchetto di installazione indipendente.
- **Percorso**. Percorso completo della cartella in cui si trova il pacchetto di installazione indipendente.

- **Indirizzo Web**. Indirizzo Web del pacchetto di installazione indipendente.
- **Hash del file**. La proprietà viene utilizzata per certificare che il pacchetto di installazione indipendente non è stato modificato da terze parti e che un utente ha lo stesso file che è stato creato e trasferito all'utente.

Per visualizzare l'elenco dei pacchetti di installazione indipendenti per un pacchetto di installazione specifico:

Selezionare il pacchetto di installazione nell'elenco e, sopra l'elenco, fare clic sul pulsante **Visualizza l'elenco dei pacchetti indipendenti**.

Nell'elenco dei pacchetti di installazione indipendenti è possibile eseguire le seguenti operazioni:

- Pubblicare un pacchetto di installazione indipendente sul server Web facendo clic sul pulsante **Pubblica**. Il pacchetto di installazione indipendente pubblicato è disponibile per il download per gli utenti a cui è stato inviato il collegamento al pacchetto di installazione indipendente.
- Annullare la pubblicazione di un pacchetto di installazione indipendente sul server Web facendo clic sul pulsante **Annulla pubblicazione**. Il pacchetto di installazione indipendente non pubblicato è disponibile per il download solo per gli amministratori.
- Scaricare un pacchetto di installazione indipendente nel dispositivo facendo clic sul pulsante **Scarica**.
- Inviare un messaggio e-mail con il collegamento a un pacchetto di installazione indipendente facendo clic sul pulsante **Invia tramite e-mail**.
- Rimuovere un pacchetto di installazione indipendente facendo clic sul pulsante **Rimuovi**.

Creazione di pacchetti di installazione personalizzati

È possibile utilizzare pacchetti di installazione personalizzati per effettuare le seguenti operazioni:

- Installare qualsiasi applicazione (come un editor di testo) in un dispositivo client, ad esempio mediante un'attività.
- Creare un pacchetto di installazione indipendente.

Un pacchetto di installazione personalizzato è una cartella con un set di file. L'origine per creare un pacchetto di installazione personalizzato è un *file di archivio*. Il file di archivio contiene uno o più file che devono essere inclusi nel pacchetto di installazione personalizzato. Durante la creazione di un pacchetto di installazione personalizzato, è possibile specificare i parametri della riga di comando, ad esempio per installare l'applicazione in modalità automatica.

Se si dispone di una chiave di licenza attiva per la funzionalità Vulnerability e patch management (VAPM), è possibile convertire le impostazioni di installazione predefinite per il pacchetto di installazione personalizzato appropriato e utilizzare i valori consigliati dagli esperti di Kaspersky. Le impostazioni vengono convertite automaticamente durante la creazione del pacchetto di installazione personalizzato solo se il file eseguibile corrispondente è incluso nel database Kaspersky di applicazioni di terze parti.

Per creare un pacchetto di installazione personalizzato:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Fare clic su **Aggiungi**.

   Viene avviata la Creazione guidata nuovo pacchetto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Selezionare **Crea pacchetto di installazione da un file**.

4. Specificare il nome del pacchetto e fare clic sul pulsante **Sfoglia**.

   Nel browser verrà visualizzata una finestra standard **Apri** di Windows per la selezione di un file per creare il pacchetto di installazione.

5. Scegliere un file di archivio presente nei dischi disponibili.

   È possibile caricare un file di archivio ZIP, CAB, TAR o TAR.GZ. Non è possibile creare un pacchetto di installazione da un file SFX (archivio autoestraente).

   > Se si desidera convertire le impostazioni durante l'installazione del pacchetto, verificare che la casella di controllo **Convertire le impostazioni nei valori consigliati per le applicazioni riconosciute da Kaspersky Security Center al termine della procedura guidata** sia selezionata e fare clic su **Avanti**.

   Verrà avviato il caricamento del file in Kaspersky Security Center Administration Server.

   > Se è stato abilitato l'utilizzo delle impostazioni di installazione consigliate, Kaspersky Security Center 15.1 verifica se il file eseguibile è incluso nel database Kaspersky di applicazioni di terze parti. Se il controllo ha esito positivo, verrà visualizzata una notifica che segnala che il file è stato riconosciuto. Le impostazioni vengono convertite e viene creato il pacchetto di installazione personalizzato. Non sono necessarie ulteriori operazioni. Fare clic sul pulsante **Fine** per chiudere la procedura guidata.

6. Selezionare un file (dall'elenco dei file estratti dal file di archivio scelto) e specificare i parametri della riga di comando di un file eseguibile.

   È possibile specificare i parametri della riga di comando per installare l'applicazione dal pacchetto di installazione in modalità automatica. Specificare i parametri della riga di comando è un'operazione facoltativa.

   Viene avviata la procedura per creare il pacchetto di installazione.

   La procedura guidata informa l'utente al termine della procedura.

   Se il pacchetto di installazione non viene creato, viene visualizzato un messaggio appropriato.

7. Fare clic sul pulsante **Fine** per chiudere la procedura guidata.

Il pacchetto di installazione creato viene scaricato nella sottocartella Pacchetti della cartella condivisa di Administration Server. Dopo il download, il pacchetto di installazione viene visualizzato nell'elenco dei pacchetti di installazione.

Nell'elenco dei pacchetti di installazione disponibili in Administration Server, facendo clic sul collegamento con il nome di un pacchetto di installazione personalizzato, è possibile:

- Visualizzare le seguenti proprietà di un pacchetto di installazione:
  - **Nome**. Nome del pacchetto di installazione personalizzato.
  - **Origine**. Nome del produttore dell'applicazione.
  - **Applicazione**. Nome dell'applicazione inclusa nel pacchetto di installazione personalizzato.
  - **Versione**. Versione applicazione.
  - **Lingua**. Lingua dell'applicazione inclusa nel pacchetto di installazione personalizzato.
  - **Dimensioni (MB)**. Dimensioni del pacchetto di installazione.
  - **Sistema operativo**. Tipo di sistema operativo a cui è destinato il pacchetto di installazione.
  - **Data creazione**. Data di creazione del pacchetto di installazione.
  - **Ultima modifica**. Data di modifica del pacchetto di installazione.
  - **Tipo**. Tipo di pacchetto di installazione.
- Modificare il nome del pacchetto e i parametri della riga di comando. Questa funzionalità è disponibile solo per i pacchetti che non vengono creati in base alle applicazioni Kaspersky.

Se per il processo di creazione del pacchetto personalizzato le impostazioni di installazione del pacchetto sono state convertite nei valori consigliati, potrebbero essere visualizzate due sezioni aggiuntive nella scheda **Impostazioni** delle proprietà del pacchetto di installazione personalizzato: **Impostazioni** e **Procedura di installazione**.

La sezione **Impostazioni** contiene le seguenti proprietà, visualizzate in una tabella:

- **Nome**. Questa colonna mostra il nome assegnato a un parametro di installazione.
- **Tipo**. Questa colonna mostra il tipo di un parametro di installazione.
- **Valore**. Questa colonna mostra il tipo di dati definito da un parametro di installazione (booleano, percorso del file, numerico, percorso o stringa).

La sezione **Procedura di installazione** contiene una tabella che descrive le seguenti proprietà dell'aggiornamento incluso nel pacchetto di installazione personalizzato:

- **Nome**. Nome dell'aggiornamento.
- **Descrizione**. Descrizione dell'aggiornamento.
- **Origine**. Origine dell'aggiornamento, ovvero se è stato rilasciato da Microsoft o da un altro sviluppatore di terze parti.
- **Tipo**. Tipo di aggiornamento, ovvero se è destinato a un driver o a un'applicazione.

- **Categoria**. Categoria WSUS (Windows Server Update Services) visualizzata per gli aggiornamenti Microsoft (Aggiornamenti critici, Aggiornamenti definizione, Driver, Feature Pack, Aggiornamenti della protezione, Service Pack, Strumenti, Aggiornamenti cumulativi, Aggiornamenti o Upgrade).
- **Livello di importanza in base a MSRC**. Livello di importanza dell'aggiornamento definito da Microsoft Security Response Center (MSRC).
- **Livello di importanza**. Livello di importanza dell'aggiornamento definito da Kaspersky.
- **Livello di importanza patch (per le patch destinate alle applicazioni Kaspersky)**. Livello di importanza della patch, se è destinata a un'applicazione Kaspersky.
- **Articolo**. Identificatore (ID) dell'articolo nella Knowledge Base che descrive l'aggiornamento.
- **Bollettino**. ID del bollettino sulla sicurezza che descrive l'aggiornamento.
- **Non assegnato per l'installazione**. Indica se l'aggiornamento ha lo stato Non assegnato per l'installazione.
- **Da installare**. Indica se l'aggiornamento ha lo stato Da installare.
- **Installazione in corso**. Indica se l'aggiornamento ha lo stato Installazione in corso.
- **Installato**. Indica se l'aggiornamento ha lo stato Installato.
- **Non riuscito**. Indica se l'aggiornamento ha lo stato Non riuscito.
- **È necessario il riavvio**. Indica se l'aggiornamento ha lo stato È necessario il riavvio.
- **Registrato**. Indica la data e l'ora in cui è stato registrato l'aggiornamento.
- **Installato in modalità interattiva**. Indica se l'aggiornamento richiede l'interazione con l'utente durante l'installazione.
- **Revocato**. Indica la data e l'ora in cui l'aggiornamento è stato revocato.
- **Stato di approvazione dell'aggiornamento**. Indica se l'aggiornamento è approvato per l'installazione.
- **Revisione**. Indica il numero di revisione corrente dell'aggiornamento.
- **ID aggiornamento**. Indica l'ID dell'aggiornamento.
- **Versione applicazione**. Visualizza il numero di versione a cui verrà aggiornata l'applicazione.
- **Sostituiti**. Indica altri aggiornamenti che possono sostituire l'aggiornamento.
- **Sostituzione**. Indica altri aggiornamenti che possono essere sostituiti dall'aggiornamento.
- **È necessario accettare i termini del Contratto di licenza**. Indica se l'aggiornamento richiede l'accettazione dei termini di un Contratto di licenza con l'utente finale (EULA).
- **Vendor**. Indica il nome del fornitore dell'aggiornamento.
- **Famiglia di applicazioni**. Indica il nome della famiglia di applicazioni a cui appartiene l'aggiornamento.
- **Applicazione**. Indica il nome dell'applicazione a cui appartiene l'aggiornamento.

- **Lingua**. Indica la lingua della localizzazione dell'aggiornamento.
- **Non assegnato per l'installazione (nuova versione)**. Indica se l'aggiornamento ha lo stato Non assegnato per l'installazione (nuova versione).
- **Richiede l'installazione dei prerequisiti**. Indica se l'aggiornamento ha lo stato Richiede l'installazione dei prerequisiti.
- **Modalità di download**. Indica la modalità di download dell'aggiornamento.
- **È una patch**. Indica se l'aggiornamento è una patch.
- **Non installato**. Indica se l'aggiornamento ha lo stato Non installato.

Distribuzione dei pacchetti di installazione agli Administration Server secondari

Kaspersky Security Center consente di creare pacchetti di installazione per le applicazioni Kaspersky e per le applicazioni di terzi, nonché distribuire i pacchetti di installazione ai dispositivi client e installare le applicazioni dai pacchetti. Per ottimizzare il carico sull'Administration Server primario, è possibile distribuire i pacchetti di installazione agli Administration Server secondari. Successivamente, i server secondari trasmettono i pacchetti ai dispositivi client e quindi è possibile eseguire l'installazione remota delle applicazioni nei dispositivi client.

Per distribuire i pacchetti di installazione agli Administration Server secondari:

1. Assicurarsi che tutti gli Administration Server secondari siano connessi all'Administration Server primario.
2. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

   Verrà visualizzato l'elenco delle attività.
3. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
4. Nella pagina **Impostazioni nuova attività**, nell'elenco a discesa **Applicazione**, selezionare **Kaspersky Security Center**. Quindi, nell'elenco a discesa **Tipo di attività**, selezionare **Distribuisci pacchetto di installazione** e specificare il nome dell'attività.
5. Nella pagina **Ambito dell'attività**, selezionare i dispositivi a cui è assegnata l'attività in uno dei seguenti modi:
   - Se si desidera creare un'attività per tutti gli Administration Server secondari in un gruppo di amministrazione specifico, selezionare questo gruppo e quindi creare un'attività di gruppo per questo.
   - Se si desidera creare un'attività per Administration Server secondari specifici, selezionare questi server e quindi creare un'attività per questi.
6. Nella pagina **Pacchetti di installazione da distribuire**, selezionare i pacchetti di installazione da copiare negli Administration Server secondari.
7. Specificare un account per eseguire l'attività *Distribuisci pacchetto di installazione* in questo account. È possibile utilizzare il proprio account e mantenere abilitata l'opzione **Account predefinito**. In alternativa, è possibile specificare che l'attività deve essere eseguita con un altro account che disponga dei diritti di accesso necessari. A tale scopo, selezionare l'opzione **Specifica account**, quindi immettere le credenziali di tale account.

8. Nella pagina **Completare la creazione dell'attività**, è possibile abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** per aprire la finestra delle proprietà dell'attività, quindi modificare le impostazioni predefinite dell'attività. In caso contrario, è possibile configurare le impostazioni dell'attività in un secondo momento, quando desiderato.

9. Fare clic sul pulsante **Fine**.

   L'attività creata per la distribuzione dei pacchetti di installazione agli Administration Server secondari viene visualizzata nell'elenco delle attività.

10. È possibile eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

    Al termine dell'attività, i pacchetti di installazione selezionati vengono copiati negli Administration Server secondari specificati.

Installazione delle applicazioni tramite un'attività di installazione remota

Kaspersky Security Center consente di installare le applicazioni nei dispositivi in remoto, utilizzando le attività di installazione remota. Tali attività vengono create e assegnate ai dispositivi attraverso un'apposita procedura guidata. Per assegnare un'attività più in modo facile e rapido, è possibile specificare i dispositivi (fino a 1000 dispositivi) nella finestra della procedura guidata in uno dei seguenti modi:

- **Seleziona i dispositivi della rete rilevati da Administration Server**. In questo caso l'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

- **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**. È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

- **Assegna un'attività a una selezione dispositivi**. In questo caso l'attività viene assegnata ai dispositivi inclusi in una selezione creata precedentemente. È possibile specificare la selezione predefinita o una selezione personalizzata creata.

- **Assegna un'attività a un gruppo di amministrazione**. In questo caso l'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione creato precedentemente.

Per evitare problemi che possono verificarsi durante l'installazione dell'applicazione in un dispositivo client senza Network Agent installato, è necessario procedere come descritto nella distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center.

Installazione remota di un'applicazione

Questa sezione contiene informazioni su come installare un'applicazione in remoto in un gruppo di amministrazione, in dispositivi con indirizzi IP specifici o in una selezione di dispositivi gestiti.

Per installare un'applicazione in dispositivi specifici:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nel campo **Tipo di attività**, selezionare **Installa l'applicazione in remoto**.
4. Selezionare una delle seguenti opzioni:

   - **Assegna attività a un gruppo di amministrazione**

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

     Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

   - **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**

     È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

   - **Assegna attività a una selezione dispositivi**

     L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

   Viene creata l'attività *Installa l'applicazione in remoto* per i dispositivi specificati. Se è stata selezionata l'opzione **Assegna attività a un gruppo di amministrazione**, si tratta di un'attività di gruppo.
5. Nel passaggio **Ambito dell'attività**, specificare un gruppo di amministrazione, dispositivi con indirizzi IP specifici o una selezione di dispositivi.

   Le impostazioni disponibili dipendono dall'opzione selezionata nel passaggio precedente.

6. Nel passaggio **Pacchetti di installazione**, specificare le seguenti impostazioni:

- Nel campo **Selezionare il pacchetto di installazione**, selezionare il pacchetto di installazione di un'applicazione da installare.
- Nel gruppo di impostazioni **Forza il download del pacchetto di installazione** specificare la modalità di distribuzione dei file necessari per l'installazione dell'applicazione ai dispositivi client:
  - **Utilizzando Network Agent**

    Se questa opzione è abilitata, i pacchetti di installazione vengono distribuiti ai dispositivi client da Network Agent installato nei dispositivi client.

    Se questa opzione è disabilitata, i pacchetti di installazione vengono distribuiti utilizzando gli strumenti del sistema operativo dei dispositivi client.

    È consigliabile abilitare questa opzione se l'attività è stata assegnata a dispositivi in cui sono installati Network Agent.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**

    Se questa opzione è abilitata, i pacchetti di installazione verranno trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo tramite i punti di distribuzione. È possibile selezionare questa opzione se è presente almeno un punto di distribuzione nella rete.

    Se l'opzione **Utilizzo di Network Agent** è abilitata, i file vengono inviati tramite gli strumenti del sistema operativo solo se gli strumenti di Network Agent non sono disponibili.

    Per impostazione predefinita, questa opzione è abilitata per le attività di installazione remota create in un Administration Server virtuale.

  - **Utilizzando le risorse del sistema operativo tramite Administration Server**

    Se questa opzione è selezionata, i file vengono trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo dei dispositivi client tramite l'Administration Server. È possibile abilitare questa opzione se Network Agent non è installato nel dispositivo client, ma il dispositivo client si trova nella stessa rete di Administration Server.

    Per impostazione predefinita, questa opzione è abilitata.

- Nel campo **Numero massimo di download simultanei**, specificare il numero massimo consentito di dispositivi client a cui Administration Server può trasmettere simultaneamente i file.
- Nel campo **Numero massimo di tentativi di installazione**, specificare il numero massimo consentito di esecuzioni del programma di installazione.

  Se il numero di tentativi specificato nel parametro viene superato, Kaspersky Security Center non avvia più il programma di installazione nel dispositivo. Per riavviare l'attività *Installa l'applicazione in remoto*, aumentare il valore del parametro **Numero massimo di tentativi di installazione** e avviare l'attività. In alternativa, è possibile creare una nuova attività *Installa l'applicazione in remoto*.
- Se si esegue la migrazione da un'applicazione Kaspersky a un'altra e l'applicazione corrente è protetta da password, immettere la password nel campo **Password per disinstallare l'applicazione Kaspersky corrente**. Tenere presente che durante la migrazione l'applicazione Kaspersky corrente verrà disinstallata.

Il campo **Password per disinstallare l'applicazione Kaspersky corrente** è disponibile solo se è stata selezionata l'opzione **Utilizzando Network Agent** nel gruppo di impostazioni **Forza il download del pacchetto di installazione**.

È possibile utilizzare la password di disinstallazione solo per lo scenario di migrazione da Kaspersky Security for Windows Server a Kaspersky Endpoint Security for Windows durante l'installazione di Kaspersky Endpoint Security for Windows utilizzando l'attività *Installa l'applicazione in remoto*. L'utilizzo della password di disinstallazione durante l'installazione di altri componenti può causare errori di installazione.

Per completare correttamente lo scenario di migrazione, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Si sta utilizzando Kaspersky Security Center Network Agent 14.2 for Windows o versioni successive.
- Si sta installando l'applicazione nei dispositivi in cui viene eseguito Windows.

- Definire l'impostazione aggiuntiva:
  - **Non reinstallare l'applicazione se è già installata**

    Se questa opzione è abilitata, l'applicazione selezionata non verrà reinstallata se è già stata installata nel dispositivo client.

    Se questa opzione è disabilitata, l'applicazione verrà installata in ogni caso.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Verifica il tipo di sistema operativo prima del download**

    Prima di trasmettere i file ai dispositivi client, Kaspersky Security Center verifica se le impostazioni dell'utilità di installazione sono applicabili al sistema operativo del dispositivo client. Se le impostazioni non sono applicabili, Kaspersky Security Center non trasmette i file e non tenta di installare l'applicazione. Ad esempio, per installare un'applicazione nei dispositivi di un gruppo di amministrazione che include dispositivi che eseguono vari sistemi operativi, è possibile assegnare l'attività di installazione al gruppo di amministrazione e quindi abilitare questa opzione per ignorare i dispositivi che eseguono un sistema operativo diverso da quello desiderato.

  - **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory**

    Se questa opzione è abilitata, un pacchetto di installazione viene installato utilizzando i criteri di gruppo di Active Directory.

    Questa opzione è disponibile se il pacchetto di installazione di Network Agent è selezionato.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Chiedi agli utenti di chiudere le applicazioni in esecuzione**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

- Selezionare in quali dispositivi installare l'applicazione:
  - **Installa in tutti i dispositivi**

    L'applicazione verrà installata anche nei dispositivi gestiti da altri Administration Server.

    Questa opzione è selezionata per impostazione predefinita. Non è necessario modificare l'impostazione se si dispone di un solo Administration Server nella rete.

  - **Installa solo nei dispositivi gestiti tramite questo Administration Server**

    L'applicazione verrà installata solo nei dispositivi gestiti da questo Administration Server. Selezionare questa opzione se si dispone di più Administration Server nella rete per evitare conflitti tra di essi.

- Specificare se i dispositivi devono essere spostati in un gruppo di amministrazione dopo l'installazione:
  - **Non spostare i dispositivi**

    I dispositivi rimangono nei gruppi in cui si trovano attualmente. I dispositivi che non sono stati inseriti in alcun gruppo rimangono non assegnati.

  - **Sposta i dispositivi non assegnati nel gruppo selezionato (è possibile selezionare un solo gruppo)**

    I dispositivi vengono spostati nel gruppo di amministrazione selezionato.

Nota: l'opzione **Non spostare i dispositivi** è selezionata per impostazione predefinita. Per motivi di sicurezza, è consigliabile spostare i dispositivi manualmente.

7. In questo passaggio della procedura guidata, specificare se i dispositivi devono essere riavviati durante l'installazione delle applicazioni:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

8. Se necessario, nel passaggio **Selezionare gli account per l'accesso ai dispositivi** è possibile aggiungere gli account che verranno utilizzati per avviare l'attività *Installa l'applicazione in remoto*:

- Nessun account richiesto (Network Agent installato)

  Se questa opzione è selezionata, non è necessario specificare un account con cui verrà eseguito il programma di installazione dell'applicazione. L'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

  Se Network Agent non è stato installato nei dispositivi client, questa opzione non è disponibile.

- Account richiesto (Network Agent non utilizzato)

  Selezionare questa opzione se Network Agent non è installato nei dispositivi a cui si assegna l'attività di installazione remota. In questo caso, è possibile specificare un account utente o un certificato SSH per installare l'applicazione.

  - **Account locale**. Se questa opzione è selezionata, specificare l'account utente con cui verrà eseguito il programma di installazione dell'applicazione. Fare clic sul pulsante **Aggiungi**, selezionare **Account locale** e quindi specificare le credenziali dell'account utente.

    È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi per cui si assegna l'attività. In questo caso, tutti gli account aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

  - **Certificato SSH**. Se si desidera installare un'applicazione in un dispositivo client basato su Linux, è possibile specificare un certificato SSH anziché un account utente. Fare clic sul pulsante **Aggiungi**, selezionare **Certificato SSH**, quindi specificare la chiave privata e quella pubblica del certificato.

    Per generare una chiave privata, è possibile utilizzare l'utilità ssh-keygen. Si noti che Kaspersky Security Center supporta il formato PEM delle chiavi private, ma l'utilità ssh-keygen genera chiavi SSH nel formato OPENSSH per impostazione predefinita. Il formato OPENSSH non è supportato da Kaspersky Security Center. Per creare una chiave privata nel formato PEM supportato, aggiungere l'opzione -m PEM nel comando ssh-keygen. Ad esempio:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail dell'utente>"
    ```

9. Nel passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

   Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata la finestra delle impostazioni dell'attività. In questa finestra, è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio delle attività, se necessario.

10. Nell'elenco delle attività, selezionare l'attività creata, quindi fare clic su **Avvia**.

    In alternativa, attendere l'avvio dell'attività in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di installazione remota, l'applicazione selezionata viene installata nei dispositivi specificati.

Installazione di un'applicazione utilizzando i criteri di gruppo di Active Directory

Kaspersky Security Center consente di installare le applicazioni Kaspersky nei dispositivi gestiti utilizzando i criteri di gruppo di Active Directory.

> È possibile installare le applicazioni tramite i criteri di gruppo di Active Directory solo da pacchetti di installazione che includono Network Agent.

Per installare un'applicazione utilizzando i criteri di gruppo di Active Directory:

1. Eseguire la Distribuzione guidata della protezione. Seguire le istruzioni della procedura guidata.

2. Nella pagina **Impostazioni dell'attività di installazione remota** della Distribuzione guidata della protezione, abilitare l'opzione **Assegna l'installazione del pacchetto in Criteri di gruppo di Active Directory**.

3. Nella pagina **Selezionare gli account per l'accesso ai dispositivi**, selezionare l'opzione **Account richiesto (Network Agent non utilizzato)**.

4. Aggiungere l'account con privilegi di amministratore nel dispositivo in cui è installato Kaspersky Security Center o l'account incluso nel gruppo di dominio Proprietari autori criteri di gruppo.

5. Concedere le autorizzazioni all'account selezionato:

    a. Accedere a **Pannello di controllo** → **Strumenti di amministrazione** e aprire **Gestione Criteri di gruppo**.

    b. Fare clic sul nodo con il dominio desiderato.

    c. Fare clic sulla sezione **Delega**.

    d. Nell'elenco a discesa **Autorizzazione** selezionare **Collega oggetti Criteri di gruppo**.

    e. Fare clic su **Aggiungi**.

    f. Nella finestra **Seleziona utente, computer o gruppo** visualizzata selezionare l'account necessario.

    g. Fare clic su **OK** per chiudere la finestra **Seleziona utente, computer o gruppo**.

    h. Nell'elenco **Gruppi e utenti** selezionare l'account appena aggiunto, quindi fare clic su **Avanzate** → **Avanzate**.

    i. Nell'elenco **Autorizzazioni** fare doppio clic sull'account appena aggiunto.

    j. Concedere le seguenti autorizzazioni:

    - **Creare oggetti Criteri di gruppo**
    - **Eliminare oggetti Criteri di gruppo**
    - **Creare oggetti del contenitore Criteri di gruppo**
    - **Eliminare oggetti dal contenitore Criteri di gruppo**

    k. Fare clic su **OK** per salvare le modifiche.

6. Definire altre impostazioni seguendo le istruzioni della procedura guidata.

7. Eseguire l'attività di installazione remota creata manualmente o attenderne l'avvio pianificato.

Verrà avviata la seguente sequenza di installazione remota:

1. Durante l'esecuzione dell'attività, verranno creati i seguenti oggetti nel dominio che include i dispositivi client per il set specificato:

    - Oggetto Criteri di gruppo denominato **Kaspersky_AK{GUID}**.
    - Un gruppo di protezione che corrisponde all'oggetto Criteri di gruppo. Questo gruppo di protezione include i dispositivi client coperti dall'attività. Il contenuto del gruppo di protezione definisce l'ambito dell'oggetto Criteri di gruppo.

2. Kaspersky Security Center installa le applicazioni Kaspersky selezionate nei dispositivi client direttamente da KLSHARE, ovvero la cartella di rete condivisa dell'applicazione. Nella cartella di installazione di Kaspersky Security Center verrà creata una sottocartella ausiliaria che contiene il file .msi per l'applicazione da installare.

3. Quando si aggiungono nuovi dispositivi all'ambito dell'attività, questi vengono aggiunti al gruppo di protezione al successivo avvio dell'attività. Se nella pianificazione dell'attività è selezionata l'opzione **Esegui attività non effettuate**, i dispositivi vengono aggiunti al gruppo di protezione immediatamente.

4. Quando si eliminano dispositivi dall'ambito dell'attività, questi vengono eliminati dal gruppo di protezione al successivo avvio dell'attività.

5. Quando si elimina un'attività da Active Directory, vengono eliminati anche l'oggetto Criteri di gruppo, il collegamento all'oggetto Criteri di gruppo e il gruppo di protezione corrispondente.

Se si desidera applicare un altro schema di installazione tramite Active Directory, è possibile configurare manualmente le impostazioni richieste. Questa operazione può essere ad esempio necessaria nei seguenti casi:

- Quando l'amministratore della protezione anti-virus non dispone dei diritti necessari per apportare modifiche ad Active Directory per determinati domini
- Quando il pacchetto di installazione originale deve essere archiviato in una risorsa di rete distinta
- Quando è necessario collegare un oggetto Criteri di gruppo a specifiche unità Active Directory

Sono disponibili le seguenti opzioni per l'utilizzo di uno schema di installazione alternativo tramite Active Directory:

- Se è necessario eseguire l'installazione direttamente dalla cartella condivisa di Kaspersky Security Center, nelle proprietà dell'oggetto Criteri di gruppo specificare il file .msi presente nella sottocartella exec della cartella del pacchetto di installazione per l'applicazione desiderata.
- Se il pacchetto di installazione deve essere posizionato in un'altra risorsa di rete, copiare in tale risorsa l'intero contenuto della cartella exec, perché questa contiene, oltre al file con estensione .msi, i file di configurazione generati al momento della creazione del pacchetto. Per installare la chiave di licenza insieme all'applicazione, copiare anche il file chiave in questa cartella.

Installazione di applicazioni negli Administration Server secondari

Per installare un'applicazione negli Administration Server secondari:

1. Stabilire una connessione all'Administration Server che controlla gli Administration Server secondari desiderati.

2. Verificare che il pacchetto di installazione corrispondente all'applicazione da installare sia disponibile in ognuno degli Administration Server secondari selezionati. Se non è possibile trovare il pacchetto di installazione in nessuno dei server secondari, è necessario distribuirlo. A tale scopo, creare un'attività con il tipo di attività **Distribuisci pacchetto di installazione**.

3. Creare un'attività per l'installazione remota di un'applicazione negli Administration Server secondari. Selezionare il tipo di attività **Installa l'applicazione nell'Administration Server secondario in remoto**.

   La Creazione guidata nuova attività crea un'attività per l'installazione remota dell'applicazione selezionata nella procedura guidata in determinati Administration Server secondari.

4. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di installazione remota, l'applicazione selezionata viene installata negli Administration Server secondari.

Definizione delle impostazioni per l'installazione remota nei dispositivi Unix

Quando si installa un'applicazione in un dispositivo Unix utilizzando un'attività di installazione remota, è possibile specificare le impostazioni specifiche per Unix per l'attività. Queste impostazioni sono disponibili nelle proprietà dell'attività dopo la creazione dell'attività.

Per specificare le impostazioni specifiche per Unix per un'attività di installazione remota:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul nome dell'attività di installazione remota per la quale si desidera specificare le impostazioni specifiche per Unix.

   Verrà visualizzata la finestra delle proprietà dell'attività.
3. Accedere a **Impostazioni applicazione** → **Impostazioni specifiche per Unix**.
4. Specificare le seguenti impostazioni:

   - **Imposta una password per l'account radice (solo per la distribuzione tramite SSH)**

     Se il comando `sudo` non può essere utilizzato nel dispositivo di destinazione senza specificare la password, selezionare questa opzione, quindi specificare la password per l'account radice. Kaspersky Security Center trasmette la password in formato criptato al dispositivo di destinazione, decripta la password e avvia la procedura di installazione per conto dell'account radice con la password specificata.

     Kaspersky Security Center non utilizza l'account o la password specificata per creare una connessione SSH.

   - **Specifica il percorso di una cartella temporanea con autorizzazioni Esecuzione nel dispositivo di destinazione (solo per la distribuzione tramite SSH)**

     Se la directory /tmp nel dispositivo di destinazione non dispone dell'autorizzazione di esecuzione, selezionare questa opzione e specificare il percorso della directory con l'autorizzazione di esecuzione. Kaspersky Security Center utilizza la directory specificata come directory temporanea per accedere tramite SSH. L'applicazione inserisce il pacchetto di installazione nella directory ed esegue la procedura di installazione.
5. Fare clic sul pulsante **Salva**.

Le impostazioni dell'attività specificata vengono salvate.

Avvio e arresto delle applicazioni Kaspersky.

È possibile utilizzare l'attività *Avvia o arresta l'applicazione* per avviare e arrestare le applicazioni Kaspersky nei dispositivi gestiti.

Per creare l'attività Avvia o arresta l'applicazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nell'elenco a discesa **Applicazione**, selezionare l'applicazione per la quale si desidera creare l'attività.

   Le applicazioni Kaspersky vengono visualizzate nell'elenco se in precedenza sono stati aggiunti plug-in Web di gestione per tali applicazioni.
4. Nell'elenco **Tipo di attività**, selezionare l'attività **Attivazione dell'applicazione**.
5. Nel campo **Nome attività**, specificare il nome della nuova attività.

   Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
6. Selezionare i dispositivi a cui verrà assegnata l'attività.
7. Nella finestra **Applicazioni**, procedere come segue:
   - Selezionare le caselle di controllo accanto ai nomi delle applicazioni per cui si desidera creare l'attività.
   - Selezionare l'opzione **Avvia applicazione** o **Arresta applicazione**.
8. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nel passaggio **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
9. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
10. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.
11. Nella finestra delle proprietà dell'attività, specificare le impostazioni generali dell'attività in base alle proprie esigenze, quindi salvare le impostazioni.

L'attività verrà creata e configurata.

Se si desidera eseguire l'attività, selezionarla nell'elenco delle attività, quindi fare clic sul pulsante **Avvia**.

Mobile Device Management

La gestione della protezione per i dispositivi mobili tramite Kaspersky Security Center viene eseguita utilizzando la funzionalità Mobile Device Management, che richiede una licenza dedicata. Per gestire i dispositivi mobili appartenenti ai dipendenti dell'organizzazione, abilitare e configurare Mobile Device Management.

Mobile Device Management consente di gestire i dispositivi Android dei dipendenti. La protezione è garantita dall'app mobile Kaspersky Endpoint Security for Android installata nei dispositivi. Questa app mobile garantisce la protezione dei dispositivi mobili da minacce Web, virus e altri programmi che costituiscono una minaccia. Per la gestione centralizzata tramite Kaspersky Security Center Web Console, è necessario installare i seguenti plug-in di gestione Web nel dispositivo in cui è installato Kaspersky Security Center Web Console:

- Plug-in di Kaspersky Security for Mobile
- Plug-in di Kaspersky Endpoint Security for Android

Per informazioni sulla gestione e sulla distribuzione della protezione dei dispositivi mobili, vedere la Guida di Kaspersky Security for Mobile.

Modifica delle impostazioni di Mobile Device Management in Kaspersky Security Center Web Console

Per modificare le impostazioni per Mobile Device Management:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Porte aggiuntive**.

3. Modificare le impostazioni appropriate:

   - **Apri porta per i dispositivi mobili**

     Se questo interruttore è abilitato, verrà aperta la porta per i dispositivi mobili in Administration Server.

     È possibile utilizzare la porta per i dispositivi mobili solo se il componente Mobile Device Management è installato.

     Se questo interruttore è disabilitato, la porta per i dispositivi mobili in Administration Server non verrà utilizzata.

     Per impostazione predefinita, questo interruttore è disabilitato.

   - **Porta per la sincronizzazione del dispositivo mobile**

     Numero della porta utilizzata per la connessione dei dispositivi mobili all'Administration Server. Il numero di porta predefinito è 13292.

     Viene utilizzato il sistema decimale per i record.

   - **Porta per l'attivazione del dispositivo mobile**

     Porta per la connessione di Kaspersky Endpoint Security for Android ai server di attivazione di Kaspersky.

     Il numero di porta predefinito è 17100.

4. Fare clic sul pulsante **Salva**.

I dispositivi mobili ora possono connettersi all'Administration Server.

Sostituzione di applicazioni di protezione di terzi

L'Installazione delle applicazioni di protezione Kaspersky tramite Kaspersky Security Center può richiedere la rimozione di software di terze parti incompatibile con l'applicazione da installare. Kaspersky Security Center offre diversi modi di rimuovere le applicazioni di terze parti.

Rimozione delle applicazioni incompatibili utilizzando il programma di installazione

Questa opzione è disponibile solo in Administration Console basata su Microsoft Management Console.

Il metodo del programma di installazione per la rimozione delle applicazioni incompatibili è supportato da vari tipi di installazione. Prima dell'installazione dell'applicazione di protezione, tutte le applicazioni incompatibili vengono rimosse automaticamente se nella finestra delle proprietà del pacchetto di installazione dell'applicazione di protezione (sezione **Applicazioni incompatibili**) è selezionata l'opzione **Disinstalla automaticamente le applicazioni incompatibili**.

Rimozione delle applicazioni incompatibili durante la configurazione dell'installazione remota di un'applicazione

È possibile abilitare l'opzione **Disinstalla automaticamente le applicazioni incompatibili** quando si configura l'installazione remota di un'applicazione di protezione. In Administration Console basata su Microsoft Management Console, questa opzione è disponibile nell'Installazione remota guidata. In Kaspersky Security Center Web Console, questa opzione è disponibile nella Distribuzione guidata della protezione. Quando questa opzione è abilitata, Kaspersky Security Center consente di rimuovere le applicazioni incompatibili prima di installare un'applicazione di protezione in un dispositivo gestito.

Istruzioni dettagliate:

- Administration Console: Rimozione delle applicazioni incompatibili tramite l'Installazione remota guidata
- Kaspersky Security Center Web Console: Rimozione delle applicazioni incompatibili prima dell'installazione

Rimozione delle applicazioni incompatibili tramite un'attività dedicata

Per rimuovere le applicazioni incompatibili, utilizzare l'attività **Disinstalla l'applicazione in remoto**. Questa attività deve essere eseguita nei dispositivi prima dell'attività di installazione dell'applicazione di protezione. Ad esempio, nell'attività di installazione è possibile selezionare il tipo di pianificazione **Al completamento di un'altra attività**, dove l'altra attività è **Disinstalla l'applicazione in remoto**.

Questo metodo di disinstallazione è consigliabile quando il programma di installazione dell'applicazione di protezione non è in grado di rimuovere correttamente un'applicazione incompatibile.

Istruzioni dettagliate per Administration Console: creazione di un'attività.

Individuazione dei dispositivi nella rete

Questa sezione descrive la ricerca e l'individuazione dei dispositivi nella rete.

Kaspersky Security Center consente di individuare i dispositivi sulla base dei criteri specificati. È possibile salvare i risultati della ricerca in un file di testo.

La funzionalità di ricerca e individuazione consente di trovare i seguenti dispositivi:

- I dispositivi gestiti nei gruppi di amministrazione di Kaspersky Security Center Administration Server e nei relativi Administration Server secondari.
- I dispositivi non assegnati gestiti da Kaspersky Security Center Administration Server e dai relativi Administration Server secondari.

Scenario: Individuazione dei dispositivi nella rete

È necessario eseguire la device discovery prima dell'installazione delle applicazioni di protezione. Administration Server riceve informazioni sui dispositivi rilevati e consente di gestire i dispositivi tramite criteri. Sono necessari polling periodici della rete per aggiornare l'elenco dei dispositivi disponibili nella rete.

Prima di avviare il polling di rete, verificare che il protocollo SMB sia abilitato. In caso contrario, Kaspersky Security Center non può rilevare i dispositivi nella rete sottoposta a polling. Per abilitare il protocollo SMB, seguire le istruzioni per il proprio sistema operativo.

Il rilevamento dei dispositivi in rete comprende i seguenti fasi:

1. **Individuazione dei dispositivi**

   L'Avvio rapido guidato fornisce supporto tramite la device discovery e aiuta a individuare i dispositivi della rete quali computer, tablet e cellulari. È inoltre possibile eseguire manualmente la device discovery.

2. **Configurazione dei polling pianificati**

   Decidere quali tipi di polling si desidera utilizzare periodicamente. Abilitare i tipi desiderati e configurare la pianificazione dei polling. È possibile fare riferimento ai suggerimenti per la frequenza dei polling della rete.

3. **Configurazione delle regole per l'aggiunta dei dispositivi individuati nei gruppi di amministrazione (facoltativa)**

   Se vengono visualizzati nuovi dispositivi nella rete, questi vengono individuati durante il polling periodico e vengono automaticamente inclusi nel gruppo **Dispositivi non assegnati**. È possibile impostare regole di spostamento dei dispositivi per automatizzare l'allocazione dei dispositivi al gruppo **Dispositivi gestiti**. È inoltre possibile configurare le regole di conservazione.

   Se si ignora il passaggio 3, i nuovi dispositivi rilevati vengono assegnati al gruppo **Dispositivi non assegnati**. Se si desidera, è possibile spostare questi dispositivi nel gruppo **Dispositivi gestiti** manualmente. Se si spostano manualmente i dispositivi nel gruppo **Dispositivi gestiti**, è possibile analizzare le informazioni su ciascun dispositivo, decidere se spostarlo in un gruppo di amministrazione e, in tal caso, in quale gruppo.

Risultati

Il completamento dello scenario dà i seguenti risultati:

- Kaspersky Security Center Administration Server rileva i dispositivi nella rete e fornisce informazioni in merito.
- Le operazioni di polling future vengono impostate ed eseguite in base alla pianificazione specificata.
- I nuovi dispositivi individuati vengono organizzati in base alle regole configurate. (In alternativa, se non è configurata alcuna regola, i dispositivi rimangono nel gruppo **Dispositivi non assegnati**).

Device discovery

In questa sezione vengono descritti i tipi di device discovery disponibili in Kaspersky Security Center e vengono fornite informazioni sull'utilizzo di ogni tipo.

L'Administration Server riceve le informazioni sulla struttura della rete e sui dispositivi al suo interno tramite il polling periodico. Le informazioni vengono registrate nel database di Administration Server. Administration Server può utilizzare i seguenti tipi di polling:

- **Polling della rete Windows**. L'Administration Server può eseguire due tipi di polling della rete Windows: rapido e completo. Durante un polling rapido Administration Server recupera informazioni solo dall'elenco dei nomi di dispositivi NetBIOS in tutti i domini di rete e i gruppi di lavoro. Durante un polling completo vengono richieste più informazioni da ogni dispositivo client: nome del sistema operativo, indirizzo IP, nome DNS e nome NetBIOS. Per impostazione predefinita sono abilitati sia il polling rapido che quello completo. Il polling della rete Windows può non essere in grado di individuare i dispositivi, ad esempio se le porte UDP 137, UDP 138, TCP 139 sono chiuse nel router o dal firewall.
- **Polling del controller di dominio**. Administration Server o un punto di distribuzione recupera le informazioni sulla struttura del dominio e sui nomi DNS dei dispositivi inclusi nel dominio. Per impostazione predefinita, questo tipo di polling è abilitato. È consigliabile utilizzare il polling del controller di dominio se tutti i dispositivi in rete sono membri di un dominio. Se alcuni dei dispositivi in rete non sono inclusi nel dominio, questi dispositivi non possono essere rilevati dal polling del controller di dominio.
- **Polling intervallo IP**. Administration Server esegue il polling dell'intervallo IP specificati utilizzando pacchetti ICMP o il protocollo NBNS e compila un set completo di dati sui dispositivi all'interno degli intervalli IP. Per impostazione predefinita, questo tipo di polling è disabilitato. Non è consigliabile utilizzare questo tipo di polling se si utilizza il polling di rete Windows e/o il polling di Active Directory.
- **Polling Zeroconf**. Un punto di distribuzione che esegue il polling della rete IPv6 utilizzando le reti zero-configuration (definite anche *Zeroconf*). Per impostazione predefinita, questo tipo di polling è disabilitato. È possibile utilizzare il polling Zeroconf se il punto di distribuzione esegue Linux.

Se sono installate e attivate le regole di spostamento dei dispositivi, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi gestiti**. Se non sono state abilitate regole di spostamento, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi non assegnati**.

È possibile modificare le impostazioni di device discovery per ciascun tipo. È ad esempio possibile modificare la pianificazione del polling o impostare l'esecuzione del polling dell'intera foresta di domini o solo di un dominio specifico.

Prima di avviare il polling di rete, verificare che il protocollo SMB sia abilitato. In caso contrario, Kaspersky Security Center non può rilevare i dispositivi nella rete sottoposta a polling. Per abilitare il protocollo SMB, seguire le istruzioni per il proprio sistema operativo.

Polling della rete Windows

Informazioni sul polling della rete Windows

Durante un polling rapido Administration Server recupera informazioni solo dall'elenco dei nomi di dispositivi NetBIOS in tutti i domini di rete e i gruppi di lavoro. Durante un polling completo sono richieste le seguenti informazioni da ogni dispositivo client:

- Nome del sistema operativo
- Indirizzo IP
- Nome DNS
- Nome NetBIOS

Sia il polling rapido che quello completo richiedono le seguenti operazioni:

- Le porte UDP 137/138, TCP 139, UDP 445, TCP 445 devono essere disponibili nella rete.
- Il protocollo SMB è abilitato.
- È necessario utilizzare il servizio Microsoft Computer Browser e il computer del browser primario deve essere abilitato in Administration Server.
- È necessario utilizzare il servizio Microsoft Computer Browser e il computer del browser primario deve essere abilitato nei dispositivi client:
  - In almeno un dispositivo, se il numero di dispositivi della rete non è superiore a 32.
  - In almeno un dispositivo ogni 32 dispositivi della rete.

Il polling completo può essere eseguito solo se il polling rapido è stato eseguito almeno una volta.

Visualizzazione e modifica delle impostazioni per il polling della rete Windows

Per modificare le proprietà del polling della rete Windows:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Domini Windows**.
2. Fare clic sul pulsante **Proprietà**.
   Verrà visualizzata la finestra delle proprietà del dominio Windows.

3. Abilitare o disabilitare il polling della rete Windows utilizzando l'interruttore **Abilita il polling della rete Windows**.

4. Configurare la pianificazione del polling. Per impostazione predefinita, il polling rapido viene eseguito ogni 15 minuti e il polling completo viene eseguito ogni 60 minuti.

   Opzioni per la pianificazione di polling:

   - **Ogni N giorni**

     Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

     Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

   - **Ogni N minuti**

     Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

   - **In base ai giorni della settimana**

     Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

   - **Ogni mese nei giorni specificati delle settimane selezionate**

     Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

   - **Esegui attività non effettuate**

     Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

     Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

     Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

     Per impostazione predefinita, questa opzione è disabilitata.

5. Salvare le proprietà del polling della rete Windows

Le proprietà verranno salvate e applicate a tutti i domini e i gruppi di lavoro di Windows rilevati.

Esecuzione manuale del polling

Per eseguire immediatamente il polling:

Fare clic su **Avvia polling rapido** o **Avvia polling completo**.

Al termine del polling, è possibile visualizzare l'elenco dei dispositivi rilevati nella pagina **Domini Windows** selezionando la casella di controllo accanto a un nome di dominio, quindi facendo clic sul pulsante **Dispositivi**.

Polling intervallo IP

Inizialmente, Kaspersky Security Center ottiene gli intervalli IP per il polling dalle impostazioni di rete del dispositivo in cui è installato. Se l'indirizzo del dispositivo è 192.168.0.1 e la subnet mask è 255.255.255.0, Kaspersky Security Center include automaticamente la rete 192.168.0.0/24 nell'elenco degli indirizzi di polling. Kaspersky Security Center esegue il polling di tutti gli indirizzi da 192.168.0.1 a 192.168.0.254.

Per tutti gli host basati su Linux all'interno di un controller di dominio Microsoft Active Directory o Samba, specificare il `netbios name` e i parametri del `workgroup` nel file `/etc/samba/smb.conf`. In caso contrario, i risultati del polling potrebbero contenere contenitori host duplicati.

Kaspersky Security Center può eseguire il polling dell'intervallo IP tramite la ricerca DNS inversa o utilizzando il protocollo NBNS:

- **Ricerca DNS inversa**

  Kaspersky Security Center tenta di eseguire la risoluzione inversa dei nomi per ogni indirizzo IP nell'intervallo specificato a un nome DNS utilizzando richieste DNS standard. Se questa operazione riesce, il server invia un messaggio `ICMP ECHO REQUEST` (equivalente al comando ping) al nome ricevuto. Se il dispositivo risponde, le informazioni su di esso vengono aggiunte al database di Kaspersky Security Center. La risoluzione inversa dei nomi è necessaria per escludere i dispositivi di rete che possono avere un indirizzo IP ma che non sono computer, ad esempio stampanti o router di rete.

  Questo metodo di polling si basa su un servizio DNS locale configurato correttamente. Deve essere presente una zona di ricerca inversa. Nelle reti in cui è utilizzato Active Directory tale zona viene mantenuta automaticamente. In queste reti, tuttavia, il polling della subnet IP non fornisce più informazioni del polling di Active Directory. Inoltre, gli amministratori delle reti di piccole dimensioni spesso non configurano la zona di ricerca inversa perché non è necessaria per il lavoro di molti servizi di rete. Per tali motivi, il polling della subnet IP è disabilitato per impostazione predefinita.

- **Protocollo NBNS**

  Se la risoluzione dei nomi inversa non è possibile nella rete per qualche motivo, Kaspersky Security Center utilizza il protocollo NBNS per eseguire il polling dell'intervallo IP. Se una richiesta a un indirizzo IP restituisce un nome NetBIOS, le informazioni su questo dispositivo vengono aggiunte al database di Kaspersky Security Center.

Prima di avviare il polling di rete, verificare che il protocollo SMB sia abilitato. In caso contrario, Kaspersky Security Center non può rilevare i dispositivi nella rete sottoposta a polling. Per abilitare il protocollo SMB, seguire le istruzioni per il proprio sistema operativo.

Visualizzazione e modifica delle impostazioni per il polling degli intervalli IP

Per visualizzare e modificare le proprietà per il polling degli intervalli IP:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Intervalli IP**.
2. Fare clic sul pulsante **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del polling IP.
3. Abilitare o disabilitare il polling IP utilizzando l'interruttore **Consenti polling**.

4. Configurare la pianificazione del polling. Per impostazione predefinita, il polling IP viene eseguito ogni 420 minuti (sette ore).

   Quando si specifica l'intervallo di polling, verificare che questa impostazione non superi il valore del parametro di durata dell'indirizzo IP. Se un indirizzo IP non viene verificato tramite il polling durante la durata dell'indirizzo IP, tale indirizzo IP viene automaticamente rimosso dai risultati del polling. Per impostazione predefinita, la durata dei risultati del polling è di 24 ore, poiché gli indirizzi IP dinamici, ovvero assegnati tramite il protocollo DHCP (Dynamic Host Configuration Protocol), cambiano ogni 24 ore.

   Opzioni per la pianificazione di polling:

   - **Ogni N giorni**

     Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

     Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

   - **Ogni N minuti**

     Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

   - **In base ai giorni della settimana**

     Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

   - **Ogni mese nei giorni specificati delle settimane selezionate**

     Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

   - **Esegui attività non effettuate**

     Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

     Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

     Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

     Per impostazione predefinita, questa opzione è disabilitata.

5. Fare clic sul pulsante **Salva**.

Le proprietà verranno salvate e applicate a tutti gli intervalli IP.

Esecuzione manuale del polling

Per eseguire immediatamente il polling:

Fare clic su **Avvia polling**.

Aggiunta e modifica di un intervallo IP

Inizialmente, Kaspersky Security Center ottiene gli intervalli IP per il polling dalle impostazioni di rete del dispositivo in cui è installato. Se l'indirizzo del dispositivo è 192.168.0.1 e la subnet mask è 255.255.255.0, Kaspersky Security Center include automaticamente la rete 192.168.0.0/24 nell'elenco degli indirizzi di polling. Kaspersky Security Center esegue il polling di tutti gli indirizzi da 192.168.0.1 a 192.168.0.254. È possibile modificare gli intervalli IP definiti automaticamente o aggiungere intervalli IP personalizzati.

È possibile creare un intervallo solo per gli indirizzi IPv4. Se si abilita Polling Zeroconf, Kaspersky Security Center eseguirà il polling dell'intera rete.

Per aggiungere un nuovo intervallo IP:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Intervalli IP**.
2. Per aggiungere un nuovo intervallo IP, fare clic sul pulsante **Aggiungi**.
3. Nella finestra visualizzata specificare le seguenti impostazioni:
   - **Nome intervallo IP**

     Nome dell'intervallo IP. È possibile specificare l'intervallo IP stesso come nome, ad esempio "192.168.0.0/24".

   - **Intervallo IP o indirizzo subnet e subnet mask**

     Impostare l'intervallo IP specificando gli indirizzi IP iniziale e finale o l'indirizzo subnet e la subnet mask. È inoltre possibile selezionare uno degli intervalli IP già esistenti facendo clic sul pulsante **Sfoglia**.

   - **Durata dell'indirizzo IP (ore)**

     Quando si specifica questo parametro, assicurarsi che superi l'intervallo di polling impostato nella pianificazione del polling. Se un indirizzo IP non viene verificato tramite il polling durante la durata dell'indirizzo IP, tale indirizzo IP viene automaticamente rimosso dai risultati del polling. Per impostazione predefinita, la durata dei risultati del polling è di 24 ore, poiché gli indirizzi IP dinamici, ovvero assegnati tramite il protocollo DHCP (Dynamic Host Configuration Protocol), cambiano ogni 24 ore.
4. Selezionare **Abilita polling intervalli IP** se si desidera eseguire il polling della subnet o dell'intervallo aggiunto. In caso contrario, non verrà effettuato il polling della subnet o dell'intervallo aggiunto.
5. Fare clic sul pulsante **Salva**.

Il nuovo intervallo IP verrà aggiunto all'elenco degli intervalli IP.

È possibile eseguire il polling di ciascun intervallo IP separatamente utilizzando il pulsante **Avvia polling**. Al termine del polling, è possibile visualizzare l'elenco dei dispositivi rilevati utilizzando il pulsante **Dispositivi**. Per impostazione predefinita, la durata dei risultati del polling è di 24 ore ed è uguale all'impostazione per la durata dell'indirizzo IP.

Per aggiungere una subnet a un intervallo IP esistente:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Intervalli IP**.
2. Fare clic sul nome dell'intervallo IP a cui si desidera aggiungere una subnet.
3. Nella finestra visualizzata fare clic sul pulsante **Aggiungi**.
4. Specificare una subnet utilizzando il relativo indirizzo e la subnet mask oppure tramite il primo e l'ultimo indirizzo IP nell'intervallo IP. In alternativa, aggiungere una subnet esistente facendo clic sul pulsante **Sfoglia**.
5. Fare clic sul pulsante **Salva**.

   La nuova subnet verrà aggiunta all'intervallo IP.
6. Fare clic sul pulsante **Salva**.

Le nuove impostazioni dell'intervallo IP verranno salvate.

È possibile aggiungere tutte le subnet necessarie. Gli intervalli IP denominati non possono sovrapporsi, ma le subnet non denominate all'interno di un intervallo IP non presentano tali restrizioni. È possibile abilitare e disabilitare il polling in modo indipendente per ogni intervallo IP.

Polling zeroconf

Questo tipo di polling è supportato solo per i punti di distribuzione basati su Linux.

Un punto di distribuzione può eseguire il polling delle reti che hanno dispositivi con indirizzi IPv6. In questo caso, gli intervalli IP non vengono specificati e il punto di distribuzione esegue il polling dell'intera rete utilizzando le reti zero-configuration (definite anche *Zeroconf*). Per iniziare a utilizzare Zeroconf è necessario installare l'utilità avahi-browse nel punto di distribuzione.

Per abilitare il polling della rete IPv6:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Intervalli IP**.
2. Fare clic sul pulsante **Proprietà**.
3. Nella finestra visualizzata attivare l'interruttore **Usa Zeroconf per il polling delle reti IPv6**.

Successivamente, il punto di distribuzione inizia a eseguire il polling della rete. In questo caso gli intervalli IP specificati vengono ignorati.

Polling del controller di dominio

Kaspersky Security Center supporta il polling di un controller di dominio Microsoft Active Directory e di un controller di dominio Samba.

Kaspersky Security Center consente di eseguire il polling di un controller di dominio Samba solo utilizzando un punto di distribuzione Linux. Per un controller di dominio Samba, Samba 4 viene utilizzato come controller di dominio Active Directory.

Quando si esegue il polling di un controller di dominio, Administration Server o un punto di distribuzione recuperano le informazioni sulla struttura del dominio, sugli account utente, sui gruppi di protezione e sui nomi DNS dei dispositivi inclusi nel dominio.

È consigliabile utilizzare il polling del controller di dominio se tutti i dispositivi in rete sono membri di un dominio. Se alcuni dei dispositivi in rete non sono inclusi nel dominio, questi dispositivi non possono essere rilevati dal polling del controller di dominio.

Prerequisiti

Prima di eseguire il polling di un controller di dominio, assicurarsi di consentire le connessioni al controller di dominio tramite un firewall o un server proxy. Verificare inoltre che i seguenti protocolli siano abilitati nel controller di dominio:

- Lightweight Directory Access Protocol (LDAP)
- Simple Authentication and Security Layer (SASL)

  Questo protocollo viene utilizzato se la connessione al controller di dominio viene stabilita utilizzando l'autenticazione SASL. Administration Server e i punti di distribuzione supportano solo il meccanismo DIGEST-MD5.
- Lightweight Directory Access Protocol over Secure Sockets Layer (LDAPS)

  Questo protocollo viene utilizzato se è necessario connettersi al controller di dominio tramite una connessione criptata.

Verificare che le seguenti porte siano disponibili nel dispositivo del controller di dominio:

- 389 per il protocollo LDAP e Simple Authentication (incluso SASL)
- 636 per il protocollo LDAPS

Per tutti gli host basati su Linux all'interno di un controller di dominio Microsoft Active Directory o Samba, è necessario specificare i parametri `netbios name` e `workgroup` nel file `/etc/samba/smb.conf`. In caso contrario, i risultati del polling potrebbero contenere contenitori host duplicati.

Se un dominio Microsoft Active Directory contiene più controller di dominio, la selezione di un controller specifico durante il polling del dominio non è supportata. La connessione viene stabilita con il primo controller di dominio rilevato. Per garantire la corretta autenticazione con il dominio Microsoft Active Directory, il campo Subject Alternative Name (SAN) del certificato deve includere tutti gli indirizzi dei controller di dominio inclusi nel dominio, nonché il nome NetBIOS del dominio di Microsoft Active Directory.

Polling del controller di dominio tramite Administration Server

È possibile utilizzare Administration Server per eseguire il polling solo di un controller di dominio Microsoft Active Directory.

Per eseguire il polling di un controller di dominio utilizzando Administration Server:

1. Nel menu principale, passare a **Individuazione e distribuzione** → **Individuazione** → **Controller di dominio**.
2. Fare clic su **Impostazioni di polling**.

   Viene visualizzata la finestra **Impostazioni di polling del controller di dominio**.
3. Selezionare l'opzione **Abilita polling controller di dominio**.
4. Nella sezione **Impostazioni avanzate**, specificare l'ambito del polling:

   - **Esegui polling dominio corrente**

     Selezionare questa opzione per eseguire il polling di un dominio a cui appartiene Kaspersky Security Center.

   - **Esegui polling di tutta la foresta di dominio**

     Selezionare questa opzione per eseguire il polling di una foresta di domini a cui appartiene Kaspersky Security Center.

   - **Esegui polling di domini specifici**

     Selezionare questa opzione per eseguire il polling di un dominio con l'indirizzo e le credenziali utente specificati.

5. Se necessario, specificare la pianificazione del polling: Il periodo predefinito è un'ora. I dati ricevuti al successivo polling sostituiscono completamente i dati precedenti.

   Sono disponibili le opzioni di pianificazione di polling seguenti:

   - **Ogni N giorni**

     Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

     Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

   - **Ogni N minuti**

     Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

   - **In base ai giorni della settimana**

     Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

   - **Ogni mese nei giorni specificati delle settimane selezionate**

     Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

   - **Esegui attività non effettuate**

     Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

     Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

     Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

     Per impostazione predefinita, questa opzione è disabilitata.

   Se si modificano gli account utente in un gruppo di protezione del dominio, queste modifiche verranno visualizzate in Kaspersky Security Center un'ora dopo il polling del controller di dominio.

6. Fare clic su **Salva** per applicare le modifiche.

7. Se si desidera eseguire immediatamente il polling, fare clic sul pulsante **Avvia polling**.

Polling del controller di dominio utilizzando un punto di distribuzione

È inoltre possibile eseguire il polling di un controller di dominio Microsoft Active Directory e di un controller di dominio Samba utilizzando un punto di distribuzione. Un dispositivo gestito basato su Windows o Linux può fungere da punto di distribuzione.

Per un punto di distribuzione Linux, sono supportati il polling di un controller di dominio Microsoft Active Directory e di un controller di dominio Samba.
Per un punto di distribuzione Windows, è supportato solo il polling di un controller di dominio Microsoft Active Directory.
Il polling con un punto di distribuzione Mac non è supportato.

Per configurare il polling del controller di dominio utilizzando il punto di distribuzione:

1. Aprire le proprietà del punto di distribuzione.
2. Selezionare la sezione **Polling del controller di dominio**.
3. Selezionare l'opzione **Abilita polling controller di dominio**.
4. Selezionare il controller di dominio di cui si desidera eseguire il polling.

   Se si utilizza un punto di distribuzione Linux, nella sezione **Esegui polling di domini specifici**, fare clic su **Aggiungi**, quindi specificare l'indirizzo e le credenziali utente del controller di dominio.

   Se si utilizza un punto di distribuzione Windows, è possibile selezionare una delle seguenti opzioni:

   - **Esegui polling dominio corrente**
   - **Esegui polling di tutta la foresta di dominio**
   - **Esegui polling di domini specifici**
5. Fare clic sul pulsante **Imposta pianificazione di polling** per specificare le opzioni di pianificazione del polling, se necessario.

   Il polling viene avviato solo in base alla pianificazione specificata. L'avvio manuale del polling non è disponibile.

Al termine del polling, la struttura del dominio verrà visualizzata nella sezione **Controller di dominio**.

Se sono installate e attivate le regole di spostamento dei dispositivi, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi gestiti**. Se non sono state abilitate regole di spostamento, i nuovi dispositivi individuati vengono automaticamente inclusi nel gruppo **Dispositivi non assegnati**.

Gli account utente rilevati possono essere utilizzati per l'autenticazione del dominio in Kaspersky Security Center Web Console.

Autenticazione e connessione a un controller di dominio

Autenticazione e connessione a un controller di dominio durante il polling di un dominio

Durante il polling di un controller di dominio utilizzando un punto di distribuzione Linux, il punto di distribuzione identifica il protocollo di connessione per stabilire la connessione iniziale al controller di dominio. Questo protocollo viene utilizzato per tutte le connessioni future al controller di dominio. Quando si stabilisce la connessione iniziale al controller di dominio, è possibile modificare le opzioni di connessione utilizzando il flag Network Agent (`KLNAG_LDAP_TLS_REQCERT` e `KLNAG_LDAP_SSL_CACERT`). È possibile configurare i flag Network Agent utilizzando klscflag come descritto in questo articolo.

La connessione iniziale a un controller di dominio procede come segue:

1. Un punto di distribuzione tenta di connettersi al controller di dominio tramite LDAPS.

   Per impostazione predefinita, la verifica del certificato non è richiesta. Impostare il contrassegno `KLNAG_LDAP_TLS_REQCERT` su 1 per applicare la verifica del certificato.

   Possibili valori del contrassegno `KLNAG_LDAP_TLS_REQCERT`:

   - `0`: il certificato viene richiesto, ma se non viene fornito o se la verifica del certificato non è riuscita, la connessione TLS viene considerata ancora creata correttamente (valore predefinito).
   - `1`: è richiesta una verifica rigorosa del certificato del server LDAP.

   Per impostazione predefinita, quando il flag `KLNAG_LDAP_SSL_CACERT` non è specificato, per accedere alla catena di certificati viene utilizzato il percorso dipendente dal sistema operativo dell'autorità di certificazione (CA). Utilizzare il contrassegno `KLNAG_LDAP_SSL_CACERT` per specificare un percorso personalizzato.

2. Se la connessione LDAPS non riesce, un punto di distribuzione Linux tenta di connettersi al controller di dominio tramite una connessione TCP non criptata tramite SASL (DIGEST-MD5).

Configurazione dei contrassegni

È possibile utilizzare l'utilità klscflag per configurare i contrassegni.

In un punto di distribuzione Linux, eseguire la riga dei comandi, quindi modificare la directory corrente nella directory con l'utilità klscflag. Per impostazione predefinita, nel punto di distribuzione Linux l'utilità klscflag si trova in /opt/kaspersky/ksc64/sbin.

Ad esempio, il seguente comando impone la verifica del certificato:

```
klscflag -fset -pv klnagent -n KLNAG_LDAP_TLS_REQCERT -t d -v 1
```

Configurazione di un controller di dominio Samba

Kaspersky Security Center supporta un controller di dominio Linux in esecuzione solo su Samba 4.

Un controller di dominio Samba supporta le stesse estensioni dello schema di un controller di dominio Microsoft Active Directory. È possibile abilitare la piena compatibilità di un controller di dominio Samba con un controller di dominio Microsoft Active Directory utilizzando l'estensione dello schema Samba 4. Questa è un'azione facoltativa.

Si consiglia di abilitare la piena compatibilità di un controller di dominio Samba con un controller di dominio Microsoft Active Directory. In questo modo, si assicurerà la corretta interazione tra Kaspersky Security Center e il controller di dominio Samba.

Per abilitare la piena compatibilità di un controller di dominio Samba con un controller di dominio Microsoft Active Directory:

1. Eseguire il seguente comando per utilizzare l'estensione dello schema RFC2307:

   ```
   samba-tool domain provision --use-rfc2307 --interactive
   ```

2. Abilitare l'aggiornamento dello schema in un controller di dominio Samba. A tale scopo, aggiungere la seguente riga al file `/etc/samba/smb.conf`:

   ```
   dsdb:schema update allowed = true
   ```

   Se l'aggiornamento dello schema viene completato con un errore, è necessario eseguire un ripristino completo del controller di dominio che funge da master dello schema.

Per tutti gli host basati su Linux all'interno di un controller di dominio Samba, specificare il `netbios name` e i parametri del `workgroup` nel file `/etc/samba/smb.conf`. In caso contrario, i risultati del polling potrebbero contenere contenitori host duplicati.

Configurazione delle regole di conservazione per i dispositivi non assegnati

Al termine del polling della rete Windows, i dispositivi trovati vengono inseriti nei sottogruppi del gruppo di amministrazione Dispositivi non assegnati. Questo gruppo di amministrazione è disponibile in **Individuazione e distribuzione** → **Individuazione** → **Domini Windows**. La cartella **Domini Windows** è il gruppo padre. Contiene gruppi figlio denominati in base ai domini e ai gruppi di lavoro corrispondenti rilevati durante il polling. Il gruppo padre può anche contenere il gruppo di amministrazione dei dispositivi mobili. È possibile configurare le regole di conservazione dei dispositivi non assegnati per il gruppo padre e ognuno dei gruppi figlio. Le regole di conservazione non dipendono dalle impostazioni di device discovery e operano anche se la device discovery è disabilitata.

Le regole di conservazione dei dispositivi non influiscono sui dispositivi con una o più unità criptate con Criptaggio dell'intero disco. Tali dispositivi non vengono eliminati automaticamente; è possibile eliminarli solo manualmente. Se è necessario eliminare un dispositivo con un'unità criptata, decriptare prima l'unità, quindi eliminare il dispositivo.

Per configurare le regole di conservazione per i dispositivi non assegnati:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Domini Windows**.
2. Eseguire una delle seguenti operazioni:
   - Per configurare le impostazioni del gruppo padre, fare clic sul pulsante **Proprietà**.
     Verrà visualizzata la finestra delle proprietà del dominio Windows.
   - Per configurare le impostazioni di un gruppo figlio, fare clic sul relativo nome.
     Verrà visualizzata la finestra delle proprietà del gruppo figlio.
3. Definire le seguenti impostazioni:
   - **Rimuovi il dispositivo dal gruppo se è inattivo da più di (giorni)**

     Se questa opzione è abilitata, è possibile specificare l'intervallo di tempo al termine del quale il dispositivo viene rimosso automaticamente dal gruppo. Per impostazione predefinita, questa opzione viene distribuita anche ai gruppi figlio. L'intervallo di tempo predefinito è 7 giorni.

     Per impostazione predefinita, questa opzione è abilitata.
   - **Eredita da gruppo padre**

     Se questa opzione è abilitata, il periodo di conservazione per i dispositivi del gruppo corrente viene ereditato dal gruppo padre e non può essere modificato.

     Questa opzione è disponibile solo per i gruppi figlio.

     Per impostazione predefinita, questa opzione è abilitata.
   - **Forza ereditarietà nei gruppi figlio**

     I valori delle impostazioni vengono distribuiti ai gruppi figlio, ma nelle proprietà dei gruppi figlio tali impostazioni sono bloccate.

     Per impostazione predefinita, questa opzione è disabilitata.
4. Fare clic sul pulsante **Accetta**.

Le modifiche verranno salvate e applicate.

Inventario dei dispositivi

L'elenco dell'hardware (**Operazioni** → **Archivi** → **Hardware**) utilizzato per eseguire l'inventario dei dispositivi viene popolato in due modi: automatico e manuale. Dopo ogni polling di rete, tutti i dispositivi rilevati vengono aggiunti automaticamente all'elenco; tuttavia è anche possibile aggiungere manualmente i dispositivi se non si desidera eseguire il polling della rete. È possibile aggiungere manualmente altri dispositivi all'elenco, ad esempio, router, stampanti o hardware di dispositivi.

Nelle proprietà di un dispositivo è possibile visualizzare e modificare informazioni dettagliate sul dispositivo.

L'elenco dell'hardware può contenere i seguenti tipi di dispositivi:

- Computer
- Dispositivi mobili
- Dispositivi di rete
- Dispositivi virtuali
- Componenti OEM
- Periferiche per computer
- Dispositivi connessi
- Telefoni VoIP
- Archivi di rete

L'amministratore può assegnare l'attributo *Aziendale* ai dispositivi rilevati. Questo attributo può essere assegnato manualmente nelle proprietà di un dispositivo o l'amministratore può specificare criteri per l'assegnazione automatica dell'attributo. In questo caso, l'attributo *Aziendale* viene assegnato in base al tipo di dispositivo.

Kaspersky Security Center consente l'eliminazione dei dispositivi. A tale scopo, selezionare l'opzione **Eliminato** nelle proprietà di un dispositivo. Il dispositivo non verrà visualizzato nell'elenco dei dispositivi.

Un amministratore può gestire l'elenco dei PLC (Programmable Logic Controller) nella cartella **Hardware**. Informazioni dettagliate sulla gestione dell'elenco PLC sono disponibili nel *manuale dell'utente di Kaspersky Industrial CyberSecurity for Nodes*.

Aggiunta di informazioni sui nuovi dispositivi

Per aggiungere informazioni sui nuovi dispositivi nella rete:

1. Nel menu principale, passare a **Operazioni** → **Archivi** → **Hardware**.
2. Fare clic sul pulsante **Aggiungi** per aprire la finestra **Nuovo dispositivo**.
3. Nella finestra **Nuovo dispositivo** selezionare nell'elenco a discesa **Tipo di dispositivo** il tipo di dispositivo da aggiungere.
4. Fare clic su **OK**.

   Verrà visualizzata la finestra delle proprietà del dispositivo, nella sezione **Generale**.

5. Nella sezione **Generale** compilare i campi di immissione con i dati sul dispositivo. Nella sezione **Generale** sono elencate le seguenti impostazioni:

   - **Dispositivo aziendale**. Selezionare la casella di controllo se si desidera assegnare l'attributo *Aziendale* al dispositivo. Utilizzando questo attributo è possibile eseguire la ricerca di dispositivi nella cartella **Hardware**.

   - **Eliminato**. Selezionare la casella di controllo se non si desidera che il dispositivo venga visualizzato nell'elenco dei dispositivi nella cartella **Hardware**.

6. Fare clic su **Applica**.

Il nuovo dispositivo verrà visualizzato nell'area di lavoro della pagina **Hardware**.

Configurazione dei criteri utilizzati per definire i dispositivi aziendali

Per configurare i criteri di rilevamento dei dispositivi aziendali:

1. Nel menu principale, passare a **Operazioni** → **Archivi** → **Hardware**.

2. Nella parte superiore della pagina **Hardware**, fare clic sul collegamento **Configura regola per i dispositivi aziendali**.

   Viene richiamato il pannello **Configura regola per i dispositivi aziendali**.

3. Nel pannello **Configura regola per i dispositivi aziendali**, abilitare **Imposta automaticamente l'attributo Dispositivo aziendale per il dispositivo**. Specificare i tipi di dispositivo a cui viene assegnato automaticamente l'attributo *Enterprise*.

   Questa opzione interessa solo i dispositivi che sono stati aggiunti tramite il polling della rete. Per i dispositivi aggiunti manualmente, impostare manualmente l'attributo *Aziendale*.

4. Fare clic su **OK**.

I criteri di rilevamento per i dispositivi aziendali sono configurati.

Applicazioni Kaspersky: licensing e attivazione

In questa sezione vengono descritte le funzionalità di Kaspersky Security Center relative all'utilizzo delle chiavi di licenza delle applicazioni Kaspersky gestite.

Kaspersky Security Center consente la distribuzione centralizzata delle chiavi di licenza per le applicazioni Kaspersky nei dispositivi client, il monitoraggio del relativo utilizzo e il rinnovo delle licenze.

Quando si aggiunge una chiave di licenza utilizzando Kaspersky Security Center, le impostazioni della chiave di licenza vengono salvate nell'Administration Server. In base a queste informazioni, l'applicazione genera un rapporto sull'utilizzo delle chiavi di licenza e segnala all'amministratore la scadenza delle licenze e la violazione delle limitazioni di licenza specificate nelle proprietà delle chiavi di licenza. È possibile configurare le notifiche dell'utilizzo delle chiavi di licenza nelle impostazioni di Administration Server.

Licensing delle applicazioni gestite

Le applicazioni Kaspersky installate nei dispositivi gestiti devono essere concesse in licenza applicando un codice di attivazione o un file chiave a ognuna delle applicazioni. È possibile distribuire un codice di attivazione o un file chiave nei seguenti modi:

- Distribuzione automatica
- Il pacchetto di installazione di un'applicazione gestita
- Attività *Aggiungi chiave di licenza* per un'applicazione gestita
- Attivazione manuale di un'applicazione gestita

È possibile aggiungere una nuova chiave di licenza attiva o di riserva con uno dei metodi sopra elencati. Un'applicazione Kaspersky utilizza una chiave attiva al momento e memorizza una chiave di riserva da applicare dopo la scadenza della chiave attiva. L'applicazione per la quale si aggiunge una chiave di licenza definisce se la chiave è attiva o aggiuntiva. La definizione della chiave non dipende dal metodo utilizzato per aggiungere una nuova chiave di licenza.

Distribuzione automatica

Se si utilizzano diverse applicazioni gestite ed è necessario distribuire un file chiave specifico o un codice di attivazione specifico nei dispositivi, valutare altre modalità di distribuzione del codice di attivazione o del file chiave in questione.

Kaspersky Security Center consente di distribuire automaticamente le chiavi di licenza disponibili nei dispositivi. Ad esempio, nell'archivio dell'Administration Server sono presenti tre chiavi di licenza. È stata selezionata la casella di controllo **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti** per tutte e tre le chiavi di licenza. Un'applicazione di protezione Kaspersky, ad esempio Kaspersky Endpoint Security for Windows, è installata nei dispositivi dell'organizzazione. Viene rilevato un nuovo dispositivo a cui deve essere distribuita una chiave di licenza. L'applicazione stabilisce, ad esempio, che due delle chiavi di licenza dell'archivio possono essere distribuite al dispositivo: la chiave di licenza denominata *Key_1*e la chiave di licenza denominata *Key_2*. Una di queste chiavi di licenza viene distribuita nel dispositivo. In questo caso non è possibile prevedere quale delle due chiavi di licenza verrà distribuita nel dispositivo poiché la distribuzione automatica delle chiavi di licenza non offre nessuna attività di amministrazione.

Quando una chiave di licenza viene distribuita, i dispositivi vengono ricalcolati per questa chiave di licenza. È necessario accertarsi che il numero di dispositivi in cui è stata distribuita la chiave di licenza non superi la limitazione licenza. Se il numero di dispositivi supera la limitazione licenza, a tutti i dispositivi non coperti dalla licenza verrà assegnato lo stato *Critico*.

Prima della distribuzione, è necessario aggiungere il codice di attivazione o il file chiave all'archivio di Administration Server.

Istruzioni dettagliate:

- Administration Console:
  - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
  - Distribuzione automatica di una chiave di licenza

  o
- Kaspersky Security Center Web Console:
  - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
  - Distribuzione automatica di una chiave di licenza

Si noti che una chiave di licenza distribuita automaticamente potrebbe non essere visualizzata nell'archivio dell'Administration Server virtuale nei seguenti casi:

- La chiave di licenza non è valida per l'applicazione.
- L'Administration Server virtuale non dispone di dispositivi gestiti.
- La chiave di licenza è già stata utilizzata per i dispositivi sotto la gestione di un altro Administration Server virtuale ed è stato raggiunto il limite del numero di dispositivi.

Aggiunta di un file chiave o di un codice di attivazione al pacchetto di installazione di un'applicazione gestita

Per motivi di sicurezza, questa opzione non è consigliata. Un codice di attivazione o un file chiave di licenza aggiunto a un pacchetto di installazione può essere compromesso.

Se si installa un'applicazione gestita utilizzando un pacchetto di installazione, è possibile specificare un codice di attivazione o un file chiave nel pacchetto di installazione o nel criterio dell'applicazione. La chiave di licenza verrà distribuita nei dispositivi gestiti alla successiva sincronizzazione del dispositivo con Administration Server.

Istruzioni dettagliate:

- Administration Console:
  - Creazione di un pacchetto di installazione
  - Installazione delle applicazioni nei dispositivi client

  o
- Kaspersky Security Center Web Console: Aggiunta di una chiave di licenza a un pacchetto di installazione

Distribuzione tramite l'attività di aggiunta della chiave di licenza per un'applicazione gestita

Se si sceglie di utilizzare l'attività *Aggiungi chiave di licenza* per un'applicazione gestita, è possibile selezionare la chiave di licenza che deve essere distribuita nei dispositivi e selezionare i dispositivi nella modalità più opportuna, ad esempio selezionando un gruppo di amministrazione o una selezione dispositivi.

Prima della distribuzione, è necessario aggiungere il codice di attivazione o il file chiave all'archivio di Administration Server.

Istruzioni dettagliate:

- Administration Console:
  - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
  - Distribuzione di una chiave di licenza ai dispositivi client

  o
- Kaspersky Security Center Web Console:
  - Aggiunta di una chiave di licenza all'archivio dell'Administration Server
  - Distribuzione di una chiave di licenza ai dispositivi client

Aggiunta manuale di un codice di attivazione o di un file chiave ai dispositivi

È possibile attivare l'applicazione Kaspersky installata in locale utilizzando gli strumenti disponibili nell'interfaccia dell'applicazione. Fare riferimento alla documentazione dell'applicazione installata.

Aggiunta di una chiave di licenza all'archivio dell'Administration Server

Per aggiungere una chiave di licenza all'archivio dell'Administration Server:

1. Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.
2. Fare clic sul pulsante **Aggiungi**.
3. Scegliere cosa si desidera aggiungere:
   - **Aggiungi un file chiave**

     Fare clic sul pulsante **Seleziona file chiave** e selezionare il file .key da aggiungere.
   - **Immetti il codice di attivazione**

     Specificare il codice di attivazione nel campo di testo e fare clic sul pulsante **Invia**.
4. Fare clic sul pulsante **Chiudi**.

Una o più chiavi di licenza verranno aggiunte all'archivio dell'Administration Server.

Aggiunta di una chiave di licenza di Administration Server

Per aggiungere una chiave di licenza di Administration Server:

1. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server che verrà visualizzata selezionare la sezione **Chiavi di licenza**.
3. Nella sezione **Chiave di licenza attiva**, fare clic sul pulsante **Modifica**.
4. Nella finestra visualizzata, aggiungere una chiave di licenza facendo clic sul pulsante **Aggiungi**.

   Verrà visualizzata l'Aggiunta guidata chiave di licenza.

Al termine della procedura guidata, è possibile verificare se le funzionalità sono visualizzate in Administration Console in base alla licenza corrispondente.

Distribuzione di una chiave di licenza ai dispositivi client

Kaspersky Security Center Web Console consente la distribuzione di una chiave di licenza ai dispositivi client automaticamente o tramite l'attività **Attivazione dell'applicazione**. È possibile utilizzare l'attività per distribuire le chiavi a un gruppo di dispositivi specifico. Durante la distribuzione di una chiave di licenza tramite l'attività, il limite di licenze relativo al numero di dispositivi non viene tenuto in considerazione. Utilizzare la distribuzione automatica delle chiavi per interrompere automaticamente la distribuzione di una chiave di licenza quando viene raggiunto il limite di licenze.

Se si abilita la distribuzione automatica di una chiave di licenza, non creare un'attività **Attivazione dell'applicazione** per distribuire tale chiave ai dispositivi client. In caso contrario, il carico su Administration Server aumenterà a causa della frequente sincronizzazione.

Prima della distribuzione, aggiungere una chiave di licenza all'archivio dell'Administration Server.

*Per distribuire una chiave di licenza ai dispositivi client tramite l'attività **Attivazione dell'applicazione**:*

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la **Creazione guidata nuova attività**. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Nell'elenco a discesa **Applicazione**, selezionare l'applicazione per la quale si desidera aggiungere una chiave di licenza.
4. Nell'elenco **Tipo di attività**, selezionare l'attività **Attivazione dell'applicazione**.
5. Nel campo **Nome attività**, specificare il nome della nuova attività.
6. Selezionare i dispositivi a cui assegnare l'attività.

7. Nel passaggio **Selezione di una chiave di licenza** della procedura guidata, fare clic sul collegamento **Aggiungi chiave** per aggiungere la chiave di licenza.

8. Nel riquadro di aggiunta della chiave, aggiungere la chiave di licenza utilizzando una delle seguenti opzioni:

   È necessario aggiungere la chiave di licenza solo se non è stata aggiunta all'archivio dell'Administration Server prima di creare l'attività **Attivazione dell'applicazione**.

   - Selezionare l'opzione **Immetti il codice di attivazione** per immettere un codice di attivazione, quindi effettuare le seguenti operazioni:

     a. Specificare il codice di attivazione, quindi fare clic sul pulsante **Invia**.

        Le informazioni sulla chiave di licenza vengono visualizzate nel riquadro di aggiunta della chiave.

     b. Fare clic sul pulsante **Salva**.

        Se si desidera distribuire automaticamente la chiave di licenza ai dispositivi gestiti, abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

        Il riquadro di aggiunta delle chiavi viene chiuso.

   - Selezionare l'opzione **Aggiungi un file chiave** per aggiungere un file chiave, quindi effettuare le seguenti operazioni:

     a. Fare clic sul pulsante **Seleziona file chiave**.

     b. Nella finestra visualizzata, selezionare un file chiave, quindi fare clic sul pulsante **Apri**.

        Le informazioni sulla chiave di licenza vengono visualizzate nel riquadro di aggiunta della chiave di licenza.

     c. Fare clic sul pulsante **Salva**.

        Se si desidera distribuire automaticamente la chiave di licenza ai dispositivi gestiti, abilitare l'opzione **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.

        Il riquadro di aggiunta delle chiavi viene chiuso.

9. Selezionare la chiave di licenza nella tabella delle chiavi.

10. Nel passaggio **Informazioni sulla licenza** della procedura guidata, deselezionare la casella di controllo **Usa come chiave di riserva** predefinita se si desidera sostituire la chiave di licenza attiva.

    Ad esempio, questo è necessario quando l'organizzazione cambia ed è richiesta la chiave di un'altra organizzazione nel dispositivo o se la chiave è stata riemessa e una nuova licenza scade prima della licenza corrente. Per evitare errori, è necessario deselezionare la casella di controllo **Usa come chiave di riserva**.

    Per ulteriori informazioni sui problemi che possono verificarsi durante l'aggiunta di una chiave di licenza a Kaspersky Security Center e sui modi per risolverli, fare riferimento alla Knowledge Base di Kaspersky Security Center.

11. Nel passaggio **Completare la creazione dell'attività** della procedura guidata, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** per modificare le impostazioni predefinite dell'attività.

    Se non si abilita questa opzione, l'attività verrà creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in un secondo momento.

12. Fare clic sul pulsante **Fine**.

    La procedura guidata crea l'attività: Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata automaticamente la finestra delle proprietà dell'attività. In questa finestra, è possibile specificare le impostazioni generali dell'attività e, se necessario, modificare le impostazioni specificate durante la creazione dell'attività.

    > È inoltre possibile aprire la finestra delle proprietà dell'attività facendo clic sul nome dell'attività creata nell'elenco delle attività.

    L'attività verrà creata, configurata e visualizzata nell'elenco delle attività.

13. Per eseguire l'attività, selezionarla nell'elenco delle attività, quindi fare clic sul pulsante **Avvia**.

    È inoltre possibile impostare una pianificazione per l'avvio dell'attività nella scheda **Pianificazione** della finestra delle proprietà dell'attività.

    Per una descrizione dettagliata delle impostazioni di avvio pianificato, fare riferimento alle impostazioni generali dell'attività.

Una volta completata l'attività, la chiave di licenza viene distribuita nei dispositivi selezionati.

Distribuzione automatica di una chiave di licenza

Kaspersky Security Center consente la distribuzione automatica delle chiavi di licenza ai dispositivi gestiti, se sono presenti nell'archivio delle chiavi di licenza in Administration Server.

Per distribuire automaticamente una chiave di licenza ai dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.
2. Fare clic sul nome della chiave di licenza da distribuire automaticamente ai dispositivi.
3. Nella finestra delle proprietà della chiave di licenza visualizzata, selezionare la casella di controllo **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti**.
4. Fare clic sul pulsante **Salva**.

La chiave di licenza verrà automaticamente distribuita a tutti i dispositivi compatibili.

La distribuzione della chiave di licenza viene eseguita tramite Network Agent. Non vengono create attività di distribuzione della chiave di licenza per l'applicazione.

Durante la distribuzione automatica di una chiave di licenza, viene tenuto in considerazione il limite di licenze relativo al numero di dispositivi. Il limite di licenze è impostato nelle proprietà della chiave di licenza. Se viene raggiunto il limite di licenze, la distribuzione della chiave di licenza nei dispositivi si interrompe automaticamente.

Si noti che una chiave di licenza distribuita automaticamente potrebbe non essere visualizzata nell'archivio dell'Administration Server virtuale nei seguenti casi:

- La chiave di licenza non è valida per l'applicazione.
- L'Administration Server virtuale non dispone di dispositivi gestiti.
- La chiave di licenza è già stata utilizzata per i dispositivi sotto la gestione di un altro Administration Server virtuale ed è stato raggiunto il limite del numero di dispositivi.

L'Administration Server virtuale distribuisce automaticamente le chiavi di licenza dal proprio archivio e dall'archivio di Administration Server. È consigliabile:

- Utilizzare l'attività *Aggiungi chiave di licenza* per selezionare la chiave di licenza da distribuire nei dispositivi.
- Evitare di disabilitare l'opzione **Consenti la distribuzione automatica delle chiavi di licenza di questo Administration Server virtuale nei relativi dispositivi** nelle impostazioni dell'Administration Server virtuale. In caso contrario, l'Administration Server virtuale non distribuirà le chiavi di licenza ai dispositivi, comprese le chiavi di licenza dall'archivio di Administration Server.

Se si seleziona la casella di controllo **Distribuisci automaticamente la chiave di licenza nei dispositivi gestiti** nella finestra delle proprietà della chiave di licenza, nella rete viene immediatamente distribuita una chiave di licenza. Se non si seleziona questa opzione, è possibile utilizzare un'attività per distribuire una chiave di licenza in un secondo momento.

La distribuzione automatica delle chiavi di licenza configurate nell'Administration Server primario non si estende ai dispositivi gestiti da Administration Server secondari non virtuali.

Visualizzazione delle informazioni sulle chiavi di licenza in uso

Per visualizzare l'elenco delle chiavi di licenza aggiunte all'archivio di Administration Server:

Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.

L'elenco visualizzato contiene i file chiave e i codici di attivazione aggiunti all'archivio di Administration Server.

Per visualizzare informazioni dettagliate su una chiave di licenza:

1. Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.
2. Fare clic sul nome della chiave di licenza desiderata.

Nella finestra delle proprietà della chiave di licenza visualizzata è possibile visualizzare:

- Nella scheda **Generale**: le informazioni principali sulla chiave di licenza
- Nella scheda **Dispositivi**: l'elenco dei dispositivi client in cui è stata utilizzata la chiave di licenza per l'attivazione dell'applicazione Kaspersky installata

Per visualizzare quali chiavi di licenza sono distribuite in un dispositivo client specifico:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo desiderato.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Applicazioni**.
4. Fare clic sul nome dell'applicazione per cui si desidera visualizzare le informazioni sulla chiave di licenza.
5. Nella finestra delle proprietà dell'applicazione visualizzata, selezionare la scheda **Generale** e quindi aprire la sezione **Licenza**.

Verranno visualizzate le informazioni principali sulla chiave di licenza attiva e quella di riserva.

Per definire le impostazioni aggiornate delle chiavi di licenza dell'Administration Server virtuale, l'Administration Server invia una richiesta ai server di attivazione di Kaspersky almeno una volta al giorno. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici.

Rimozione di una chiave di licenza dall'archivio

Quando si rimuove la chiave di licenza attiva per una funzionalità aggiuntiva di Administration Server, ad esempio Vulnerability e patch management o Mobile Device Management, la funzionalità corrispondente diventa non disponibile. Se è stata aggiunta una chiave di licenza di riserva, questa diventa automaticamente la chiave di licenza attiva quando viene rimossa la precedente chiave di licenza attiva.

Quando si rimuove la chiave di licenza attiva distribuita in un dispositivo gestito, l'applicazione continuerà a funzionare sul dispositivo gestito.

Per rimuove un file chiave o un codice di attivazione dall'archivio di Administration Server:

1. Verificare che Administration Server non utilizzi un file chiave o un codice di attivazione che si desidera rimuovere. In questo caso, non è possibile rimuovere la chiave. Per eseguire il controllo:
   a. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

      Verrà visualizzata la finestra delle proprietà di Administration Server.

   b. Nella scheda **Generale** selezionare la sezione **Chiavi di licenza**.
   c. Se il file chiave o il codice di attivazione desiderato viene visualizzato nella sezione aperta, fare clic sul pulsante **Rimuovi chiave di licenza attiva**, quindi confermare l'operazione. Successivamente, Administration Server non utilizza la chiave di licenza rimossa, ma la chiave rimane nell'archivio dell'Administration Server. Se il file chiave o il codice di attivazione o desiderato non viene visualizzato, Administration Server non lo utilizza.
2. Nel menu principale accedere a **Operazioni** → **Licensing** → **Licenze di Kaspersky**.
3. Selezionare il file chiave o il codice di attivazione richiesti, quindi fare clic sul pulsante **Elimina**.

Il file chiave o il codice di attivazione selezionato verrà rimosso dall'archivio.

È possibile aggiungere nuovamente una chiave di licenza rimossa o aggiungerne una nuova.

Revoca del consenso a un Contratto di licenza con l'utente finale

Se si decide di interrompere la protezione di alcuni dispositivi client, è possibile revocare il Contratto di licenza con l'utente finale (EULA) per qualsiasi applicazione Kaspersky gestita. È necessario disinstallare l'applicazione selezionata prima di revocarne il Contratto di licenza con l'utente finale.

I Contratti di licenza con l'utente finale accettati in un Administration Server virtuale possono essere revocati nell'Administration Server virtuale o nell'Administration Server primario. I Contratti di licenza con l'utente finale accettati in un Administration Server primario possono essere revocati solo nell'Administration Server primario.

Per revocare un EULA per le applicazioni Kaspersky gestite:

1. Aprire la finestra delle proprietà di Administration Server e, nella scheda **Generale**, selezionare la sezione **Contratti di licenza con l'utente finale**.

   Verrà visualizzato un elenco degli EULA accettati al momento della creazione dei pacchetti di installazione, dell'installazione immediata degli aggiornamenti o della distribuzione di Kaspersky Security for Mobile.

2. Nell'elenco selezionare il Contratto di licenza con l'utente finale che si desidera revocare.

   È possibile visualizzare le seguenti proprietà degli EULA:

   - Data di accettazione del Contratto di licenza con l'utente finale
   - Nome dell'utente che ha accettato il Contratto di licenza con l'utente finale

3. Fare clic sulla data di accettazione di qualsiasi Contratto di licenza con l'utente finale per aprirne la finestra delle proprietà in cui sono visualizzati i seguenti dati:

   - Nome dell'utente che ha accettato il Contratto di licenza con l'utente finale
   - Data di accettazione del Contratto di licenza con l'utente finale
   - Identificatore univoco (UID) del Contratto di licenza con l'utente finale
   - Testo completo del Contratto di licenza con l'utente finale
   - Elenco di oggetti (pacchetti di installazione, aggiornamenti immediati, app mobili) collegati al Contratto di licenza con l'utente finale e relativi nomi e tipi

4. Nella parte inferiore della finestra delle proprietà del Contratto di licenza con l'utente finale fare clic sul pulsante **Revoca Contratto di licenza**.

   Se esistono oggetti (pacchetti di installazione e rispettive attività) che impediscono la revoca del Contratto di licenza con l'utente finale, viene visualizzata la notifica corrispondente. Non è possibile procedere con la revoca fino a quando non si eliminano questi oggetti.

   Nella finestra visualizzata l'utente viene informato della necessità di disinstallare prima l'applicazione Kaspersky corrispondente al Contratto di licenza con l'utente finale.

5. Fare clic sul pulsante per confermare la revoca.

L'EULA è revocato. Non viene più visualizzato nell'elenco dei Contratti di licenza nella sezione **Contratti di licenza con l'utente finale**. La finestra delle proprietà del Contratto di licenza con l'utente finale viene chiusa; l'applicazione non è più installata.

Rinnovo delle licenze per le applicazioni Kaspersky

È possibile rinnovare una licenza dell'applicazione Kaspersky scaduta o in scadenza (fra meno di 30 giorni).

Per rinnovare una licenza scaduta o una licenza che sta per scadere:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Operazioni → Licensing → Licenze di Kaspersky**.
   - Nel menu principale, passare a **Monitoraggio e generazione dei rapporti → Dashboard**, quindi fare clic sul collegamento **View expiring licenses** accanto a una notifica.

   Verrà visualizzata la finestra **Licenze di Kaspersky** in cui è possibile visualizzare e rinnovare le licenze.

2. Fare clic sul collegamento **Rinnova licenza** accanto alla licenza richiesta.

   Facendo clic su un collegamento per il rinnovo della licenza l'utente accetta di trasferire a Kaspersky le seguenti informazioni su Kaspersky Security Center: la versione, la localizzazione in uso, l'ID della licenza software (cioè l'ID della licenza per la quale si sta eseguendo il rinnovo) e se la licenza è stata acquistata tramite un'azienda partner o meno.

3. Nella finestra del servizio di rinnovo della licenza visualizzata seguire le istruzioni per rinnovare una licenza.

   La licenza viene rinnovata.

In Kaspersky Security Center Web Console le notifiche vengono visualizzate quando una licenza sta per scadere, in base alla seguente pianificazione:

- 30 giorni prima della scadenza
- 7 giorni prima della scadenza
- 3 giorni prima della scadenza
- 24 ore prima della scadenza
- Quando una licenza è scaduta

Utilizzo di Kaspersky Marketplace per scegliere le soluzioni aziendali Kaspersky

Marketplace è una sezione del menu principale che consente di visualizzare l'intera gamma di soluzioni aziendali Kaspersky, selezionare quelle desiderate e procedere all'acquisto nel sito Web di Kaspersky. È possibile utilizzare i filtri per visualizzare solo le soluzioni che si adattano alla propria organizzazione e ai requisiti del proprio sistema di sicurezza delle informazioni. Quando si seleziona una soluzione, Kaspersky Security Center reindirizza alla relativa pagina Web nel sito Web di Kaspersky per ulteriori informazioni sulla soluzione. Ogni pagina Web consente di procedere all'acquisto o contiene istruzioni sulla procedura di acquisto.

Nella sezione **Marketplace** è possibile filtrare le soluzioni Kaspersky utilizzando i seguenti criteri:

- Numero di dispositivi (endpoint, server e altri tipi di asset) che si desidera proteggere:
  - 50–250
  - 250–1000
  - Più di 1000
- Livello di maturità del team di sicurezza delle informazioni dell'organizzazione:
  - **Foundations**

    Questo livello è tipico delle aziende che dispongono solo di un team IT. Il numero massimo di minacce possibili viene bloccato automaticamente.
  - **Optimum**

    Questo livello è tipico delle aziende che hanno una funzione di sicurezza IT specifica all'interno del team IT. A questo livello, le aziende richiedono soluzioni che consentano loro di contrastare le minacce commodity e le minacce che eludono i meccanismi di prevenzione esistenti.
  - **Expert**

    Questo livello è tipico delle aziende con ambienti IT complessi e distribuiti. Il team di sicurezza IT ha un livello di maturità ottimale o l'azienda dispone di un team SOC (Security Operations Center). Le soluzioni richieste consentono alle aziende di contrastare minacce complesse e attacchi mirati.
- Tipi di asset da proteggere:
  - **Endpoint**: workstation dei dipendenti, macchine fisiche e virtuali, sistemi integrati
  - **Server**: server fisici e virtuali
  - **Cloud**: ambienti cloud pubblici, privati o ibridi; servizi cloud
  - **Rete**: LAN, infrastruttura IT
  - **Servizio**: servizi relativi alla sicurezza forniti da Kaspersky

Per trovare e acquistare una soluzione aziendale Kaspersky:

1. Nel menu principale accedere a **Marketplace**.

   Per impostazione predefinita, la sezione mostra tutte le soluzioni aziendali Kaspersky disponibili.

2. Per visualizzare solo le soluzioni adatte alla propria organizzazione, selezionare i valori desiderati nei filtri.

3. Fare clic sulla soluzione che si desidera acquistare o per cui si desidera ottenere maggiori informazioni.

   Si verrà reindirizzati alla pagina Web della soluzione. È possibile seguire le istruzioni visualizzate per procedere all'acquisto.

Configurazione della protezione di rete

Questa sezione contiene informazioni sulla configurazione manuale di criteri e attività, sui ruoli utente, sulla creazione di una struttura di gruppi di amministrazione e sulla gerarchia delle attività.

Scenario: Configurazione della protezione di rete

L'avvio rapido guidato crea criteri e attività con le impostazioni predefinite. Queste impostazioni possono risultare non ottimali o addirittura non consentite dall'organizzazione. Pertanto, è consigliabile ottimizzare tali criteri e attività e creare altri criteri e attività, se necessario per la rete.

Prerequisiti

Prima di iniziare, verificare di avere:

- Installato Kaspersky Security Center Administration Server
- Installato Kaspersky Security Center Web Console (facoltativo)
- completato lo scenario di installazione principale di Kaspersky Security Center
- completato l'Avvio rapido guidato o creato manualmente i seguenti criteri e attività nel gruppo di amministrazione **Dispositivi gestiti**:
  - Criterio di Kaspersky Endpoint Security
  - Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
  - Criterio di Network Agent
  - Attività *Trova vulnerabilità e aggiornamenti richiesti*

La configurazione della protezione della rete procede per fasi:

1. **Installazione e propagazione dei criteri e dei profili criterio delle applicazioni Kaspersky**

Per configurare e propagare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti, è possibile utilizzare due diversi metodi di gestione della protezione: quello incentrato sui dispositivi o quello incentrato sugli utenti. Questi due metodi possono anche essere combinati. Per l'implementazione della gestione della protezione incentrata sui dispositivi, è possibile utilizzare gli strumenti offerti in Administration Console basata su Microsoft Management Console o Kaspersky Security Center Web Console. La gestione della protezione incentrata sugli utenti può essere implementata solo tramite Kaspersky Security Center Web Console.

2. **Configurazione delle attività per la gestione remota delle applicazioni Kaspersky**

   Controllare le attività create con l'avvio rapido guidato e, se necessario, ottimizzarle.

   Istruzioni dettagliate:

   - Administration Console:
     - Configurazione dell'attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
     - Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
   - Kaspersky Security Center Web Console:
     - Configurazione dell'attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
     - Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

   Se necessario, creare attività aggiuntive per gestire le applicazioni Kaspersky installate nei dispositivi client.

3. **Valutazione e limitazione del carico di eventi nel database**

   Le informazioni sugli eventi che si verificano durante il funzionamento delle applicazioni gestite vengono trasferite da un dispositivo client e registrate nel database di Administration Server. Per ridurre il carico su Administration Server, valutare e limitare il numero massimo di eventi che possono essere archiviati nel database.

   Istruzioni dettagliate:

   - Administration Console: Impostazione del numero massimo di eventi
   - Kaspersky Security Center Web Console: Impostazione del numero massimo di eventi

Risultati

Quando viene completato questo scenario, la rete sarà protetta tramite la configurazione delle applicazioni Kaspersky, delle attività e degli eventi ricevuti da parte di Administration Server:

- Le applicazioni Kaspersky sono configurate in base ai criteri e ai profili criterio.
- Le applicazioni vengono gestite attraverso un set di attività.
- Viene impostato il numero massimo di eventi che è possibile archiviare nel database.

Al termine della configurazione della protezione di rete, è possibile procedere alla configurazione degli aggiornamenti standard nei database e nelle applicazioni Kaspersky.

Per informazioni dettagliate su come configurare le risposte automatiche alle minacce rilevate da Kaspersky Sandbox, fare riferimento alla Guida in linea di Kaspersky Sandbox 2.0.

Informazioni sui metodi di gestione della protezione incentrati sui dispositivi e incentrati sugli utenti

È possibile gestire le impostazioni di protezione dal punto di vista delle funzionalità del dispositivo e dal punto di vista dei ruoli utente. Il primo metodo è denominato *gestione della protezione incentrata sui dispositivi* e il secondo è denominato *gestione della protezione incentrata sugli utenti*. Per applicare impostazioni dell'applicazione diverse a diversi dispositivi è possibile utilizzare uno o entrambi i tipi di gestione insieme. Per l'implementazione della gestione della protezione incentrata sui dispositivi, è possibile utilizzare gli strumenti offerti in Administration Console basata su Microsoft Management Console o Kaspersky Security Center Web Console. La gestione della protezione incentrata sugli utenti può essere implementata solo tramite Kaspersky Security Center Web Console.

La gestione della protezione incentrata sui dispositivi consente di applicare diverse impostazioni dell'applicazione di protezione ai dispositivi gestiti in base alle funzionalità specifiche del dispositivo. È ad esempio possibile applicare impostazioni diverse ai dispositivi allocati in diversi gruppi di amministrazione. È inoltre possibile differenziare i dispositivi in base all'utilizzo di tali dispositivi in Active Directory o alle relative specifiche hardware.

La gestione della protezione incentrata sugli utenti consente di applicare diverse impostazioni dell'applicazione di protezione a diversi ruoli utente. È possibile creare diversi ruoli utente, assegnare un ruolo utente appropriato a ciascun utente e definire diverse impostazioni dell'applicazione per i dispositivi di proprietà di utenti con ruoli diversi. È ad esempio possibile applicare differenti impostazioni dell'applicazione ai dispositivi degli addetti alla contabilità e degli specialisti delle risorse umane (HR). Di conseguenza, quando viene implementata la gestione della protezione incentrata sugli utenti, ciascun reparto (reparto account e reparto HR) dispone della propria configurazione delle impostazioni per le applicazioni Kaspersky. Una configurazione delle impostazioni definisce le impostazioni delle applicazioni che possono essere modificate dagli utenti e quelle che vengono forzatamente impostate e bloccate dall'amministratore.

Utilizzando la gestione della protezione incentrata sugli utenti è possibile applicare impostazioni specifiche di un'applicazione per singoli utenti. Questo può essere necessario quando un dipendente ha un ruolo esclusivo nell'azienda o quando si desidera monitorare i problemi di sicurezza relativi ai dispositivi di una persona specifica. A seconda del ruolo di questo dipendente nell'azienda, è possibile espanderne o limitarne i diritti di modifica delle impostazioni dell'applicazione. È ad esempio possibile espandere i diritti di un amministratore di sistema che gestisce i dispositivi client in una sede locale.

È inoltre possibile combinare gli approcci di gestione della protezione incentrata sui dispositivi e incentrata sugli utenti. È ad esempio possibile configurare uno specifico criterio dell'applicazione per ogni gruppo di amministrazione e quindi creare profili criterio per uno o più ruoli utente dell'azienda. In questo caso criteri e profili criterio vengono applicati nel seguente ordine:

1. Vengono applicati i criteri creati per la gestione della protezione incentrata sui dispositivi.
2. Questi vengono modificati dai profili criterio secondo le priorità dei profili criterio.
3. I criteri vengono modificati dai profili criterio associati ai ruoli utente.

Configurazione e propagazione dei criteri: approccio incentrato sui dispositivi

Al termine di questo scenario, le applicazioni saranno configurate in tutti i dispositivi gestiti in base ai criteri delle applicazioni e ai profili criterio specificati.

Prerequisiti

Prima di iniziare, verificare di aver installato Kaspersky Security Center Administration Server e Kaspersky Security Center Web Console (opzionale). Se è stato installato Kaspersky Security Center Web Console, è inoltre consigliabile valutare la gestione della protezione incentrata sugli utenti come opzione alternativa o aggiuntiva rispetto all'approccio incentrato sui dispositivi.

Passaggi

Lo scenario di gestione incentrata sui dispositivi delle applicazioni Kaspersky comprende i seguenti passaggi:

1. **Configurazione dei criteri delle applicazioni**

   Configurare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti tramite la creazione di un criterio per ogni applicazione. Questo set di criteri sarà propagato ai dispositivi client.

   Quando si configura la protezione della rete in Avvio rapido guidato, Kaspersky Security Center crea il criterio predefinito per le seguenti applicazioni:

   - Kaspersky Endpoint Security for Windows: per dispositivi client basati su Windows
   - Kaspersky Endpoint Security for Linux: per dispositivi client basati su Linux

   Se è stata completata la configurazione tramite questa procedura guidata, non è necessario creare un nuovo criterio per questa applicazione. Passare alla configurazione manuale del criterio di Kaspersky Endpoint Security.

   Se si dispone di una struttura gerarchica con più Administration Server e/o gruppi di amministrazione, per impostazione predefinita gli Administration Server secondari e i gruppi di amministrazione figlio ereditano i criteri dall'Administration Server primario. È possibile forzare l'ereditarietà da parte dei gruppi figlio e degli Administration Server secondari per impedire eventuali modifiche delle impostazioni configurate nel criterio upstream. Se si desidera forzare l'ereditarietà solo di una parte delle impostazioni, è possibile bloccarle nel criterio upstream. Le restanti impostazioni sbloccate saranno disponibili per la modifica nei criteri downstream. La gerarchia di criteri creata consente di gestire in modo efficace i dispositivi nei gruppi di amministrazione.

   Istruzioni dettagliate:

   - Administration Console: Creazione di un criterio
   - Kaspersky Security Center Web Console: Creazione di un criterio

2. **Creazione dei profili criterio (facoltativo)**

   Se si desidera applicare differenti impostazioni dei criteri ai dispositivi all'interno di un singolo gruppo di amministrazione, creare profili criterio per tali dispositivi. Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo nel dispositivo gestito.

   Utilizzando le condizioni di attivazione del profilo, è possibile applicare diversi profili criterio, ad esempio ai dispositivi appartenenti a un determinato gruppo di protezione o a un'unità specifica di Active Directory, con una specifica configurazione hardware o contrassegnati con tag specifici. Utilizzare i tag per filtrare i dispositivi che soddisfano i criteri specificati. È ad esempio possibile creare un tag denominato *Windows*, contrassegnare tutti i dispositivi con sistema operativo Windows con questo tag e quindi specificare il tag come condizione di attivazione per un profilo criterio. Come risultato, le applicazioni Kaspersky installate in tutti i dispositivi che eseguono Windows verranno gestite dal profilo criterio corrispondente.

   Istruzioni dettagliate:

   - Administration Console:

- Creazione di un profilo criterio
- Creazione di una regola di attivazione del profilo criterio

- Kaspersky Security Center Web Console:
  - Creazione di un profilo criterio
  - Creazione di una regola di attivazione del profilo criterio

3. **Propagazione di criteri e profili criterio nei dispositivi gestiti**

   Per impostazione predefinita, Administration Server si sincronizza automaticamente con i dispositivi gestiti ogni 15 minuti. È possibile ignorare la sincronizzazione automatica ed eseguire manualmente la sincronizzazione utilizzando il comando Forza sincronizzazione. Anche la sincronizzazione viene forzata dopo aver creato o modificato un criterio o un profilo criterio. Durante la sincronizzazione, i criteri e i profili criterio nuovi o modificati vengono propagati ai dispositivi gestiti.

   Se si utilizza Kaspersky Security Center Web Console, è possibile verificare se a un dispositivo sono stati inviati criteri e profili criterio. Kaspersky Security Center specifica la data e l'ora di invio nelle proprietà del dispositivo.

   Istruzioni dettagliate:

   - Administration Console: Sincronizzazione forzata
   - Kaspersky Security Center Web Console: Sincronizzazione forzata

Risultati

Al termine dello scenario incentrato sui dispositivi, le applicazioni Kaspersky vengono configurate in base alle impostazioni specificate e propagate tramite la gerarchia di criteri.

I criteri delle applicazioni e i profili criterio configurati verranno applicati automaticamente ai nuovi dispositivi aggiunti ai gruppi di amministrazione.

Configurazione e propagazione dei criteri: approccio incentrato sull'utente

Questa sezione descrive lo scenario relativo all'approccio incentrato sugli utenti alla configurazione centralizzata delle applicazioni Kaspersky installate nei dispositivi gestiti. Al termine di questo scenario, le applicazioni saranno configurate in tutti i dispositivi gestiti in base ai criteri delle applicazioni e ai profili criterio specificati.

> Questo scenario può essere implementato tramite Kaspersky Security Center Web Console versione 13 o successive.

Prerequisiti

Prima di iniziare, verificare di aver installato correttamente Kaspersky Security Center Administration Server e Kaspersky Security Center Web Console e completato lo scenario di installazione principale. È inoltre possibile valutare la gestione della protezione incentrata sui dispositivi come opzione alternativa o aggiuntiva all'approccio incentrato sugli utenti. Ulteriori informazioni sui due approcci di gestione.

Processo

Lo scenario di gestione incentrata sugli utenti delle applicazioni Kaspersky comprende i seguenti passaggi:

1. **Configurazione dei criteri delle applicazioni**

   Configurare le impostazioni per le applicazioni Kaspersky installate nei dispositivi gestiti tramite la creazione di un criterio per ogni applicazione. Questo set di criteri sarà propagato ai dispositivi client.

   Quando si configura la protezione della rete in Avvio rapido guidato, Kaspersky Security Center crea il criterio predefinito per Kaspersky Endpoint Security. Se è stata completata la configurazione tramite questa procedura guidata, non è necessario creare un nuovo criterio per questa applicazione. Passare alla configurazione manuale del criterio di Kaspersky Endpoint Security.

   Se si dispone di una struttura gerarchica con più Administration Server e/o gruppi di amministrazione, per impostazione predefinita gli Administration Server secondari e i gruppi di amministrazione figlio ereditano i criteri dall'Administration Server primario. È possibile forzare l'ereditarietà da parte dei gruppi figlio e degli Administration Server secondari per impedire eventuali modifiche delle impostazioni configurate nel criterio upstream. Se si desidera forzare l'ereditarietà solo di una parte delle impostazioni, è possibile bloccarle nel criterio upstream. Le restanti impostazioni sbloccate saranno disponibili per la modifica nei criteri downstream. La gerarchia di criteri creata consente di gestire in modo efficace i dispositivi nei gruppi di amministrazione.

   Istruzioni dettagliate: Creazione di un criterio

2. **Specificazione dei proprietari dei dispositivi**

   Assegnare i dispositivi gestiti agli utenti corrispondenti.

   Istruzioni dettagliate: Assegnazione di un utente come proprietario dispositivo

3. **Definizione dei ruoli utente tipici dell'azienda**

   Prendere in considerazione i diversi tipi di attività eseguite dai dipendenti dell'azienda. È necessario suddividere tutti i dipendenti in base ai rispettivi ruoli. È ad esempio possibile suddividerli per reparto, professioni o posizioni. A questo punto, sarà necessario creare un ruolo utente per ciascun gruppo. Tenere presente che ogni ruolo utente avrà uno specifico profilo criterio che contiene le impostazioni delle applicazioni specifiche per questo ruolo.

4. **Creazione dei ruoli utente**

   Creare e configurare un ruolo utente per ogni gruppo di dipendenti che è stato definito nel passaggio precedente o utilizzare i ruoli utente predefiniti. I ruoli utente conterranno set di diritti di accesso alle funzionalità dell'applicazione.

   Istruzioni dettagliate: Creazione di un ruolo utente

5. **Definizione dell'ambito di ogni ruolo utente**

   Per ognuno dei ruoli utente creati, definire gli utenti e/o i gruppi di protezione e i gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

   Istruzioni dettagliate: Modifica dell'ambito di un ruolo utente

6. **Creazione di profili criterio**

   Creare un profilo criterio per ogni ruolo utente nell'organizzazione. I profili criterio definiscono le impostazioni che saranno applicate alle applicazioni installate nei dispositivi degli utenti, a seconda del ruolo di ogni utente.

   Istruzioni dettagliate: Creazione di un profilo criterio

7. **Associazione dei profili criterio ai ruoli utente**

Associare i profili criterio creati ai ruoli utente. In tal modo, il profilo criterio diventa attivo per un utente che ha il ruolo specificato. Le impostazioni configurate nel profilo criterio verranno applicate alle applicazioni Kaspersky installate nei dispositivi dell'utente.

Istruzioni dettagliate: Associazione dei profili criterio ai ruoli

8. **Propagazione di criteri e profili criterio nei dispositivi gestiti**

   Per impostazione predefinita, Administration Server si sincronizza automaticamente con i dispositivi gestiti ogni 15 minuti. Durante la sincronizzazione, i criteri e i profili criterio nuovi o modificati vengono propagati ai dispositivi gestiti. È possibile ignorare la sincronizzazione automatica ed eseguire manualmente la sincronizzazione utilizzando il comando Forza sincronizzazione. Al termine della sincronizzazione, i criteri e i profili criterio vengono inviati e applicati alle applicazioni Kaspersky installate.

   È possibile verificare se i criteri e i profili criterio sono stati distribuiti a un dispositivo. Kaspersky Security Center specifica la data e l'ora di invio nelle proprietà del dispositivo.

   Istruzioni dettagliate: Sincronizzazione forzata

Risultati

Al termine dello scenario incentrato sugli utenti, le applicazioni Kaspersky vengono configurate in base alle impostazioni specificate e propagate tramite la gerarchia di criteri e profili criterio.

Per un nuovo utente, sarà necessario creare un nuovo account e quindi assegnare all'utente uno dei ruoli utente creati e i dispositivi. I criteri delle applicazioni e i profili criterio configurati verranno applicati automaticamente ai dispositivi di questo utente.

Impostazioni del criterio di Network Agent

Per configurare il criterio di Network Agent:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul nome del criterio di Network Agent.

   Verrà visualizzata la finestra delle proprietà del criterio di Network Agent.

Consultare la tabella di confronto che illustra nel dettaglio come si applicano le impostazioni riportate di seguito, a seconda del tipo di sistema operativo utilizzato.

Generale

In questa scheda è possibile modificare lo stato del criterio e specificare l'ereditarietà delle impostazioni criterio:

- In **Stato criterio** è possibile selezionare una modalità criterio:
  - **Attivo**

    Se questa opzione è selezionata, il criterio diventa attivo.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Inattivo**

    Se questa opzione è selezionata, il criterio diventa inattivo, ma viene comunque salvato nella cartella **Criteri**. Se necessario, il criterio può essere attivato.

- Nel gruppo di impostazioni **Ereditarietà impostazioni** è possibile configurare l'ereditarietà del criterio:
  - **Eredita impostazioni dal criterio padre**

    Se questa opzione è abilitata, i valori delle impostazioni del criterio vengono ereditati dal criterio di gruppo di livello superiore e pertanto vengono bloccati.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Forza ereditarietà impostazioni nei criteri figlio**

    Se questa opzione è abilitata, una volta applicate le modifiche ai criteri, verranno eseguite le seguenti azioni:

    - I valori delle impostazioni dei criteri saranno propagati ai criteri dei sottogruppi di amministrazione, ovvero ai criteri secondari.
    - Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio secondario, l'opzione **Eredita impostazioni dal criterio principale** sarà abilitata automaticamente.

    Se questa opzione è abilitata, le impostazioni dei criteri secondari vengono bloccate.

    Per impostazione predefinita, questa opzione è disabilitata.

Configurazione eventi

In questa scheda è possibile configurare la registrazione degli eventi e le notifiche degli eventi. Gli eventi vengono distribuiti in base al livello di importanza nelle seguenti sezioni nella scheda **Configurazione eventi**:

- **Errore funzionale**
- **Avviso**
- **Informazioni**

In ogni sezione l'elenco dei tipi di eventi mostra i tipi di eventi e il periodo di archiviazione predefinito per gli eventi in Administration Server (in giorni). Dopo aver fatto clic sul tipo di evento è possibile specificare le impostazioni di registrazione degli eventi e le notifiche sugli eventi selezionati nell'elenco. Per impostazione predefinita, le impostazioni di notifica comuni specificate per l'intero Administration Server vengono utilizzate per tutti i tipi di eventi. Tuttavia, è possibile modificare impostazioni specifiche per i tipi di eventi desiderati.

Ad esempio, nella sezione **Avviso**, è possibile configurare il tipo di evento **Si è verificato un problema di sicurezza**. Tali eventi possono ad esempio verificarsi quando lo spazio libero sul disco di un punto di distribuzione è inferiore a 2 GB (sono necessari almeno 4 GB per installare le applicazioni e scaricare gli aggiornamenti in remoto). Per configurare l'evento **Si è verificato un problema di sicurezza**, fare clic su di esso e specificare la posizione di archiviazione degli eventi che si sono verificati e le modalità di notifica.

Se Network Agent ha rilevato un problema di sicurezza, è possibile gestire tale problema utilizzando le impostazioni di un dispositivo gestito.

Impostazioni applicazione

Impostazioni

Nella sezione **Impostazioni** è possibile configurare il criterio di Network Agent:

- **Distribuisci i file solo tramite punti di distribuzione**

  Se questa opzione è abilitata, i Network Agent nei dispositivi gestiti recuperano gli aggiornamenti solo dai punti di distribuzione.

  Se questa opzione è disabilitata, i Network Agent nei dispositivi gestiti recuperano gli aggiornamenti dai punti di distribuzione o da Administration Server.

  Le applicazioni di protezione nei dispositivi gestiti recuperano gli aggiornamenti dalla sorgente impostata nell'attività di aggiornamento per ciascuna applicazione di protezione. Se si abilita l'opzione **Distribuisci i file solo tramite punti di distribuzione**, assicurarsi che Kaspersky Security Center sia impostato come sorgente degli aggiornamenti nelle attività di aggiornamento.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima della coda di eventi (MB)**

  In questo campo è possibile specificare la quantità massima di spazio su disco che una coda di eventi può occupare.

  Il valore predefinito è 2 megabyte (MB).

- **L'applicazione può recuperare i dati estesi del criterio nel dispositivo**

  Network Agent installato in un dispositivo gestito trasferisce le informazioni sul criterio dell'applicazione di protezione applicato all'applicazione di protezione (ad esempio Kaspersky Endpoint Security for Windows). È possibile visualizzare le informazioni trasferite nell'interfaccia dell'applicazione di protezione.

  Network Agent trasferisce le seguenti informazioni:

  - Ora della distribuzione del criterio al dispositivo gestito.
  - Nome del criterio attivo al momento della distribuzione del criterio al dispositivo gestito.
  - Nome del criterio fuori sede al momento della distribuzione del criterio al dispositivo gestito (non disponibile per Network Agent for Linux).
  - Nome e percorso completo del gruppo di amministrazione che conteneva il dispositivo gestito al momento della distribuzione del criterio al dispositivo gestito.
  - Elenco dei profili di criteri attivi con i relativi nomi e priorità al momento della distribuzione del criterio al dispositivo gestito.

  È possibile utilizzare le informazioni per assicurarsi che venga applicato il criterio corretto al dispositivo e per la risoluzione dei problemi. Per impostazione predefinita, questa opzione è disabilitata.

- **Proteggi il servizio Network Agent dalle operazioni non autorizzate di rimozione o terminazione e impedisci la modifica delle impostazioni**

  Quando questa opzione è abilitata, dopo l'installazione di Network Agent in un dispositivo gestito, il componente non può essere rimosso o riconfigurato senza i privilegi richiesti. Il servizio Network Agent non può essere arrestato. Questa opzione non ha effetto sui controller di dominio.

  Abilitare questa opzione per proteggere Network Agent sulle workstation gestite con diritti di amministratore locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa password di disinstallazione**

  Se questa opzione è abilitata, facendo clic sul pulsante **Modifica** è possibile specificare la password per l'utilità klmover e la disinstallazione remota di Network Agent.

  Per impostazione predefinita, questa opzione è disabilitata.

Archivi

Nella sezione **Archivi** è possibile selezionare i tipi di oggetti i cui dettagli verranno inviati da Network Agent ad Administration Server. Se la modifica di alcune impostazioni in questa sezione non è consentita dal criterio di Network Agent, non è possibile modificare tali impostazioni.

- **Informazioni dettagliate sulle applicazioni installate**

  Se questa opzione è abilitata, le informazioni sulle applicazioni installate nei dispositivi client vengono inviate ad Administration Server.

  Per impostazione predefinita, questa opzione è abilitata.

- **Includi informazioni sulle patch**

  Le informazioni sulle patch delle applicazioni installate nei dispositivi client vengono inviate ad Administration Server. L'abilitazione di questa opzione può aumentare il carico su Administration Server e DBMS, nonché incrementare il volume del database.

  Per impostazione predefinita, questa opzione è abilitata. È disponibile solo per Windows.

- **Informazioni dettagliate sugli aggiornamenti Windows Update**

  Se questa opzione è abilitata, le informazioni sugli aggiornamenti di Microsoft Windows Update da installare nei dispositivi client vengono inviate ad Administration Server.

  A volte, anche se l'opzione è disabilitata, gli aggiornamenti vengono visualizzati nelle proprietà del dispositivo, nella sezione **Aggiornamenti disponibili**. Questo potrebbe ad esempio accadere se i dispositivi dell'organizzazione presentassero vulnerabilità correggibili tramite questi aggiornamenti.

  Per impostazione predefinita, questa opzione è abilitata. È disponibile solo per Windows.

  Le informazioni sugli aggiornamenti facoltativi di Microsoft Windows non vengono inviate ad Administration Server.

- **Dettagli delle vulnerabilità del software e degli aggiornamenti corrispondenti**

  Se questa opzione è abilitata, le informazioni sulle vulnerabilità del software di terze parti (incluso il software Microsoft) rilevate nei dispositivi gestiti e sugli aggiornamenti software per correggere le vulnerabilità di terze parti (escluso il software Microsoft) vengono inviate ad Administration Server.

  Selezionando questa opzione (**Dettagli sulle vulnerabilità del software e sugli aggiornamenti corrispondenti**) aumentano il carico di rete, il carico sul disco di Administration Server e il consumo di risorse di Network Agent.

  Per impostazione predefinita, questa opzione è abilitata. È disponibile solo per Windows.

  Per gestire gli aggiornamenti software del software Microsoft, utilizzare l'opzione **Informazioni dettagliate sugli aggiornamenti Windows Update.**

- **Dettagli registro hardware**

  Network Agent installato in un dispositivo invia informazioni sull'hardware del dispositivo ad Administration Server. È possibile visualizzare i dettagli hardware nelle proprietà del dispositivo.

  Assicurarsi che l'utilità lshw sia installata nei dispositivi Linux da cui si desidera recuperare i dettagli dell'hardware. I dettagli dell'hardware recuperati dalle macchine virtuali potrebbero essere incompleti a seconda dell'hypervisor utilizzato.

Vulnerabilità e aggiornamenti software

Nella sezione **Vulnerabilità e aggiornamenti software** è possibile configurare la ricerca e la distribuzione degli aggiornamenti di Windows, nonché abilitare la scansione dei file eseguibili per rilevare la presenza di vulnerabilità:

- **Usa Administration Server come server WSUS**

  Se questa opzione è abilitata, gli aggiornamenti di Windows vengono scaricati in Administration Server. Administration Server fornisce gli aggiornamenti scaricati a Windows Update nei dispositivi client in modalità centralizzata tramite Network Agent.

  Se questa opzione è disabilitata, Administration Server non viene utilizzato per scaricare gli aggiornamenti di Windows. In questo caso, i dispositivi client ricevono autonomamente gli aggiornamenti di Windows.

  Per impostazione predefinita, questa opzione è disabilitata.

- È possibile limitare gli aggiornamenti Windows che gli utenti possono installare manualmente nei propri dispositivi tramite Windows Update.

  Nei dispositivi che eseguono Windows 10, se Windows Update ha già rilevato aggiornamenti per il dispositivo, la nuova opzione selezionata in **Consentire agli utenti di gestire l'installazione degli aggiornamenti Windows Update** verrà applicata solo dopo l'installazione degli aggiornamenti rilevati.

  Selezionare un elemento nell'elenco a discesa:

  - **Consentire agli utenti di installare tutti gli aggiornamenti Windows Update applicabili**

    Gli utenti possono installare nei propri dispositivi tutti gli aggiornamenti di Microsoft Windows Update applicabili.

    Selezionare questa opzione se non si desidera interferire nell'installazione degli aggiornamenti.

    Quando l'utente installa manualmente gli aggiornamenti di Microsoft Windows Update, gli aggiornamenti possono essere scaricati dai server Microsoft anziché da Administration Server. Questo è possibile se Administration Server non ha ancora scaricato gli aggiornamenti. Il download degli aggiornamenti dai server Microsoft comporta un traffico aggiuntivo.

  - **Consentire agli utenti di installare solo gli aggiornamenti Windows Update approvati**

    Gli utenti possono installare nei propri dispositivi tutti gli aggiornamenti di Microsoft Windows Update applicabili e approvati dall'amministratore.

    Ad esempio, potrebbe essere utile controllare prima l'installazione degli aggiornamenti in un ambiente di test e verificare che non interferiscano con l'utilizzo dei dispositivi e solo successivamente consentire l'installazione degli aggiornamenti approvati nei dispositivi client.

    Quando l'utente installa manualmente gli aggiornamenti di Microsoft Windows Update, gli aggiornamenti possono essere scaricati dai server Microsoft anziché da Administration Server. Questo è possibile se Administration Server non ha ancora scaricato gli aggiornamenti. Il download degli aggiornamenti dai server Microsoft comporta un traffico aggiuntivo.

- **Non consentire agli utenti di installare gli aggiornamenti Windows Update**

  Gli utenti non possono installare manualmente gli aggiornamenti di Microsoft Windows Update nei propri dispositivi. Tutti gli aggiornamenti applicabili vengono installati in base alla configurazione specificata dall'amministratore.

  Selezionare questa opzione se si desidera gestire l'installazione degli aggiornamenti in modo centralizzato.

  È ad esempio possibile ottimizzare la pianificazione degli aggiornamenti in modo da evitare di sovraccaricare la rete. È possibile pianificare le installazioni degli aggiornamenti in orario non lavorativo, in modo che non interferiscano con la produttività degli utenti.

- Nel gruppo di impostazioni **Modalità di ricerca di Windows Update** è possibile selezionare la modalità di ricerca degli aggiornamenti:

  - **Attiva**

    Se questa opzione è selezionata, Administration Server con il supporto di Network Agent avvia una richiesta da un Windows Update Agent nel dispositivo client alla sorgente degli aggiornamenti: server Windows Update o WSUS. Successivamente, Network Agent trasmette le informazioni ricevute da Windows Update Agent ad Administration Server.

    L'opzione è valida solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** dell'attività *Trova vulnerabilità e aggiornamenti richiesti* è selezionata.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Passiva**

    Se questa opzione è selezionata, Network Agent trasmette periodicamente ad Administration Server le informazioni sugli aggiornamenti recuperati durante l'ultima sincronizzazione di Windows Update Agent con la sorgente degli aggiornamenti. Se non viene eseguita la sincronizzazione di Windows Update Agent con una sorgente degli aggiornamenti, le informazioni sugli aggiornamenti in Administration Server diventano obsolete.

    Selezionare questa opzione se si desidera ottenere gli aggiornamenti dalla cache della memoria della sorgente degli aggiornamenti.

  - **Disabilitata**

    Se questa opzione è selezionata, Administration Server non richiede informazioni sugli aggiornamenti.

    Selezionare questa opzione se, ad esempio, si desidera prima testare gli aggiornamenti nel dispositivo locale.

- **Esegui la scansione dei file eseguibili per rilevarne le vulnerabilità al momento dell'esecuzione**

  Se questa opzione è abilitata, i file eseguibili vengono esaminati alla ricerca di vulnerabilità al momento dell'esecuzione.

  Per impostazione predefinita, questa opzione è abilitata.

Gestione riavvio

Nella sezione **Gestione riavvio** è possibile specificare l'azione che deve essere eseguita se il sistema operativo di un dispositivo gestito deve essere riavviato per utilizzare, installare o disinstallare correttamente un'applicazione:

- **Non riavviare il sistema operativo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia automaticamente il sistema operativo se necessario**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Forza riavvio dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  - **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

Condivisione desktop Windows

Nella sezione **Condivisione desktop Windows** è possibile abilitare e configurare il controllo delle azioni eseguite dall'amministratore in un dispositivo remoto quando viene condiviso l'accesso al desktop:

- **Abilita controllo**

  Se questa opzione è abilitata, il controllo delle azioni dell'amministratore nel dispositivo remoto è abilitato. I record relativi alle azioni dell'amministratore nel dispositivo remoto vengono registrati:

  - Nel registro eventi del dispositivo remoto
  - In un file con estensione syslog nella cartella di installazione di Network Agent nel dispositivo remoto
  - Nel database degli eventi di Kaspersky Security Center

  Il controllo delle azioni dell'amministratore è disponibile quando sono soddisfatte le seguenti condizioni:

  - È in uso la licenza per Vulnerability e patch management
  - L'amministratore dispone del diritto per l'avvio dell'accesso condiviso al desktop del dispositivo remoto

  Se questa opzione è disabilitata, il controllo delle azioni dell'amministratore nel dispositivo remoto è disabilitato.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Maschere dei file da monitorare durante la lettura**

  L'elenco contiene le maschere dei file. Quando il controllo è abilitato, l'applicazione monitora i file di lettura dell'amministratore corrispondenti alle maschere e salva le informazioni sui file letti. L'elenco è disponibile se la casella di controllo **Abilita controllo** è selezionata. È possibile modificare le maschere dei file e aggiungerne di nuove all'elenco. Ogni nuova maschera di file deve essere specificata nell'elenco su una nuova riga.

  Per impostazione predefinita, sono specificate le seguenti maschere dei file: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Maschere dei file da monitorare durante la modifica**

  L'elenco contiene maschere dei file nel dispositivo remoto. Quando il controllo è abilitato, l'applicazione monitora le modifiche apportate dall'amministratore ai file corrispondenti alle maschere e salva le informazioni su tali modifiche. L'elenco è disponibile se la casella di controllo **Abilita controllo** è selezionata. È possibile modificare le maschere dei file e aggiungerne di nuove all'elenco. Ogni nuova maschera di file deve essere specificata nell'elenco su una nuova riga.

  Per impostazione predefinita, sono specificate le seguenti maschere dei file: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Gestire patch e aggiornamenti

Nella sezione **Gestire patch e aggiornamenti** è possibile configurare il download e la distribuzione degli aggiornamenti, nonché l'installazione delle patch nei dispositivi gestiti:

- **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito**

  Se questa opzione è abilitata, le patch di Kaspersky con lo stato di approvazione *Indefinito* vengono installate automaticamente nei dispositivi gestiti subito dopo il download dai server di aggiornamento.

  Se questa opzione è disabilitata, le patch di Kaspersky che sono state scaricate e contrassegnate con lo stato *Indefinito* saranno installate solo dopo che si modifica il relativo stato in *Approvato*.

  Per impostazione predefinita, questa opzione è abilitata.

- **Scarica aggiornamenti e database anti-virus da Administration Server anticipatamente (scelta consigliata)**

  Se questa opzione è abilitata, viene utilizzato il modello offline di download degli aggiornamenti. Quando Administration Server riceve gli aggiornamenti, segnala a Network Agent (nei dispositivi in cui è installato) gli aggiornamenti che saranno necessari per le applicazioni gestite. Quando Network Agent riceve le informazioni su questi aggiornamenti, scarica anticipatamente i file appropriati da Administration Server. Alla prima connessione con Network Agent, Administration Server avvia un download degli aggiornamenti. Una volta che Network Agent ha scaricato tutti gli aggiornamenti in un dispositivo client, tali aggiornamenti diventano disponibili per le applicazioni nel dispositivo.

  Quando un'applicazione gestita in un dispositivo client tenta di accedere a Network Agent per gli aggiornamenti, questo Network Agent verifica se dispone di tutti gli aggiornamenti richiesti. Se gli aggiornamenti sono stati ricevuti da Administration Server non più di 25 ore prima del momento in cui vengono richiesti dall'applicazione gestita, il Network Agent non si connette ad Administration Server, ma fornisce all'applicazione gestita gli aggiornamenti dalla cache locale. La connessione con Administration Server potrebbe non essere stabilita quando Network Agent fornisce gli aggiornamenti alle applicazioni nei dispositivi client, ma la connessione non è necessaria per l'aggiornamento.

  Se questa opzione è disabilitata, non viene utilizzato il modello offline di download degli aggiornamenti. Gli aggiornamenti vengono distribuiti in base alla pianificazione dell'attività di download degli aggiornamenti.

  Per impostazione predefinita, questa opzione è abilitata.

Connettività

La sezione **Connettività** include tre sottosezioni:

- **Rete**
- **Profili connessione**
- **Pianificazione connessione**

Nella sottosezione **Rete**, è possibile configurare la connessione ad Administration Server, abilitare l'utilizzo di una porta UDP e specificare il numero della porta UDP.

- Nel gruppo di impostazioni **Connetti ad Administration Server** è possibile configurare la connessione ad Administration Server e specificare l'intervallo di tempo per la sincronizzazione tra i dispositivi client e Administration Server:

  - **Intervallo di sincronizzazione (min.)**

    Network Agent sincronizza il dispositivo gestito con Administration Server. È consigliabile impostare l'intervallo di sincronizzazione (anche denominato heartbeat) su 15 minuti per 10.000 dispositivi gestiti.

    Se l'intervallo di sincronizzazione è impostato su meno di 15 minuti, la sincronizzazione viene eseguita ogni 15 minuti. Se l'intervallo di sincronizzazione è impostato su 15 minuti o più, la sincronizzazione viene eseguita all'intervallo di sincronizzazione specificato.

  - **Comprimi traffico di rete**

    Se questa opzione è abilitata, la velocità di trasferimento dei dati da parte di Network Agent viene aumentata attraverso una riduzione della quantità di informazioni da trasferire e una conseguente riduzione del carico di Administration Server.

    Il carico di lavoro sulla CPU del computer client potrebbe aumentare.

    Per impostazione predefinita, questa casella di controllo è abilitata.

  - **Apri porte di Network Agent in Microsoft Windows Firewall**

    Se questa opzione è abilitata, le porte, necessarie per l'utilizzo di Network Agent e Administration Server vengono aggiunte all'elenco di esclusioni di Microsoft Windows Firewall.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Usa connessione SSL**

    Se questa opzione è abilitata, la connessione ad Administration Server viene stabilita attraverso una porta sicura tramite SSL.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Usa il gateway di connessione in un punto di distribuzione (se disponibile) con le impostazioni di connessione predefinite**

    Se questa opzione è abilitata, viene utilizzato il gateway di connessione nel punto di distribuzione con le impostazioni specificate nelle proprietà del gruppo di amministrazione.

    Per impostazione predefinita, questa opzione è abilitata.

- **Usa porta UDP**

Se è necessario che Network Agent si connetta ad Administration server attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in **Porta UDP**. Per impostazione predefinita, questa opzione è abilitata. La porta UDP predefinita per la connessione ad Administration Server è 15000.

- **Numero di porta UDP**

  In questo campo è possibile immettere il numero della porta UDP. Il numero di porta predefinito è 15000.

  Viene utilizzato il sistema decimale per i record.

  Se il dispositivo client esegue Windows XP Service Pack 2, il firewall integrato blocca la porta UDP 15000. Si consiglia di aprire questa porta manualmente.

- **Usa punto di distribuzione per forzare una connessione ad Administration Server**

  Selezionare questa opzione se è stata selezionata l'opzione **Usa questo punto di distribuzione come server push** nella finestra delle impostazioni del punto di distribuzione. In caso contrario, il punto di distribuzione non fungerà da server push.

Nella sottosezione **Profili connessione**, è possibile specificare le impostazioni del percorso di rete e abilitare la modalità fuori sede quando Administration Server non è disponibile:

- **Impostazioni percorso di rete**

  Le impostazioni del percorso di rete definiscono le caratteristiche della rete alla quale è connesso il dispositivo client e specificano le regole per il passaggio di Network Agent da un profilo di connessione Administration Server all'altro quando tali caratteristiche di rete subiscono variazioni.

- **Profili connessione di Administration Server**

  In questa sezione è possibile visualizzare e aggiungere profili per la connessione di Network Agent ad Administration Server. In questa sezione è inoltre possibile creare regole per il passaggio di Network Agent a diversi Administration Server quando si verificano i seguenti eventi:

  - Quando il dispositivo client si connette a un'altra rete locale
  - Quando il dispositivo perde la connessione con la rete locale dell'organizzazione
  - Quando cambia l'indirizzo del gateway di connessione o l'indirizzo del server DNS viene modificato

  I profili di connessione sono supportati solo per i dispositivi che eseguono Windows e macOS.

- **Abilita la modalità fuori sede quando Administration Server non è disponibile**

  Se questa opzione è abilitata, in caso di utilizzo di questo profilo per la connessione, le applicazioni installate nel dispositivo client utilizzeranno i profili criterio per i dispositivi in modalità fuori sede, nonché i criteri fuori sede. Se non è definito alcun criterio fuori sede per l'applicazione, verrà utilizzato il criterio attivo.

  Se questa opzione è disabilitata, le applicazioni utilizzeranno i criteri attivi.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Pianificazione connessione** è possibile specificare gli intervalli di tempo durante i quali Network Agent invia i dati ad Administration Server:

- **Connetti quando necessario**

  Se questa opzione è selezionata, la connessione viene stabilita quando Network Agent deve inviare i dati ad Administration Server.

  Per impostazione predefinita, questa opzione è selezionata.

- **Connetti negli intervalli di tempo specificati**

  Se questa opzione è selezionata, Network Agent si connette ad Administration Server all'ora specificata. È possibile aggiungere diversi periodi di tempo per la connessione.

Polling di rete per punti di distribuzione

Nella sezione **Polling di rete per punti di distribuzione** è possibile configurare il polling automatico della rete. È possibile utilizzare le seguenti opzioni per abilitare il polling e impostarne la frequenza:

- **Rete Windows**

  Se l'opzione è abilitata, Administration Server esegue automaticamente il polling della rete in base alla pianificazione configurata facendo clic sui collegamenti **Imposta pianificazione di polling rapido** e **Imposta pianificazione di polling completo**.

  Se questa opzione è disabilitata, Administration Server esegue il polling della rete con l'intervallo specificato nel campo **Frequenza di polling della rete (min.)**.

  L'intervallo di device discovery per le versioni di Network Agent precedenti alla 10.2 può essere configurato nei campi **Frequenza dei polling dai domini Windows (min.)** (per il polling di rete Windows rapido) e **Frequenza di polling della rete (min.)** (per il polling di rete Windows completo).

  Per impostazione predefinita, questa opzione è disabilitata.

- **Zeroconf**

  Se questa opzione è abilitata, il punto di distribuzione esegue automaticamente il polling della rete con i dispositivi IPv6 utilizzando le reti zero-configuration (definite anche *Zeroconf*). In questo caso, il polling dell'intervallo IP abilitati viene ignorato, poiché il punto di distribuzione esegue il polling dell'intera rete.

  Per iniziare a utilizzare Zeroconf è necessario soddisfare le seguenti condizioni:

  - Il punto di distribuzione deve eseguire Linux.
  - È necessario installare l'utilità avahi-browse nel punto di distribuzione.

  Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling delle reti con i dispositivi IPv6.

  Per impostazione predefinita, questa opzione è disabilitata.

- Intervalli IP

  Se l'opzione è abilitata, il punto di distribuzione esegue automaticamente il polling dell'intervallo IP in base alla pianificazione configurata facendo clic sul pulsante **Imposta pianificazione di polling**.

  Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling degli intervalli IP.

  La frequenza di polling dell'intervallo IP per le versioni di Network Agent precedenti alla 10.2 può essere configurata nel campo **Intervallo di polling (min.)**. Il campo è disponibile se l'opzione è abilitata.

  Per impostazione predefinita, questa opzione è disabilitata.

- Controller di dominio

  Se l'opzione è abilitata, il punto di distribuzione esegue automaticamente il polling di Active Directory in base alla pianificazione configurata facendo clic sul collegamento **Imposta pianificazione di polling**.

  Se questa opzione è disabilitata, Administration Server non esegue il polling di Active Directory.

  La frequenza di polling di Active Directory per le versioni di Network Agent precedenti alla 10.2 può essere configurata nel campo **Intervallo di polling (min.)**. Il campo è disponibile se questa opzione è abilitata.

  Per impostazione predefinita, questa opzione è disabilitata.

  Se l'opzione è abilitata, il punto di distribuzione esegue automaticamente il polling dei controller di dominio in base alla pianificazione configurata facendo clic sul pulsante **Imposta pianificazione di polling**.

  Se questa opzione è disabilitata, il punto di distribuzione non esegue il polling dei controller di dominio.

  La frequenza di polling dei controller di dominio per le versioni di Network Agent precedenti alla 10.2 può essere configurata nel campo **Intervallo di polling (min.)**. Il campo è disponibile se questa opzione è abilitata.

  Per impostazione predefinita, questa opzione è disabilitata.

Impostazioni di rete per punti di distribuzione

Se i punti di distribuzione utilizzano un server proxy durante la connessione a Internet, nella sezione **Impostazioni di rete per punti di distribuzione** è possibile specificare le seguenti impostazioni:

- **Usa server proxy**
- **Indirizzo**
- **Numero di porta**
- Ignora il server proxy per gli indirizzi locali

  Se questa opzione è abilitata, non viene utilizzato alcun server proxy per la connessione ai dispositivi nella rete locale.

  Per impostazione predefinita, questa opzione è disabilitata.

- Autenticazione server proxy

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Nome utente**
- **Password**

Proxy KSN (punti di distribuzione)

Nella sezione **Proxy KSN (punti di distribuzione)** è possibile configurare l'applicazione per l'utilizzo del punto di distribuzione per l'inoltro delle richieste di Kaspersky Security Network (KSN) dai dispositivi gestiti:

- Abilita proxy KSN da parte del punto di distribuzione

  Il servizio proxy KSN viene eseguito nel dispositivo utilizzato come punto di distribuzione. Utilizzare questa funzionalità per ridistribuire e ottimizzare il traffico nella rete.

  Il punto di distribuzione invia le statistiche KSN, elencate nell'informativa di Kaspersky Security Network, a Kaspersky. Per impostazione predefinita, l'informativa KSN è disponibile in %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Per impostazione predefinita, questa opzione è disabilitata. L'attivazione di questa opzione ha effetto solo se le opzioni **Usa Administration Server come server proxy** e **Accetto di utilizzare Kaspersky Security Network** sono abilitate nella finestra delle proprietà di Administration Server.

  È possibile assegnare il nodo di un cluster attivo-passivo a un punto di distribuzione e abilitare il proxy KSN in tale nodo.

- Inoltra richieste KSN ad Administration Server

  Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti ad Administration Server.

  Per impostazione predefinita, questa opzione è abilitata.

- Accedi a KSN Cloud/KPSN direttamente tramite Internet

  Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti a KSN Cloud o KPSN. Anche le richieste KSN generate nello stesso punto di distribuzione vengono inviate direttamente a KSN Cloud o KPSN.

  I punti di distribuzione in cui è installato Network Agent versione 11 (o precedente) non possono accedere direttamente a KPSN. Se si desidera riconfigurare i punti di distribuzione per inviare richieste KSN a KPSN, abilitare l'opzione **Inoltra richieste KSN ad Administration Server** per ciascun punto di distribuzione.

  I punti di distribuzione in cui è installato Network Agent versione 12 (o successive) possono accedere direttamente a KPSN.

- **Porta**

  Numero della porta TCP utilizzata dai dispositivi gestiti per la connessione al server proxy KSN. Il numero di porta predefinito è 13111.

- **Porta UDP**

  Se è necessario che Network Agent si connetta ad Administration server attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in **Porta UDP**. Per impostazione predefinita, questa opzione è abilitata. La porta UDP predefinita per la connessione ad Administration Server è 15000.

Aggiornamenti (punti di distribuzione)

Nella sezione **Aggiornamenti (punti di distribuzione)** è possibile abilitare la funzionalità per il download dei file diff, in modo che i punti di distribuzione acquisiscano gli aggiornamenti sotto forma di file diff dai server degli aggiornamenti Kaspersky.

Gestione account locali (solo Linux)

La sezione **Gestione account locali (solo Linux)** include tre sottosezioni:

- **Gestione dei certificati utente**
- **Aggiungi o modifica i gruppi di amministratori locali applicabili**
- **Carica un file di riferimento per proteggere il file sudoers sul dispositivo dell'utente dalle modifiche**

Nella sottosezione **Gestione dei certificati utente** è possibile specificare quali certificati radice installare. Questi certificati possono essere utilizzati, ad esempio, per verificare l'autenticità di siti Web o server Web.

- **Installa certificati radice**

  Se questa opzione è abilitata, i certificati aggiunti alla tabella verranno installati nei dispositivi specificati.

  Se questa opzione è disabilitata, nessun certificato verrà installato nei dispositivi specificati.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Aggiungi**

  Facendo clic su questo pulsante viene aperta una finestra in cui è possibile aggiungere un certificato.

  Il certificato deve essere inferiore a 10 MB.

  Kaspersky Security Center supporta i certificati con estensioni CER, CRT, CERT, PEM e KEY.

Nella sottosezione **Aggiungi o modifica i gruppi di amministratori locali applicabili**, è possibile gestire i gruppi di amministratori locali. Questi gruppi vengono utilizzati, ad esempio, quando si revocano i diritti di amministratore locale. È inoltre possibile controllare l'elenco degli account utente privilegiati utilizzando il **Rapporto sugli utenti dei dispositivi (solo Linux)**.

- **Aggiungi**

  Questo pulsante consente di aprire una finestra in cui è possibile aggiungere un gruppo di amministratori locali.

- **Modifica**

  Questo pulsante consente di aprire una finestra in cui è possibile modificare il gruppo di amministratori locali.

  Questo pulsante è disponibile se la casella di controllo accanto al gruppo di amministratori locali è selezionata.

- **Elimina**

  Questo pulsante consente di eliminare dalla tabella il gruppo di amministratori locali selezionato.

  Questo pulsante è disponibile se la casella di controllo accanto al gruppo di amministratori locali è selezionata.

Nella sottosezione **Carica un file di riferimento per proteggere il file sudoers sul dispositivo dell'utente dalle modifiche**, è possibile configurare il controllo del file sudoers. I gruppi privilegiati e gli utenti del dispositivo sono definiti dal file sudoers nel dispositivo. Il file sudoers si trova in `/etc/sudoers`. È possibile caricare un file sudoers di riferimento per proteggere il file sudoers dalle modifiche. Questo impedirà modifiche indesiderate al file sudoers.

Un file sudoers di riferimento non valido può causare il malfunzionamento del dispositivo dell'utente.

- **File sudoers di controllo**

  Se questa opzione è abilitata, il file sudoers verrà sostituito dal file sudoers di riferimento corrente.

  Se questa opzione è disabilitata, il file sudoers rimarrà invariato.

  Per impostazione predefinita, questa opzione è disabilitata.

- **File sudoers di riferimento**

  Questo campo visualizza il nome del file sudoers di riferimento caricato.

- **Carica**

  Questo pulsante consente di aprire una finestra in cui è possibile caricare un file sudoers di riferimento.

- **File sudoers di riferimento corrente**

  Questo pulsante consente di visualizzare il contenuto del file sudoers corrente.

Cronologia revisioni

In questa scheda è possibile visualizzare l'elenco delle revisioni del criterio ed eseguire il rollback delle modifiche apportate al criterio, se necessario.

Confronto tra le impostazioni dei criteri di Network Agent in base ai sistemi operativi

La seguente tabella mostra quali impostazioni dei criteri di Network Agent è possibile utilizzare in Administration Console e Kaspersky Security Center Web Console per configurare Network Agent con un sistema operativo specifico.

Impostazioni dei criteri di Network Agent: confronto in base ai sistemi operativi

Sezione Criterio	Windows	macOS	Linux
Generale	✓	✓	✓
Configurazione eventi	✓	✓	✓
Impostazioni	✓	✓	✓ Sono disponibili le seguenti opzioni: • **Distribuisci i file solo tramite punti di distribuzione** • **Dimensione massima della coda di eventi (MB)** • **L'applicazione può recuperare i dati estesi del criterio nel dispositivo**
Archivi	✓	✓ L'opzione **Dettagli registro hardware** è disponibile.	✓ Sono disponibili le seguenti opzioni: • **Informazioni dettagliate sulle applicazioni installate** • **Dettagli registro hardware**
Vulnerabilità e aggiornamenti software	✓	—	—
Gestione riavvio	✓	—	—
Condivisione desktop Windows	✓	—	—
Gestire patch e aggiornamenti	✓	—	—
Connettività → Rete	✓	✓	✓ Ad eccezione dell'opzione **Apri porte di Network Agent in Microsoft Windows Firewall**.
Connettività → Profili connessione	✓	✓	—

Sezione Criterio	Windows	macOS	Linux
Connettività → Pianificazione connessione	✓	✓	✓
Polling di rete per punti di distribuzione	✓ Sono disponibili solo le opzioni **Rete Windows**, **Intervalli IP** e **Controller di dominio**.	—	✓ Sono disponibili le seguenti opzioni: • **Zeroconf** • **Intervalli IP** • **Controller di dominio**
Impostazioni di rete per punti di distribuzione	✓	✓	✓
Proxy KSN (punti di distribuzione)	✓	—	✓
Aggiornamenti (punti di distribuzione)	✓	—	✓
Cronologia revisioni	✓	✓	✓

Abilitazione e disabilitazione della modalità a basso consumo di risorse per Network Agent

La modalità a basso consumo di risorse consente di limitare l'utilizzo della RAM del Network Agent installato nel dispositivo client. Per impostazione predefinita, la modalità a basso consumo di risorse è disabilitata.

Nella modalità a basso consumo di risorse, le seguenti funzioni non vengono eseguite:

- Network Agent non può essere assegnato come punto di distribuzione (manualmente o automaticamente).
- Network Agent non registra le informazioni sullo stato di Network Agent in un file di testo separato.
- Network Agent non supporta il modello offline di download degli aggiornamenti.
- I seguenti componenti e processi sono disabilitati:
  - Ottenere informazioni su aggiornamenti e vulnerabilità di terze parti.
  - Esecuzione del proxy KSN sul lato del punto di distribuzione.
  - Caricamento degli aggiornamenti nell'archivio del punto di distribuzione.
  - Ignorare il blocco del server DNS.
  - Recupero di informazioni sullo spazio libero su disco.

I componenti e i processi riprendono il funzionamento dopo aver disabilitato la modalità a basso consumo di risorse.

Per abilitare la modalità a basso consumo di risorse:

1. Eseguire il seguente comando nella riga di comando nel dispositivo client:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 1
   ```

2. Riavviare il Network Agent.

3. Per verificare che la modalità a basso consumo di risorse sia abilitata, in Windows aprire **Visualizzatore eventi**, quindi selezionare **Registri applicazioni e servizi → Registro eventi Kaspersky**.

   Verificare che il registro contenga eventi come **Kaspersky Security Center Network Agent funziona in modalità a basso consumo di risorse**.

La modalità a basso consumo di risorse è abilitata.

Per disabilitare la modalità a basso consumo di risorse:

1. Eseguire il seguente comando nella riga di comando nel dispositivo client:

   ```
   C:\Program files (x86)\Kaspersky Lab\NetworkAgent>klscflag -fset -pv klnagent -n
   KLNAG_FLAG_TEST_VM_PERF -t d -v 0
   ```

2. Riavviare il Network Agent.

3. Per verificare che la modalità a basso consumo di risorse sia disabilitata, in Windows aprire **Visualizzatore eventi**, quindi selezionare **Registri applicazioni e servizi → Registro eventi Kaspersky**.

   Verificare che l'ultimo evento klnagent non contenga il messaggio **Kaspersky Security Center Network Agent funziona in modalità a basso consumo di risorse**.

La modalità a basso consumo di risorse è disabilitata.

È inoltre possibile abilitare la modalità a basso consumo di risorse in remoto utilizzando un'attività *Esegui script da remoto*.

Configurazione manuale del criterio di Kaspersky Endpoint Security

Questa sezione offre suggerimenti per la configurazione del criterio di Kaspersky Endpoint Security. È possibile eseguire la configurazione nella finestra delle proprietà del criterio. Quando si modifica un'impostazione, fare clic sull'icona del lucchetto a destra del gruppo di impostazioni pertinente per applicare i valori specificati a una workstation.

Configurazione di Kaspersky Security Network

Kaspersky Security Network (KSN) è l'infrastruttura dei servizi cloud che contiene informazioni sulla reputazione di file, risorse Web e software. Kaspersky Security Network consente a Kaspersky Endpoint Security for Windows di rispondere più rapidamente a diversi tipi di minacce, migliora le prestazioni dei componenti della protezione e riduce la probabilità di falsi positivi. Per ulteriori informazioni su Kaspersky Security Network, vedere la Guida di Kaspersky Endpoint Security for Windows.

Per specificare le impostazioni consigliate di KSN:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio passare a **Impostazioni applicazione** → **Protezione minacce avanzata** → **Kaspersky Security Network**.
4. Verificare che l'opzione **Kaspersky Security Network** sia abilitata. L'utilizzo di questa opzione consente di ridistribuire e ottimizzare il traffico nella rete.

   Se si utilizza Managed Detection and Response, è necessario abilitare l'opzione **Kaspersky Security Network** per il punto di distribuzione e abilitare la modalità KSN estesa.
5. Abilitare l'utilizzo dei server KSN se il servizio proxy KSN non è disponibile. I server KSN possono essere posizionati sul lato di Kaspersky (quando si utilizza KSN) o sul lato di terzi (quando si utilizza KPSN).
6. Fare clic su **OK**.

Sono state specificate le impostazioni consigliate di KSN.

Controllo dell'elenco delle reti protette dal Firewall

Verificare che il Firewall Kaspersky Endpoint Security for Windows protegga tutte le reti. Per impostazione predefinita il Firewall protegge le reti con i seguenti tipi di connessione:

- **Rete pubblica**. Le applicazioni di protezione, i firewall o i filtri non proteggono i dispositivi in una rete di questo tipo.
- **Rete locale**. L'accesso a file e stampanti è limitato per i dispositivi in questa rete.
- **Rete attendibile**. I dispositivi in tale rete sono protetti da attacchi e accessi non autorizzati a file e dati.

Se è stata configurata una rete personalizzata, assicurarsi che il Firewall la protegga. A tale scopo, controllare l'elenco delle reti nelle proprietà dei criteri di Kaspersky Endpoint Security for Windows. L'elenco potrebbe non contenere tutte le reti.

Per ulteriori informazioni sul Firewall vedere la Guida di Kaspersky Endpoint Security for Windows.

Per controllare l'elenco delle reti:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio passare a **Impostazioni applicazione** → **Protezione minacce essenziale** → **Firewall**.

4. In **Reti disponibili**, fare clic sul collegamento **Impostazioni di rete**.

   Verrà aperta la finestra **Connessioni di rete**. Questa finestra mostra l'elenco delle reti.

5. Se nell'elenco non è presente una rete, aggiungerla.

Disabilitazione della scansione delle unità di rete

Quando Kaspersky Endpoint Security for Windows esegue la scansione delle unità di rete, ciò può comportare un carico significativo su queste. È più pratico eseguire la scansione indiretta sui file server.

È possibile disabilitare la scansione delle unità di rete nelle proprietà dei criteri di Kaspersky Endpoint Security for Windows. Per una descrizione delle proprietà di questi criteri, consultare la Guida di Kaspersky Endpoint Security for Windows.

Per disabilitare la scansione delle unità di rete:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio, passare a **Impostazioni applicazione** → **Protezione minacce essenziale** → **Protezione minacce file**.
4. In **Ambito della protezione**, disabilitare l'opzione **Tutte le unità di rete**.
5. Fare clic su **OK**.

La scansione delle unità di rete è disabilitata.

Esclusione dei dettagli del software dalla memoria di Administration Server

È consigliabile evitare che Administration Server salvi le informazioni sui moduli software avviati nei dispositivi di rete. Di conseguenza, la memoria di Administration Server non viene sovraccaricata.

È possibile disabilitare il salvataggio di queste informazioni nelle proprietà dei criteri di Kaspersky Endpoint Security for Windows.

Per disabilitare il salvataggio delle informazioni sui moduli software installati:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.

3. Nelle proprietà del criterio passare a **Impostazioni applicazione** → **Impostazioni generali** → **Rapporti e archivi**.

4. In **Trasferimento dei dati ad Administration Server** disabilitare la casella di controllo **Informazioni sulle applicazioni avviate** se è ancora abilitata nel criterio di primo livello.

   Quando questa casella di controllo è selezionata, il database di Administration Server salva informazioni su tutte le versioni di tutti i moduli software nei dispositivi connessi alla rete. Queste informazioni possono richiedere una quantità significativa di spazio su disco nel database di Kaspersky Security Center (decine di gigabyte).

Le informazioni sui moduli software installati non vengono più salvate nel database di Administration Server.

Configurazione dell'accesso all'interfaccia di Kaspersky Endpoint Security for Windows nelle workstation

Se la protezione dalle minacce nella rete dell'organizzazione deve essere gestita in modalità centralizzata tramite Kaspersky Security Center, specificare le impostazioni dell'interfaccia nelle proprietà del criterio di Kaspersky Endpoint Security for Windows, come descritto di seguito. In questo modo, si impedirà l'accesso non autorizzato a Kaspersky Endpoint Security for Windows sulle workstation e la modifica delle impostazioni di Kaspersky Endpoint Security for Windows.

Per una descrizione delle proprietà di questi criteri, consultare la Guida di Kaspersky Endpoint Security for Windows.

Per specificare le impostazioni dell'interfaccia consigliate:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.

3. Nelle proprietà del criterio, passare a **Impostazioni applicazione** → **Impostazioni generali** → **Interfaccia**.

4. In **Interazione con l'utente**, selezionare l'opzione **Non visualizzare l'interfaccia utente**. In questo modo, si disabilita la visualizzazione dell'interfaccia utente di Kaspersky Endpoint Security for Windows sulle workstation, quindi i relativi utenti non possono modificare le impostazioni di Kaspersky Endpoint Security for Windows.

5. In **Protezione tramite password**, abilitare l'interruttore. Questo riduce il rischio di modifiche non autorizzate o accidentali nelle impostazioni di Kaspersky Endpoint Security for Windows nelle workstation.

Sono state specificate le impostazioni consigliate per l'interfaccia di Kaspersky Endpoint Security for Windows.

Salvataggio degli eventi di criteri importanti nel database dell'Administration Server

Per evitare l'overflow del database di Administration Server, è consigliabile salvare solo gli eventi importanti nel database.

Per configurare la registrazione degli eventi importanti nel database di Administration Server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Kaspersky Endpoint Security for Windows.

   Verrà visualizzata la finestra delle proprietà del criterio selezionato.
3. Nelle proprietà del criterio aprire la scheda **Configurazione eventi**.
4. Nella sezione **Critico** fare clic su **Aggiungi evento** e selezionare solo le caselle di controllo accanto ai seguenti eventi:
   - *Contratto di licenza con l'utente finale violato*
   - *L'esecuzione automatica dell'applicazione è disabilitata*
   - *Errore di attivazione*
   - *È stata rilevata una minaccia attiva. Si consiglia di avviare Disinfezione avanzata*
   - *Disinfezione impossibile*
   - *Rilevato collegamento pericoloso aperto in precedenza*
   - *Processo terminato*
   - *Attività di rete bloccata*
   - *Attacco di rete rilevato*
   - *Avvio dell'applicazione non consentito*
   - *Accesso negato (database locali)*
   - *Accesso negato (KSN)*
   - *Errore di aggiornamento locale*
   - *Impossibile avviare due attività contemporaneamente*
   - *Errore durante l'interazione con Kaspersky Security Center*
   - *Non tutti i componenti sono stati aggiornati*
   - *Errore durante l'applicazione delle regole di criptaggio/decriptaggio dei file*
   - *Errore durante l'abilitazione della modalità portatile*
   - *Errore durante la disabilitazione della modalità portatile*
   - *Impossibile caricare il modulo di criptaggio*
   - *Il criterio non può essere applicato*
   - *Errore durante la modifica dei componenti dell'applicazione*

5. Fare clic su **OK**.

6. Nella sezione **Errore funzionale**, fare clic su **Aggiungi evento** e selezionare solo la casella di controllo accanto all'evento *Impostazioni delle attività non valide. Impostazioni non applicate*.

7. Fare clic su **OK**.

8. Nella sezione **Avviso** fare clic su **Aggiungi evento** e selezionare solo le caselle di controllo accanto ai seguenti eventi:

   - *L'Auto-difesa è disabilitata*
   - *I componenti della protezione sono disabilitati*
   - *Chiave di riserva errata*
   - *È stato rilevato software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali (basi locali)*
   - *È stato rilevato software legittimo utilizzabile da intrusi per danneggiare il computer o i dati personali (KSN)*
   - *Oggetto eliminato*
   - *Oggetto disinfettato*
   - *L'utente ha scelto di non applicare il criterio di criptaggio*
   - *Il file è stato ripristinato dalla Quarantena nel server Kaspersky Anti Targeted Attack Platform dall'amministratore*
   - *Il file è stato messo in quarantena nel server di Kaspersky Anti Targeted Attack Platform dall'amministratore*
   - *Messaggio all'amministratore per il blocco dell'avvio di un'applicazione*
   - *Messaggio all'amministratore per il blocco dell'accesso a un dispositivo*
   - *Messaggio all'amministratore per il blocco dell'accesso a una pagina Web*

9. Fare clic su **OK**.

10. Nella sezione **Informazioni** fare clic su **Aggiungi evento** e selezionare solo le caselle di controllo accanto ai seguenti eventi:

    - *È stata creata una copia di backup dell'oggetto*
    - *Avvio dell'applicazione non consentito in modalità di test*

11. Fare clic su **OK**.

La registrazione degli eventi importanti nel database di Administration Server è configurata.

Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security

L'opzione di pianificazione ottimale e consigliata per Kaspersky Endpoint Security è **Quando vengono scaricati nuovi aggiornamenti nell'archivio** quando la casella di controllo **Usa automaticamente il ritardo casuale per l'avvio delle attività** è selezionata.

Concessione dell'accesso offline al dispositivo esterno bloccato da Controllo Dispositivi

Nel componente Controllo Dispositivi dei criteri di Kaspersky Endpoint Security for Windows è possibile gestire l'accesso degli utenti ai dispositivi esterni installati nel dispositivo client o connessi a quest'ultimo (ad esempio, dischi rigidi, fotocamere o moduli Wi-Fi). Ciò consente di proteggere il dispositivo client dalle infezioni quando vengono collegati tali dispositivi esterni e impedire perdite o fughe di dati.

Se è necessario concedere l'accesso temporaneo al dispositivo esterno bloccato da Controllo Dispositivi ma il dispositivo esterno non può essere aggiunto all'elenco dei dispositivi attendibili, è possibile concedere l'accesso offline temporaneo al dispositivo esterno. Accesso offline significa che il dispositivo client non ha accesso alla rete.

> È possibile concedere l'accesso offline al dispositivo esterno bloccato da Controllo dispositivi solo se l'opzione **Consenti richieste di accesso temporaneo** è abilitata nelle impostazioni del criterio di Kaspersky Endpoint Security for Windows, nella sezione **Impostazioni applicazione → Controlli di sicurezza → Controllo dispositivi** section.

La concessione dell'accesso offline al dispositivo esterno bloccato da Controllo Dispositivi comprende le seguenti fasi:

1. Nella finestra di dialogo Kaspersky Endpoint Security for Windows l'utente del dispositivo che desidera avere accesso al dispositivo esterno bloccato genera un file della richiesta di accesso e lo invia all'amministratore di Kaspersky Security Center.

2. Quando riceve questa richiesta, l'amministratore di Kaspersky Security Center crea un file della chiave di accesso e lo invia all'utente del dispositivo.

3. Nella finestra di dialogo Kaspersky Endpoint Security for Windows l'utente del dispositivo attiva il file della chiave di accesso e ottiene l'accesso temporaneo al dispositivo esterno.

Per concedere l'accesso temporaneo al dispositivo esterno bloccato da Controllo Dispositivi:

1. Nel menu principale accedere a **Risorse (dispositivi) → Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. In questo elenco, selezionare il dispositivo dell'utente che richiede l'accesso al dispositivo esterno bloccato da Controllo Dispositivi.

   È possibile selezionare un solo dispositivo.

3. Sopra l'elenco dei dispositivi gestiti, fare clic sul pulsante con i puntini di sospensione (...), quindi fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.

4. Nella finestra **Impostazioni applicazione** visualizzata, nella sezione **Controllo Dispositivi**, fare clic sul pulsante **Sfoglia**.

5. Selezionare il file della richiesta di accesso ricevuto dall'utente, quindi fare clic sul pulsante **Apri**. Il file dovrebbe essere nel formato AKEY.

   Verranno visualizzati i dettagli del dispositivo bloccato a cui l'utente ha richiesto l'accesso.

6. Specificare il valore dell'impostazione **Durata accesso**.

   Questa impostazione definisce il periodo di tempo per cui verrà concesso all'utente l'accesso al dispositivo bloccato. Il valore predefinito è il valore specificato dall'utente durante la creazione del file della richiesta di accesso.

7. Specificare il periodo di tempo durante il quale la chiave di accesso può essere attivata sul dispositivo.

   Questa impostazione definisce il periodo di tempo per cui l'utente può attivare l'accesso al dispositivo bloccato utilizzando la chiave di accesso fornita.

8. Fare clic sul pulsante **Salva**.

   Verrà visualizzata la finestra standard di Microsoft Windows **Salvare la chiave di accesso**.

9. Selezionare la cartella di destinazione in cui salvare il file contenente la chiave di accesso per il dispositivo bloccato.

10. Fare clic sul pulsante **Salva**.

Come risultato, quando si invia all'utente il file della chiave di accesso e l'utente lo attiva nella finestra di dialogo Kaspersky Endpoint Security for Windows, l'utente ha accesso temporaneo al dispositivo bloccato per il periodo specifico.

Rimozione di applicazioni o aggiornamenti software in remoto

Per rimuovere applicazioni o aggiornamenti software in remoto dai dispositivi selezionati:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.

2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Disinstalla l'applicazione in remoto**.

4. Specificare il nome dell'attività che si intende creare.

   Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).

5. Selezionare i dispositivi a cui assegnare l'attività.

6. Selezionare il tipo di software da rimuovere, quindi selezionare specifiche applicazioni, aggiornamenti o patch che si desidera rimuovere:

   - **Disinstalla l'applicazione gestita**

     Verrà visualizzato un elenco di applicazioni Kaspersky. Selezionare l'applicazione che si desidera rimuovere.

   - **Disinstalla l'applicazione incompatibile**

     Viene visualizzato un elenco di applicazioni incompatibili con le applicazioni di protezione Kaspersky o Kaspersky Security Center. Selezionare le caselle di controllo accanto alle applicazioni da rimuovere.

   - **Disinstalla l'applicazione dal registro delle applicazioni**

Per impostazione predefinita, i Network Agent inviano ad Administration Server le informazioni sulle applicazioni installate nei dispositivi gestiti. L'elenco delle applicazioni installate è memorizzato nel Registro delle applicazioni.

Per selezionare un'applicazione dal Registro delle applicazioni:

a. Fare clic sul campo **Applicazione da disinstallare**, quindi selezionare l'applicazione che si desidera rimuovere.

Se si seleziona Kaspersky Security Center Network Agent, quando si esegue l'attività, lo stato *Completato correttamente* mostra che il processo di rimozione è stato avviato. Se Kaspersky Security Center Network Agent viene rimosso, lo stato non cambia. Se l'attività non riesce, lo stato diventa *Non riuscito*.

b. Specificare le opzioni di disinstallazione:

- Modalità di disinstallazione

Selezionare come si desidera rimuovere l'applicazione:

- **Definisci automaticamente il comando di disinstallazione**

  Se l'applicazione dispone di un comando di disinstallazione definito dal fornitore dell'applicazione, Kaspersky Security Center utilizza questo comando. È consigliabile selezionare questa opzione.

- **Specificare il comando di disinstallazione**

  Selezionare questa opzione se si desidera specificare il proprio comando per la disinstallazione dell'applicazione.

  È consigliabile provare prima a rimuovere l'applicazione utilizzando l'opzione **Definisci automaticamente il comando di disinstallazione**. Se la disinstallazione tramite il comando definito automaticamente non va a buon fine, utilizzare il proprio comando.

  Digitare un comando di installazione nel campo, quindi specificare la seguente opzione:

  Usa questo comando per la disinstallazione solo se il comando predefinito non è stato rilevato automaticamente

  Kaspersky Security Center controlla se l'applicazione selezionata dispone o meno di un comando di disinstallazione definito dal fornitore dell'applicazione. Se il comando viene rilevato, Kaspersky Security Center lo utilizzerà al posto del comando specificato nel campo **Comando per la disinstallazione dell'applicazione**.

  È consigliabile abilitare questa opzione.

- Esegui il riavvio dopo la disinstallazione dell'applicazione

Se l'applicazione richiede il riavvio del sistema operativo nel dispositivo gestito dopo la disinstallazione, il sistema operativo viene riavviato automaticamente.

- **Disinstalla l'aggiornamento dell'applicazione specificato, la patch o l'applicazione di terze parti specificata**

  Viene visualizzato un elenco di aggiornamenti, patch e applicazioni di terze parti. Selezionare l'elemento da rimuovere.

  L'elenco visualizzato è un elenco generale di applicazioni e aggiornamenti e non corrisponde alle applicazioni e agli aggiornamenti installati nei dispositivi gestiti. Prima di selezionare un elemento, è consigliabile assicurarsi che l'applicazione o l'aggiornamento sia installato nei dispositivi definiti nell'ambito dell'attività. È possibile visualizzare l'elenco dei dispositivi in cui è installato l'aggiornamento o l'applicazione tramite la finestra delle proprietà.

  Per visualizzare l'elenco dei dispositivi:

  a. Fare clic sul nome dell'applicazione o dell'aggiornamento.

     Verrà visualizzata la finestra delle proprietà.

  b. Aprire la sezione **Dispositivi**.

     È inoltre possibile visualizzare l'elenco delle applicazioni installate e degli aggiornamenti nella finestra delle proprietà del dispositivo.

7. Specificare il modo in cui i dispositivi client scaricheranno l'utilità di disinstallazione:

- **Utilizzando Network Agent**

  I file vengono distribuiti nei dispositivi client da Network Agent installato in tali dispositivi client.

  Se questa opzione è disabilitata, i file vengono distribuiti utilizzando gli strumenti di Microsoft Windows.

  È consigliabile abilitare questa opzione se l'attività è stata assegnata a dispositivi in cui sono installati Network Agent.

- **Utilizzando le risorse del sistema operativo tramite Administration Server**

  I file vengono trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo di Administration Server. È possibile abilitare questa opzione se Network Agent non è installato nel dispositivo client, ma il dispositivo client è incluso nella stessa rete di Administration Server.

- **Utilizzando le risorse del sistema operativo tramite punti di distribuzione**

  I file vengono trasmessi ai dispositivi client utilizzando gli strumenti del sistema operativo tramite punti di distribuzione. È possibile abilitare questa opzione se è presente almeno un punto di distribuzione nella rete.

  Se l'opzione **Utilizzando Network Agent** è abilitata, i file vengono distribuiti utilizzando gli strumenti del sistema operativo solo se gli strumenti di Network Agent non sono disponibili.

- **Numero massimo di download simultanei**

  Il numero massimo consentito di dispositivi client a cui Administration Server può trasmettere simultaneamente i file. Maggiore è questo numero, più velocemente l'applicazione verrà disinstallata, ma in questo caso il carico su Administration Server sarà più elevato.

- **Numero massimo di tentativi di disinstallazione**

Se, durante l'esecuzione dell'attività *Disinstalla l'applicazione in remoto*, Kaspersky Security Center non riesce a disinstallare un'applicazione in un dispositivo gestito entro il numero di esecuzioni del programma di installazione specificate dal parametro, Kaspersky Security Center interrompe la distribuzione dell'utilità di disinstallazione a tale dispositivo gestito e non avvia più il programma di installazione nel dispositivo.

Il parametro **Numero massimo di tentativi di disinstallazione** consente di salvare le risorse del dispositivo gestito, nonché di ridurre il traffico (disinstallazione, esecuzione del file MSI e messaggi di errore).

I tentativi ricorrenti di avvio dell'attività possono indicare un problema nel dispositivo che impedisce la disinstallazione. L'amministratore dovrebbe risolvere il problema entro il numero specificato di tentativi di disinstallazione e quindi riavviare l'attività (manualmente o in base a una pianificazione).

Se la disinstallazione non va a buon fine, il problema è ritenuto irrisolvibile e ulteriori tentativi di avvio dell'attività sono considerati dispendiosi in termini di risorse e traffico.

Quando viene creata l'attività, il conteggio dei tentativi è impostato su `0`. Per ogni esecuzione del programma di installazione che restituisce un errore nel dispositivo il numero aumenta.

Se il numero di tentativi specificati nel parametro è stato superato e il dispositivo è pronto per la disinstallazione dell'applicazione, è possibile aumentare il valore del parametro **Numero massimo di tentativi di disinstallazione** e avviare l'attività per disinstallare l'applicazione. In alternativa, è possibile creare una nuova attività *Disinstalla l'applicazione in remoto*.

- **Verifica il tipo di sistema operativo prima del download**

  Prima di trasmettere i file ai dispositivi client, Kaspersky Security Center verifica se le impostazioni dell'utilità di installazione sono applicabili al sistema operativo del dispositivo client. Se le impostazioni non sono applicabili, Kaspersky Security Center non trasmette i file e non tenta di installare l'applicazione. Ad esempio, per installare un'applicazione nei dispositivi di un gruppo di amministrazione che include dispositivi che eseguono vari sistemi operativi, è possibile assegnare l'attività di installazione al gruppo di amministrazione e quindi abilitare questa opzione per ignorare i dispositivi che eseguono un sistema operativo diverso da quello desiderato.

- **Usa password di disinstallazione**

  Questo parametro viene visualizzato se nel passaggio precedente è stato selezionato **Disinstalla applicazione gestita** e quindi è stato specificato Kaspersky Security Center Network Agent nel campo **Applicazione da disinstallare**.

  Se la password per la disinstallazione remota di Network Agent è stata impostata in precedenza nelle impostazioni dei criteri di Network Agent, selezionare la casella di controllo **Usa password di disinstallazione**, quindi immettere la password di disinstallazione nel campo **Password**. Se non è stata impostata la password per la disinstallazione remota di Network Agent, non selezionare la casella di controllo.

8. Specificare le impostazioni per il riavvio del sistema operativo:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ripeti la richiesta ogni (min.)**

  Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

  Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

- **Riavvia dopo (min.)**

  Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

  Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

9. Se necessario, aggiungere gli account che verranno utilizzati per avviare l'attività di disinstallazione remota:

- **Nessun account richiesto (Network Agent installato)**

  Se questa opzione è selezionata, non è necessario specificare un account con cui verrà eseguito il programma di installazione dell'applicazione. L'attività sarà eseguita tramite l'account con cui viene eseguito Administration Server.

  Se Network Agent non è stato installato nei dispositivi client, questa opzione non è disponibile.

- **Account richiesto (Network Agent non utilizzato)**

  Selezionare questa opzione se Network Agent non è installato nei dispositivi a cui si assegna l'attività *Disinstalla l'applicazione in remoto*. In questo caso, è possibile specificare un account utente o un certificato SSH per disinstallare l'applicazione.

  - **Account locale**. Se questa opzione è selezionata, specificare l'account utente con cui verrà eseguito il programma di installazione dell'applicazione. Fare clic sul pulsante **Aggiungi**, selezionare **Account locale** e quindi specificare le credenziali dell'account utente.

    È possibile specificare più account utente, ad esempio se nessuno di essi dispone di tutti i diritti richiesti per tutti i dispositivi per cui si assegna l'attività. In questo caso, tutti gli account aggiunti vengono utilizzati per l'esecuzione dell'attività, consecutivamente, dall'alto in basso.

  - **Certificato SSH**. Se si desidera disinstallare un'applicazione da un dispositivo client basato su Linux, è possibile specificare un certificato SSH anziché un account utente. Fare clic sul pulsante **Aggiungi**, selezionare **Certificato SSH**, quindi specificare la chiave privata e quella pubblica del certificato.

    Per generare una chiave privata, è possibile utilizzare l'utilità ssh-keygen. Si noti che Kaspersky Security Center supporta il formato PEM delle chiavi private, ma l'utilità ssh-keygen genera chiavi SSH nel formato OPENSSH per impostazione predefinita. Il formato OPENSSH non è supportato da Kaspersky Security Center. Per creare una chiave privata nel formato PEM supportato, aggiungere l'opzione -m PEM nel comando ssh-keygen.

    Ad esempio:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail dell'utente>"
    ```

10. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

11. Fare clic sul pulsante **Fine**.

    L'attività verrà creata e visualizzata nell'elenco delle attività.

12. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

13. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività.

14. Fare clic sul pulsante **Salva**.

15. Eseguire l'attività manualmente o attenderne l'avvio in base alla pianificazione specificata nelle impostazioni dell'attività.

    Al termine dell'attività di disinstallazione remota, l'applicazione selezionata verrà rimossa dai dispositivi selezionati.

Problemi di disinstallazione remota

A volte la disinstallazione remota di applicazioni di terze parti può terminare con il seguente avviso: "La disinstallazione remota è terminata su questo dispositivo con avvisi: l'applicazione per la rimozione delle applicazioni non è installata". Questo problema si verifica quando l'applicazione da disinstallare è già stata disinstallata o è stata installata solo per un singolo utente. Le applicazioni installate per un singolo utente (chiamate anche applicazioni per utente) diventano invisibili e non possono essere disinstallate da remoto se l'utente non ha effettuato l'accesso.

Questo comportamento è in contrasto con le applicazioni pensate per essere utilizzate da più utenti sullo stesso dispositivo (chiamate anche applicazioni per dispositivo). Le applicazioni per dispositivo sono visibili e accessibili a tutti gli utenti del dispositivo.

Pertanto, le applicazioni per utente devono essere disinstallate solo quando l'utente ha effettuato l'accesso.

Fonte di informazioni sulle applicazioni installate

Network Agent recupera informazioni sul software installato nei dispositivi Windows dalle seguenti chiavi di registro:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contiene informazioni sulle applicazioni installate per tutti gli utenti.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Contiene informazioni sulle applicazioni installate per tutti gli utenti.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contiene informazioni sulle applicazioni installate per l'utente corrente.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contiene informazioni sulle applicazioni installate per utenti specifici.

Attività

Questa sezione descrive le attività utilizzate da Kaspersky Security Center.

Informazioni sulle attività

Kaspersky Security Center consente di gestire le applicazioni di protezione Kaspersky installate nei dispositivi creando ed eseguendo *attività*. Le attività sono necessarie per l'installazione, l'avvio e l'arresto delle applicazioni, la scansione dei file, l'aggiornamento dei database e dei moduli software, oltre che per eseguire altre azioni sulle applicazioni.

Le attività per un'applicazione specifica possono essere create utilizzando Kaspersky Security Center Web Console solo se il plug-in di gestione per tale applicazione è installato in Kaspersky Security Center Web Console Server.

Le attività possono essere eseguite nell'Administration Server e nei dispositivi.

Le attività eseguite in Administration Server includono:

- Distribuzione automatica dei rapporti
- Download degli aggiornamenti nell'archivio
- Backup dei dati di Administration Server
- Manutenzione del database

I seguenti tipi di attività vengono eseguiti nei dispositivi:

- *Attività locali* - Attività eseguite in un dispositivo specifico

  Le attività locali possono essere modificate dall'amministratore utilizzando gli strumenti di Administration Console oppure dall'utente di un dispositivo remoto (ad esempio, attraverso l'interfaccia dell'applicazione di protezione). Se un'attività locale viene modificata contemporaneamente dall'amministratore e dall'utente di un dispositivo gestito, hanno effetto le modifiche apportate dall'amministratore perché hanno una priorità più alta.

- *Attività di gruppo* - Attività eseguite su tutti i dispositivi di un gruppo specifico

  A meno che non sia diversamente specificato nelle proprietà dell'attività, un'attività di gruppo si applica anche a tutti i sottogruppi del gruppo selezionato. Un'attività di gruppo influisce anche (facoltativamente) sui dispositivi connessi agli Administration Server secondari e virtuali distribuiti nel gruppo o in uno dei relativi sottogruppi.

- *Attività globali* - Attività eseguite su un set di dispositivi, indipendentemente dalla loro appartenenza a un gruppo.

Per ogni applicazione è possibile creare attività di gruppo, attività globali o attività locali.

È possibile apportare modifiche alle impostazioni delle attività, visualizzarne l'avanzamento, copiarle, esportarle, importarle ed eliminarle.

Le attività vengono avviate in un dispositivo solo se l'applicazione per cui l'attività è stata creata è in esecuzione.

I risultati dell'esecuzione delle attività vengono salvati nel registro eventi del sistema operativo in ciascun dispositivo, nel registro eventi del sistema operativo in Administration Server e nel database di Administration Server.

Non includere dati privati nelle impostazioni dell'attività. Ad esempio, non specificare la password dell'amministratore del dominio.

Informazioni sull'ambito dell'attività

L'*ambito di un'attività* è il set di dispositivi in cui viene eseguita l'attività. I tipi di ambito sono i seguenti:

- Per un'*attività locale*, l'ambito è il dispositivo stesso.
- Per un'*attività di Administration Server*, l'ambito è Administration Server.
- Per un'*attività di gruppo*, l'ambito è l'elenco dei dispositivi inclusi nel gruppo.

Durante la creazione di un'*attività globale*, è possibile utilizzare i seguenti metodi per specificare l'ambito:

- Specificare manualmente specifici dispositivi.

  È possibile utilizzare un indirizzo IP (o un intervallo IP), un nome NetBIOS o un nome DNS come indirizzo del dispositivo.

- Importare un elenco di dispositivi da un file TXT con gli indirizzi dei dispositivi da aggiungere (ogni indirizzo deve essere specificato su una riga distinta).

  Se si importa un elenco di dispositivi da un file o se ne crea uno manualmente e i dispositivi vengono identificati con i rispettivi nomi, l'elenco deve contenere solo dispositivi per cui sono già state immesse le informazioni nel database di Administration Server. Inoltre, le informazioni devono essere state immesse al momento della connessione dei dispositivi o durante la device discovery.

- Specificare una selezione dispositivi.

  Nel corso del tempo, l'ambito un'attività si modifica, perché il set di dispositivi inclusi nella selezione cambia. Una selezione di dispositivi può essere creata sulla base degli attributi dei dispositivi, incluso il software installato in un dispositivo, e utilizzando i tag assegnati ai dispositivi. Una selezione dispositivi è il modo più flessibile per specificare l'ambito di un'attività.

  Le attività per le selezioni dispositivi vengono sempre eseguite in base a una pianificazione da Administration Server. Queste attività non possono essere eseguite nei dispositivi che non dispongono di una connessione ad Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite direttamente nei dispositivi, pertanto non dipendono dalla connessione del dispositivo ad Administration Server.

Le attività per le selezioni dispositivi non vengono eseguite in base all'ora locale di un dispositivo, ma in base all'ora locale di Administration Server. Le attività il cui ambito è specificato tramite altri metodi vengono eseguite in base all'ora locale di un dispositivo.

Creazione di un'attività

Per creare un'attività:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni visualizzate.
3. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
4. Fare clic sul pulsante **Fine**.

L'attività verrà creata e visualizzata nell'elenco delle attività.

Per creare una nuova attività assegnata ai dispositivi selezionati:

1. Nel menu principale accedere a **Risorse (dispositivi)** →**Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.
2. Nell'elenco dei dispositivi gestiti, selezionare le caselle di controllo accanto ai dispositivi per eseguire l'attività per gli stessi. È possibile utilizzare le funzioni di ricerca e filtraggio per trovare i dispositivi cercati.
3. Fare clic sul pulsante **Esegui attività**, quindi selezionare **Aggiungi nuova attività**.

   Verrà avviata la Creazione guidata nuova attività.

   Nel primo passaggio della procedura guidata, è possibile rimuovere i dispositivi selezionati da includere nell'ambito dell'attività. Seguire le istruzioni della procedura guidata.
4. Fare clic sul pulsante **Fine**.

L'attività viene creata per i dispositivi selezionati.

Avvio manuale di un'attività

L'applicazione avvia le attività in base alle impostazioni di pianificazione specificate nelle proprietà di ciascuna attività. È possibile avviare manualmente un'attività in qualsiasi momento dall'elenco di attività. In alternativa, è possibile selezionare i dispositivi nell'elenco **Dispositivi gestiti** e quindi avviare un'attività esistente per questi.

Per avviare un'attività manualmente:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Nell'elenco delle attività selezionare la casella di controllo accanto all'attività da avviare.
3. Fare clic sul pulsante **Avvia**.

L'attività viene avviata. È possibile controllare lo stato dell'attività nella colonna **Stato** o facendo clic sul pulsante **Risultato**.

Visualizzazione dell'elenco delle attività

È possibile visualizzare l'elenco delle attività create in Kaspersky Security Center.

Per visualizzare l'elenco delle attività,

Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

Verrà visualizzato l'elenco delle attività. Le attività sono raggruppate in base ai nomi delle applicazioni a cui sono correlate. Ad esempio, l'attività *Disinstalla l'applicazione in remoto* è correlata ad Administration Server e l'attività *Trova vulnerabilità e aggiornamenti richiesti* fa riferimento a Network Agent.

Per visualizzare le proprietà di un'attività:

Fare clic sul nome dell'attività.

Verrà visualizzata la finestra delle proprietà dell'attività con diverse schede denominate. Ad esempio, **Tipo di attività** viene visualizzato nella scheda **Generale** e la pianificazione dell'attività nella scheda **Pianificazione**.

Impostazioni generali delle attività

Questa sezione contiene le impostazioni che è possibile configurare per la maggior parte delle attività. L'elenco delle impostazioni disponibili dipende dall'attività che si sta configurando.

Impostazioni specificate durante la creazione dell'attività

È possibile specificare le seguenti impostazioni durante la creazione di un'attività. Alcune di queste impostazioni possono anche essere modificate nelle proprietà dell'attività creata.

- Impostazioni per il riavvio del sistema operativo:
  - **Non riavviare il dispositivo**

    I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

  - **Riavvia il dispositivo**

    I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

  - **Richiedi l'intervento dell'utente**

    Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Ripeti la richiesta ogni (min.)**

    Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

    Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

    Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

  - **Riavvia dopo (min.)**

    Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

    Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  - **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

- Impostazioni di pianificazione dell'attività:

  I tipi di pianificazione possono variare a seconda dell'attività.

  - **Impostazione Avvia attività:**

    - Ogni N ore

      L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

      Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

    - Ogni N giorni

      L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

      Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

    - Ogni N minuti

      L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

      Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

    - In base ai giorni della settimana

      L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

      Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

    - Mensile

L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

- **Manualmente**

  L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

  Per impostazione predefinita, questa opzione è selezionata.

- **Una sola volta**

  L'attività viene eseguita una volta, nella data e nell'ora specificate (per impostazione predefinita, il giorno in cui è stata creata l'attività).

- **Immediatamente**

  L'attività viene eseguita immediatamente dopo il salvataggio delle impostazioni.

- **Ogni mese nei giorni specificati delle settimane selezionate**

  L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

  Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

  > Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

  È possibile selezionare più giorni della settimana.

- **Quando vengono scaricati nuovi aggiornamenti nell'archivio**

  L'attività viene eseguita dopo il download degli aggiornamenti nell'archivio. È ad esempio possibile utilizzare questa pianificazione per l'attività Trova vulnerabilità e aggiornamenti richiesti.

- **Durante un'epidemia di virus**

L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

- Anti-virus per workstation e file server
- Anti-virus per la difesa perimetrale
- Anti-virus per i sistemi di posta

Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

  L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

  È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

  Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

  - Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
  - Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

    Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
  - Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

  Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

  Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

  Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale automaticamente per l'avvio delle attività con un intervallo di**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

- Dispositivi a cui assegnare l'attività:
  - Selezionare i dispositivi della rete rilevati da Administration Server

    L'attività viene assegnata a dispositivi specifici. I dispositivi specifici possono includere i dispositivi nei gruppi di amministrazione, nonché i dispositivi non assegnati.

    Questa opzione può ad esempio essere utilizzata in un'attività per l'installazione di Network Agent nei dispositivi non assegnati.

  - Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco

    È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

    Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

  - Assegna attività a una selezione dispositivi

    L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

    Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

  - Assegna attività a un gruppo di amministrazione

    L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

    Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

    Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

- Impostazioni per l'account:
  - Account predefinito

    L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

    Per impostazione predefinita, questa opzione è selezionata.

  - Specificare un account

    Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

  - Account

Account tramite il quale viene eseguita l'attività.

- **Password**

  Password dell'account con cui verrà eseguita l'attività.

Impostazioni specificate dopo la creazione dell'attività

È possibile specificare le seguenti impostazioni solo dopo la creazione di un'attività.

- Impostazioni delle attività di gruppo:
  - **Distribuisci ai sottogruppi**

    Questa opzione è disponibile solo nelle impostazioni delle attività di gruppo.

    Quando questa opzione è abilitata, l'ambito dell'attività include:

    - Il gruppo di amministrazione selezionato durante la creazione dell'attività.
    - I gruppi di amministrazione subordinati al gruppo di amministrazione selezionato a qualsiasi livello inferiore nella gerarchia dei gruppi.

    Quando questa opzione è disabilitata, l'ambito dell'attività include solo il gruppo di amministrazione selezionato durante la creazione dell'attività.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Distribuisci negli Administration Server secondari e virtuali**

    Quando questa opzione è abilitata, l'attività valida nell'Administration Server primario viene applicata anche negli Administration Server secondari (compresi quelli virtuali). Se un'attività dello stesso tipo esiste già nell'Administration Server secondario, nell'Administration Server secondario vengono applicate entrambe le attività: quella esistente e quella ereditata dall'Administration Server primario.

    Questa opzione è disponibile solo quando l'opzione **Distribuisci ai sottogruppi** è abilitata.

    Per impostazione predefinita, questa opzione è disabilitata.

- Impostazioni di pianificazione avanzate:
  - **Accendi i dispositivi utilizzando la funzione Wake-on-LAN prima di avviare l'attività**

    Il sistema operativo nel dispositivo verrà avviato in base al periodo di tempo specificato prima dell'avvio dell'attività pianificata. Il periodo di tempo predefinito è cinque minuti.

    Abilitare questa opzione se si desidera eseguire l'attività in tutti i dispositivi client nell'ambito dell'attività, inclusi quelli che sono spenti al momento dell'avvio dell'attività.

    Se si desidera che il dispositivo si spenga automaticamente al termine dell'attività, abilitare l'opzione **Spegni i dispositivi dopo il completamento dell'attività**. Questa opzione è disponibile nella stessa finestra.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Spegni i dispositivi dopo il completamento dell'attività**

    Questa opzione può ad esempio essere abilitata per un'attività di aggiornamento dell'installazione che installa gli aggiornamenti nei dispositivi client ogni venerdì dopo l'orario lavorativo e quindi spegne tali dispositivi per il fine settimana.

    Per impostazione predefinita, questa opzione è disabilitata.

- **Arresta se l'attività viene eseguita per più di**

  Al termine del periodo di tempo specificato, l'attività viene arrestata automaticamente, che sia stata completata o meno.

  Abilitare questa opzione se si desidera interrompere (o arrestare) le attività che richiedono troppo tempo per l'esecuzione.

  Per impostazione predefinita, questa opzione è disabilitata. Il tempo predefinito per l'esecuzione dell'attività è 120 minuti.

- Impostazioni di notifica:
  - Blocco **Salva cronologia attività**:
    - Archivia nel database di Administration Server per (giorni)

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività in tutti i dispositivi client nell'ambito dell'attività vengono archiviati nell'Administration Server per il numero di giorni specificato. Al termine di questo periodo, le informazioni vengono eliminate da Administration Server.

      Per impostazione predefinita, questa opzione è abilitata.

    - Archivia nel registro eventi del sistema operativo del dispositivo

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività vengono archiviati in locale nel registro eventi di Windows di ogni dispositivo client.

      Per impostazione predefinita, questa opzione è disabilitata.

    - Archivia nel registro eventi del sistema operativo in Administration Server

      Gli eventi dell'applicazione relativi all'esecuzione dell'attività in tutti i dispositivi client nell'ambito dell'attività vengono archiviati in modo centralizzato nel registro eventi di Windows del sistema operativo di Administration Server.

      Per impostazione predefinita, questa opzione è disabilitata.

    - Salva tutti gli eventi

      Se questa opzione è selezionata, nei registri eventi vengono salvati tutti gli eventi relativi all'attività.

    - Salva eventi correlati all'avanzamento dell'attività

      Se questa opzione è selezionata, nei registri eventi vengono salvati solo gli eventi relativi all'esecuzione dell'attività.

    - Salva solo i risultati dell'esecuzione dell'attività

      Se questa opzione è selezionata, nei registri eventi vengono salvati solo gli eventi relativi ai risultati dell'attività.

  - Notifica all'amministratore i risultati dell'esecuzione dell'attività

    È possibile selezionare i metodi con cui inviare agli amministratori le notifiche relative ai risultati dell'esecuzione dell'attività: tramite e-mail, SMS o un file eseguibile. Per configurare la notifica, fare clic sul collegamento **Impostazioni**.

    Per impostazione predefinita, tutti i metodi di notifica sono disabilitati.

  - Notifica solo errori

Se questa opzione è abilitata, agli amministratori viene inviata una notifica solo quando l'esecuzione di un'attività viene completata con un errore.

Se questa opzione è disabilitata, agli amministratori viene inviata una notifica dopo il completamento dell'esecuzione di ogni attività.

Per impostazione predefinita, questa opzione è abilitata.

- Impostazioni della protezione.
- Impostazioni dell'ambito dell'attività.

  A seconda del modo in cui viene determinato l'ambito dell'attività, sono disponibili le seguenti impostazioni:

  - **Dispositivi**

    Se l'ambito di un'attività è determinato in base a un gruppo di amministrazione, è possibile visualizzare tale gruppo. In questo caso, non è possibile apportare modifiche. Tuttavia, è possibile impostare l'opzione **Esclusioni dall'ambito dell'attività**.

    Se l'ambito di un'attività è determinato in base a un elenco di dispositivi, è possibile modificare l'elenco aggiungendo e rimuovendo dispositivi.

  - **Selezione dispositivi**

    È possibile modificare la selezione dispositivi a cui viene applicata l'attività.

  - **Esclusioni dall'ambito dell'attività**

    È possibile specificare gruppi di dispositivi a cui non deve essere applicata l'attività. I gruppi da escludere possono essere solo sottogruppi del gruppo di amministrazione a cui è applicata l'attività.

- **Cronologia revisioni**.

Esportazione di un'attività

Kaspersky Security Center consente di salvare un'attività e le relative impostazioni in un file KLT. È possibile utilizzare questo file KLT per importare l'attività salvata sia per Kaspersky Security Center Windows che per Kaspersky Security Center Linux.

Per esportare un'attività:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Selezionare la casella di controllo accanto all'attività che si desidera esportare.

   Non è possibile esportare più attività contemporaneamente. Se si selezionano più attività, il pulsante **Esporta** verrà disabilitato. Neanche le attività di Administration Server sono disponibili per l'esportazione.

3. Fare clic sul pulsante **Esporta**.

4. Nella finestra **Salva con nome** visualizzata, specificare il percorso e il nome del file di attività. Fare clic sul pulsante **Salva**.

   La finestra **Salva con nome** viene visualizzata solo se si utilizza Google Chrome, Microsoft Edge oppure Opera. Se si utilizza un altro browser, il file di attività viene salvato automaticamente nella cartella **Download**.

Importazione di un'attività

Kaspersky Security Center consente di importare un'attività da un file KLT. Il file KLT contiene l'attività esportata e le sue impostazioni.

Per importare un'attività:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

2. Fare clic sul pulsante **Importa**.

3. Fare clic sul pulsante **Sfoglia** per scegliere un file di attività da importare.

4. Nella finestra visualizzata, specificare il percorso del file di attività KLT, quindi fare clic sul pulsante **Apri**. Si noti che è possibile selezionare solo un file di attività.

   Viene avviata l'elaborazione dell'attività.

5. Dopo che l'attività è stata elaborata correttamente, selezionare i dispositivi a cui si desidera assegnare l'attività. A tale scopo, selezionare una delle seguenti opzioni:

   - **Assegna attività a un gruppo di amministrazione**

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

     Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

   - **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**

     È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

   - **Assegna attività a una selezione dispositivi**

     L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

6. Specificare l'ambito dell'attività.

7. Fare clic sul pulsante **Completa** per completare l'importazione dell'attività.

Viene visualizzata la notifica con i risultati dell'importazione. Se l'attività viene importata correttamente, è possibile fare clic sul collegamento **Dettagli** per visualizzare le proprietà dell'attività.

Dopo un'importazione riuscita, l'attività viene visualizzata nell'elenco delle attività. Vengono importate anche le impostazioni e la pianificazione dell'attività. L'attività verrà avviata in base alla sua pianificazione.

Se l'attività appena importata ha un nome identico a un'attività esistente, il nome dell'attività importata viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Avvio della Procedura guidata per la modifica della password delle attività

Per un'attività non locale, è possibile specificare un account con il quale deve essere eseguita l'attività. È possibile specificare l'account durante la creazione dell'attività o nelle proprietà di un'attività esistente. Se l'account specificato è utilizzato conformemente alle istruzioni di sicurezza dell'organizzazione, queste istruzioni possono occasionalmente richiedere la modifica della password dell'account. Quando scade la password dell'account e viene impostata una nuova password, l'attività non verrà avviata fino a quando non viene specificata la nuova password valida nelle proprietà dell'attività.

La Procedura guidata per la modifica della password delle attività consente di sostituire automaticamente la vecchia password con la nuova in tutte le attività in cui è specificato l'account. In alternativa, è possibile modificare manualmente questa password nelle proprietà di ogni attività.

Per avviare la Procedura guidata per la modifica della password delle attività:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Gestisci credenziali degli account per l'avvio delle attività**.

Seguire le istruzioni della procedura guidata.

Passaggio 1. Immissione delle credenziali

Specificare le nuove credenziali attualmente valide nel sistema (ad esempio, in Active Directory). Quando si passa al passaggio successivo della procedura guidata, Kaspersky Security Center verifica se il nome dell'account specificato corrisponde al nome dell'account nelle proprietà di ogni attività non locale. Se il nome dell'account corrisponde, la password nelle proprietà dell'attività verrà automaticamente sostituita con quella nuova.

Per specificare il nuovo account, selezionare un'opzione:

- **Usa account corrente**

  La procedura guidata utilizza il nome dell'account con cui si è attualmente connessi a Kaspersky Security Center Web Console. Specificare manualmente la password dell'account nel campo **Password corrente da utilizzare nelle attività**.

- **Specifica un account diverso**

  Specificare il nome dell'account con cui devono essere avviate le attività. Specificare la password dell'account nel campo **Password corrente da utilizzare nelle attività**.

Se si compila il campo **Password precedente (opzionale; se si desidera sostituirla con quella corrente)**, Kaspersky Security Center sostituisce la password solo per le attività in cui si trovano sia il nome dell'account sia la password precedente. La sostituzione viene eseguita automaticamente. In tutti gli altri casi è necessario scegliere un'azione da eseguire nel passaggio successivo della procedura guidata.

Passaggio 2. Selezione di un'azione da eseguire

Se non è stata specificata la password precedente nel primo passaggio della procedura guidata o se la password precedente specificata non corrisponde alle password nelle proprietà delle attività, è necessario scegliere un'azione da eseguire per le attività rilevate.

Per scegliere un'azione per un'attività:

1. Selezionare la casella di controllo accanto all'attività per cui si desidera scegliere un'azione.
2. Eseguire una delle operazioni seguenti:
   - Per rimuovere la password nelle proprietà dell'attività, fare clic su **Elimina credenziali**.

     L'attività viene configurata per l'esecuzione con l'account predefinito.
   - Per sostituire la password con una nuova, fare clic su **Applica la modifica della password anche se la password precedente è errata o non specificata**.
   - Per annullare la modifica della password, fare clic su **Nessuna azione selezionata**.

Le azioni scelte vengono applicate una volta che si procede al passaggio successivo della procedura guidata.

Passaggio 3. Visualizzazione dei risultati

Nell'ultimo passaggio della procedura guidata, visualizzare i risultati per ciascuna attività rilevata. Per completare la procedura guidata, fare clic sul pulsante **Fine**.

Creazione dell'attività Esegui script da remoto

È possibile creare un'attività *Esegui script da remoto* per eseguire un pacchetto di installazione in un dispositivo client e per installare in remoto un'applicazione.

Un pacchetto di installazione contiene un archivio ZIP con un set di script per l'esecuzione nei dispositivi client e un file manifest.json. Ulteriori informazioni sulla creazione di questo tipo di pacchetto di installazione sono contenute in questo articolo.

Questa attività deve essere avviata solo nei dispositivi con Network Agent for Linux.

Per avviare un'attività Esegui script da remoto:

1. Passare alla **Creazione guidata nuova attività** e selezionare il tipo di attività **Esegui script da remoto**.
2. Immettere il nome dell'attività e selezionare i dispositivi a cui verrà assegnata l'attività. Fare clic sul pulsante **Avanti**.
3. Selezionare un pacchetto di installazione basato su un archivio ZIP con un file manifest.json per l'esecuzione remota.

   Se non si desidera eseguire nuovamente l'attività nei dispositivi in cui è già stata completata, attivare l'opzione **Non avviare questa attività su dispositivi in cui è già stata completata**.

4. Selezionare un account per l'esecuzione dell'attività.

   Se si seleziona l'account predefinito, l'attività verrà eseguita dal Network Agent (account root).

   > Quando l'attività *Esegui script da remoto* viene avviata, non è possibile modificare l'account a cui è assegnata. Per modificare l'account a cui è assegnata l'attività, interrompere l'attività nelle impostazioni dell'attività e crearla di nuovo con i dettagli dell'account corretti.

5. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

6. Fare clic sul pulsante **Fine**.

   L'attività *Esegui script da remoto* verrà creata e visualizzata nell'elenco delle attività.

> Dopo aver ricevuto i dati dall'attività *Esegui script da remoto*, Network Agent limita l'accesso ai dati ricevuti per tutti gli utenti, ad eccezione dell'amministratore e dell'utente specificato nelle impostazioni dell'attività.

Installazione remota delle applicazioni nei dispositivi che utilizzano l'attività Esegui script da remoto

L'attività *Esegui script da remoto* può essere utilizzata per installare in remoto un'applicazione in un dispositivo client creando un pacchetto di installazione personalizzato.

Le istruzioni per preparare un archivio per questa attività sono contenute in questo articolo.

Per creare un pacchetto di installazione per l'installazione remota di un'applicazione in un dispositivo client, i seguenti file devono essere inclusi nell'archivio che si desidera caricare per questa attività:

- <nome pacchetto>.deb
- install.sh

  ```
  sudo apt-get install <nome pacchetto>.deb
  ```

- manifest.json

Schema JSON per l'installazione remota di un'applicazione

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "install.sh",
      "args": "<immettere gli argomenti, se necessario>",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

Descrizione degli array

1. `version`: versione del file manifest e dell'attività.

   Al momento, l'unico valore accettabile è 1.

2. Gli elementi dell'array delle `actions` determinano la composizione e l'ordine degli script eseguiti nell'attività.

   L'ordine di esecuzione dello script corrisponde all'indice (posto) di un elemento nell'array.

3. Per ogni elemento dell'array delle `actions`, sono definiti i seguenti elementi.

   a. `type`: tipo di comando eseguibile dagli script. Al momento, il valore viene sempre `execute`.

   b. `path`: percorso del file di script nell'archivio.

   c. `args`: argomenti passati allo script come parte del comando eseguibile.

   d. `results`: array che definisce ulteriori azioni a seconda del risultato dell'attività.

      1. `code`: valore che restituisce uno script.

      2. `next`: azione successiva da completare. L'azione `continue` procede con l'esecuzione dello script successivo (elemento nell'array delle `actions`); l'azione di `break` interrompe l'attività.

   e. `default_next`: azione se uno script restituisce un valore che non è contenuto nei `results`.

Quando l'attività *Esegui script da remoto* viene avviata, Network Agent caricherà il pacchetto di installazione con l'applicazione nel dispositivo client. Quando il dispositivo client riceve il pacchetto di installazione, Network Agent in questo dispositivo analizza il file manifest.json e definisce l'ordine di esecuzione degli script e delle azioni in base al risultato, quindi avvia l'esecuzione.

Al termine dell'attività *Esegui script da remoto*, l'applicazione verrà installata nel dispositivo client.

Configurazione delle notifiche e del monitoraggio per l'attività Esegui script da remoto

È possibile configurare il monitoraggio, il comportamento di salvataggio degli eventi e le notifiche per l'attività *Esegui script da remoto*.

Per visualizzare lo stato dell'attività Esegui script da remoto:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
   Verrà visualizzato l'elenco delle attività.
2. Selezionare l'attività e fare clic su **Cronologia dei dispositivi**.
   Viene mostrato lo stato di avanzamento dell'attività.

Per configurare il comportamento di salvataggio degli eventi:

1. Nell'elenco delle attività, fare clic sull'attività e accedere alla scheda **Impostazioni**.
2. Nella sezione **Notifiche**, fare clic sul pulsante **Impostazioni**.
3. Selezionare una delle seguenti opzioni per il comportamento dell'applicazione al termine dell'attività:
   - **Salva tutti gli eventi**.
   - **Salva eventi correlati all'avanzamento dell'attività**.
   - **Salva solo i risultati dell'esecuzione dell'attività**.
     Gli eventi vengono salvati nella **Cronologia dei dispositivi** e nell'**Archivio eventi**.
     Per impostazione predefinita, vengono salvati solo i risultati dell'esecuzione dell'attività.

     > Se si seleziona **Salva tutti gli eventi**, verranno salvati solo i risultati dell'esecuzione dell'attività.
4. Se si desidera mantenere gli eventi nel database di Administration Server, nel registro eventi di Administration Server o nel dispositivo, attivare l'opzione corrispondente.

Ulteriori informazioni sulla configurazione delle notifiche sono disponibili in questo articolo.

Preparazione di un archivio per l'attività Esegui script da remoto

Un archivio per l'attività *Esegui script da remoto* basata su un file manifest.json deve soddisfare i seguenti requisiti:

- Formato archivio: ZIP.
- Dimensione totale: non più di 1 GB.
- Il numero di file e cartelle nell'archivio è illimitato.

- Il file manifesto per l'archivio deve corrispondere allo schema seguente e deve essere denominato manifest.json. Lo schema viene convalidato solo durante l'esecuzione dell'attività in un dispositivo.

  Schema JSON del file manifesto e descrizione degli array

Schema JSON

```
{
 "$schema": "http://json-schema.org/draft-07/schema#",
  "title": "Schema for execute scripts task",
   "type": "object",
    "properties": {
        "version": {
            "type": "integer",
            "enum": [1]
        },
        "actions":{
            "type": "array",
            "items": {
                "type": "object",
                "properties": {
                    "type": {
                        "type": "string",
                        "enum": ["execute"]
                    },
                    "path": {
                        "type": "string"
                    },
                    "args": {
                        "type": "string"
                    },
                    "results":{
                        "type": "array",
                        "items": {
                            "type": "object",
                            "properties": {
                                "code": {
                                    "type": "integer",
                                    "minimum": -255,
                                    "maximum": 255
                                },
                                "next":{
                                    "type": "string",
                                    "enum": ["break", "continue"]
                                }
                            },
                            "required": [
                                "code",
                                "next"
                            ]
                        }
                    },
                    "default_next":{
                        "type": "string",
                        "enum": ["break", "continue"]
                    }
                },
                "required": [
                    "type",
                    "path",
```

```
                    "default_next"
                ]
            }
        }
    },
    "required": [
        "version",
        "actions"
    ]
}
```

Esempio del file manifesto

```
{
  "version": 1,
  "actions": [
    {
      "type": "execute",
      "path": "scripts/run1.cmd",
      "args": "testArg",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run2.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    },
    {
      "type": "execute",
      "path": "scripts/run3.cmd",
      "results": [
        {
          "code": 0,
          "next": "continue"
        }
      ],
      "default_next": "break"
    }
  ]
}
```

- L'archivio deve essere così strutturato:

  `manifest.json`

  `<file1>`

<file2>

<folder1>/<file3>

<folder2>/<folder3>/<file4>

...

<fileX>

manifest.json è il file manifesto dell'attività.

<file1>, ..., <fileX> è il set di file con gli script da eseguire.

Creazione di un pacchetto di installazione basato su un file manifesto

Per creare un pacchetto di installazione basato su un file manifesto:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.
   - Nel menu principale accedere a **Operazioni** → **Archivi** → **Pacchetti di installazione**.

   Verrà visualizzato un elenco dei pacchetti di installazione disponibili in Administration Server.

2. Fare clic su **Aggiungi**.

   Viene avviata la Creazione guidata nuovo pacchetto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Selezionare **Crea pacchetto di installazione per l'attività Esegui script da remoto basato su un archivio ZIP con il file manifest.json**.

4. Specificare il nome del pacchetto e fare clic sul pulsante **Sfoglia**.

   Nel browser verrà visualizzata una finestra standard **Apri** di Windows per la selezione di un file per creare il pacchetto di installazione.

5. Scegliere un file di archivio presente nei dischi disponibili. Le istruzioni per preparare un archivio per questa attività sono contenute in questo articolo.

   Il file inizia a essere caricato in Kaspersky Security Center Administration Server.

   Viene avviata la procedura per creare il pacchetto di installazione.

   La procedura guidata informa l'utente al termine della procedura.

   Se il pacchetto di installazione non viene creato, viene visualizzato un messaggio appropriato.

6. Fare clic sul pulsante **Fine** per chiudere la procedura guidata.

Il pacchetto di installazione creato viene scaricato nella sottocartella Pacchetti della cartella condivisa di Administration Server. Dopo il download, il pacchetto di installazione viene visualizzato nell'elenco dei pacchetti di installazione.

Nell'elenco dei pacchetti di installazione disponibili in Administration Server, è possibile fare clic sul collegamento con il nome di un pacchetto di installazione personalizzato per:

- Visualizzare le seguenti proprietà di un pacchetto di installazione:
  - **Nome.** Nome del pacchetto di installazione personalizzato.
  - **Origine.** Nome del produttore dell'applicazione.
  - **Versione.** Versione applicazione.
  - **Data creazione.** Data di creazione del pacchetto di installazione.
  - **Ultima modifica.** Data di modifica del pacchetto di installazione.
  - **Percorso.** Percorso del pacchetto di installazione personalizzato in Administration Server.
- Modificare il nome del pacchetto e i parametri della riga di comando. Questa funzionalità è disponibile solo per i pacchetti che non vengono creati in base alle applicazioni Kaspersky.

Gestione dei dispositivi client

Kaspersky Security Center consente di gestire i dispositivi client:

- Visualizzare impostazioni e stati dei dispositivi gestiti, inclusi cluster e array dei server.
- Configurare i punti di distribuzione.
- Gestire le attività.

È possibile utilizzare i gruppi di amministrazione per combinare i dispositivi client in un set che può essere gestito come singola unità. Un dispositivo client può essere incluso in un solo gruppo di amministrazione. I dispositivi possono essere allocati in un gruppo basato automaticamente sulle **Condizioni delle regole**:

- Creazione delle regole di spostamento dei dispositivi.
- Copia delle regole di spostamento dei dispositivi.
- Condizioni di una regola di spostamento dei dispositivi.

È possibile utilizzare selezioni dispositivi per filtrare i dispositivi in base a una condizione. È inoltre possibile eseguire il tagging dei dispositivi per creare selezioni, per trovare dispositivi e per distribuire dispositivi tra i gruppi di amministrazione.

Impostazioni di un dispositivo gestito

Per visualizzare le impostazioni di un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
   Verrà visualizzato l'elenco dei dispositivi gestiti.
2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo richiesto.

Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.

Nella parte superiore della finestra delle proprietà vengono visualizzate le seguenti schede che rappresentano i principali gruppi di impostazioni:

- Generale

Questa scheda comprende le seguenti sezioni:

- La sezione **Generale** visualizza informazioni generali sul dispositivo client. Le informazioni sono fornite in base ai dati ricevuti durante l'ultima sincronizzazione del dispositivo client con Administration Server:

  - Nome

    In questo campo è possibile visualizzare e modificare il nome di un dispositivo client nel gruppo di amministrazione.

  - Descrizione

    In questo campo è possibile immettere un'ulteriore descrizione di un dispositivo client.

  - Stato dispositivo

    Stato del dispositivo client assegnato in base ai criteri definiti dall'amministratore per lo stato della protezione anti-virus nel dispositivo e l'attività del dispositivo nella rete.

  - Nome completo del gruppo

    Gruppo di amministrazione che include il dispositivo client.

  - Ultimo aggiornamento dei database anti-virus

    Data dell'ultimo aggiornamento delle applicazioni o dei database anti-virus.

  - Connesso ad Administration Server

    Data e ora dell'ultima connessione del Network Agent installato nel dispositivo client ad Administration Server.

  - Ultima visibilità

    Data e ora in cui il dispositivo è risultato visibile nella rete per l'ultima volta.

  - Versione di Network Agent

    Versione del Network Agent installato.

  - Data creazione

    Data di creazione del dispositivo in Kaspersky Security Center.

  - Proprietario dispositivo

Nome del proprietario del dispositivo. È possibile assegnare o rimuovere un utente come proprietario del dispositivo facendo clic sul collegamento **Gestisci proprietario dispositivo**.

- **Non eseguire la disconnessione da Administration Server**

  Se questa opzione è abilitata, viene mantenuta una connessione continua tra il dispositivo gestito e Administration Server. È consigliabile utilizzare questa opzione se non si utilizzano server push, che offrono questo tipo di connettività.

  Se questa opzione è disabilitata e i server push non sono in uso, il dispositivo gestito si connette ad Administration Server solo per sincronizzare i dati o trasmettere le informazioni.

  Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

  Questa opzione è disabilitata per impostazione predefinita nei dispositivi gestiti. Questa opzione è abilitata per impostazione predefinita nel dispositivo in cui è installato Administration Server e rimane abilitata anche se si tenta di disabilitarla.

- La sezione **Rete** visualizza le seguenti informazioni sulle proprietà di rete del dispositivo client:
  - **Indirizzo IP**

    Indirizzo IP del dispositivo.

  - **Dominio Windows**

    Gruppo di lavoro o dominio Windows che contiene il dispositivo.

  - **Nome DNS**

    Nome del dominio DNS del dispositivo client.

  - **Nome NetBIOS**

    Nome di rete di Windows del dispositivo client.

  - **Indirizzo IPv6**

- La sezione **Sistema** fornisce le informazioni sul sistema operativo installato nel dispositivo client.
  - **Sistema operativo**
  - **Architettura della CPU**
  - **Nome dispositivo**
  - **Tipo di macchina virtuale**

    Produttore della macchina virtuale.

- **Macchina virtuale dinamica come parte di VDI**

  Questa riga mostra se il dispositivo client è una macchina virtuale dinamica come parte della VDI.

- Nella sezione **Protezione** vengono visualizzate le seguenti informazioni sullo stato corrente della protezione anti-virus nel dispositivo client:

  - **Visibile**

    Stato di visibilità del dispositivo client.

  - **Stato dispositivo**

    Stato del dispositivo client assegnato in base ai criteri definiti dall'amministratore per lo stato della protezione anti-virus nel dispositivo e l'attività del dispositivo nella rete.

  - **Descrizione stato**

    Stato della protezione del dispositivo client e della connessione ad Administration Server.

  - **Stato protezione**

    Questo campo indica lo stato corrente della protezione in tempo reale nel dispositivo client.

    Quando cambia lo stato del dispositivo, il nuovo stato viene visualizzato nella finestra delle proprietà del dispositivo solo dopo la sincronizzazione del dispositivo client con l'Administration Server.

  - **Ultima scansione completa**

    Data e ora dell'ultima scansione malware eseguita nel dispositivo client.

  - **Rilevato virus**

    Numero totale di minacce rilevate nel dispositivo client dall'installazione dell'applicazione di protezione (prima scansione) o dall'ultimo azzeramento del contatore delle minacce.

  - **Oggetti per cui la disinfezione non è riuscita**

    Numero di file non elaborati nel dispositivo client.

    Questo campo ignora il numero di file non elaborati nei dispositivi mobili.

  - **Stato criptaggio disco**

    Stato corrente del criptaggio dei file nelle unità locali del dispositivo. Per una descrizione degli stati consultare la Guida di Kaspersky Endpoint Security for Windows.

- La sezione **Stato dispositivo definito dall'applicazione** fornisce informazioni sullo stato del dispositivo definito dall'applicazione gestita installata nel dispositivo. Lo stato del dispositivo può essere diverso da quello definito da Kaspersky Security Center.

- Applicazioni

  Questa scheda elenca tutte le applicazioni Kaspersky installate nel dispositivo client. Questa scheda contiene i pulsanti **Avvia** e **Arresta** che consentono di avviare e arrestare l'applicazione Kaspersky selezionata (escluso Network Agent). È possibile usare questi pulsanti se la porta 15000 UDP è disponibile nei dispositivi gestiti per la ricezione delle notifiche push da Administration Server. Se il dispositivo gestito non è disponibile per le notifiche push, ma la modalità di connessione continua ad Administration Server è abilitata (l'opzione **Non eseguire la disconnessione da Administration Server** nella sezione **Generale** è abilitata), anche i pulsanti **Avvia** e **Arresta** sono disponibili. Altrimenti, quando si tenta di avviare o arrestare l'applicazione viene visualizzato un messaggio di errore. È inoltre possibile fare clic sul nome dell'applicazione per visualizzare informazioni generali sull'applicazione, un elenco di eventi che si sono verificati nel dispositivo e le impostazioni dell'applicazione.

- Criteri attivi e profili criterio

  In questa scheda, sono elencati i criteri e i profili criterio attualmente assegnato al dispositivo gestito.

- Attività

  Nella scheda **Attività**, è possibile gestire le attività dei dispositivi client: visualizzare l'elenco delle attività esistenti, creare nuove attività, rimuovere, avviare e arrestare le attività, modificare le relative impostazioni e visualizzare i risultati dell'esecuzione. L'elenco delle attività è basato sui dati ricevuti durante l'ultima sessione di sincronizzazione del client con Administration Server. Administration Server richiede i dettagli dello stato delle attività al dispositivo client. Se la porta 15000 UDP è disponibile nel dispositivo gestito per la ricezione delle notifiche push da Administration Server, lo stato dell'attività viene visualizzato e i pulsanti per la gestione delle attività sono abilitati. Se il dispositivo gestito non è disponibile per le notifiche push, ma la modalità di connessione continua ad Administration Server è abilitata (l'opzione **Non eseguire la disconnessione da Administration Server** nella sezione **Generale** è abilitata), anche le azioni con le attività sono disponibili.

  Se la connessione non viene stabilita, lo stato non viene visualizzato e i bottoni vengono disabilitati.

- Eventi

  Nella scheda **Eventi** sono visualizzati gli eventi registrati in Administration Server per il dispositivo client selezionato.

- Problemi di sicurezza

  Nella scheda **Problemi di sicurezza**, è possibile visualizzare, modificare e creare problemi di sicurezza per il dispositivo client. I problemi di sicurezza possono essere creati automaticamente, tramite le applicazioni gestite Kaspersky installate nel dispositivo client, o manualmente, dall'amministratore. Se ad esempio alcuni utenti trasferiscono regolarmente malware dalle proprie unità rimovibili nei dispositivi, l'amministratore può creare un problema di sicurezza. L'amministratore può fornire una breve descrizione del caso e le azioni consigliate (ad esempio, azioni disciplinari da intraprendere nei confronti di un utente) nel testo del problema di sicurezza e può aggiungere un collegamento per l'utente o gli utenti.

  Un problema di sicurezza per cui sono state eseguite tutte le azioni richieste viene definito *elaborato*. La presenza di problemi di sicurezza non elaborati può essere selezionata come condizione per il passaggio dello stato del dispositivo a *Critico* o *Avviso*.

  Questa sezione contiene un elenco dei problemi di sicurezza creati per il dispositivo. I problemi di sicurezza sono classificati in base al tipo e al livello di criticità. Il tipo di un problema di sicurezza è definito dall'applicazione Kaspersky che crea il problema di sicurezza. È possibile evidenziare i problemi di sicurezza elaborati nell'elenco selezionando la casella di controllo nella colonna **Trattati**.

- Tag

  Nella sezione **Tag** è possibile gestire l'elenco di parole chiave utilizzate per cercare i dispositivi client: visualizzare l'elenco dei tag esistenti, assegnare tag dall'elenco, configurare le regole per il tagging automatico, aggiungere nuovi tag e rinominare tag esistenti, nonché rimuovere tag.

- Avanzate

Questa scheda comprende le seguenti sezioni:

- **Registro delle applicazioni**. In questa sezione, è possibile visualizzare il registro delle applicazioni installate nel dispositivo client e i relativi aggiornamenti, nonché configurare la visualizzazione del registro delle applicazioni.

  Le informazioni sulle applicazioni installate vengono fornite se Network Agent installato nel dispositivo client invia le informazioni richieste ad Administration Server. È possibile configurare l'invio di informazioni ad Administration Server nella finestra delle proprietà di Network Agent o del relativo criterio, nella sezione **Archivi**.

  Facendo clic sul nome di un'applicazione, viene visualizzata una finestra che contiene i dettagli dell'applicazione e un elenco dei pacchetti di aggiornamento installati per l'applicazione.

- **File eseguibili**. In questa sezione sono visualizzati i file eseguibili rilevati nel dispositivo client.

- **Punti di distribuzione**. In questa sezione viene fornito un elenco dei punti di distribuzione con cui interagisce il dispositivo.

  - **Esporta in un file**

    Fare clic sul pulsante **Esporta in un file** per salvare in un file un elenco di punti di distribuzione con cui interagisce il dispositivo. Per impostazione predefinita, l'applicazione esporta l'elenco di dispositivi in un file CSV.

  - **Proprietà**

    Fare clic sul pulsante **Proprietà** per visualizzare e configurare il punto di distribuzione con cui interagisce il dispositivo.

- **Registro hardware**. In questa sezione è possibile visualizzare le informazioni relative all'hardware installato nel dispositivo client.

  Se Network Agent è installato in un dispositivo che esegue Windows, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo:

  - RAM
  - Dispositivi di archiviazione di massa
  - Scheda madre
  - CPU
  - Schede di rete
  - Monitor
  - Scheda video
  - Scheda audio

  Se Network Agent è installato in un dispositivo che esegue Linux o macOS, invia ad Administration Server le seguenti informazioni sull'hardware del dispositivo, se tali informazioni sono fornite dal sistema operativo:

- Volume totale RAM
- Volume totale dei dispositivi di archiviazione di massa
- Scheda madre
- CPU
- Schede di rete

- **Aggiornamenti disponibili**. Questa sezione visualizza un elenco degli aggiornamenti software rilevati nel dispositivo, ma non ancora installati.

- **Vulnerabilità del software**. In questa sezione, sono fornite informazioni sulle vulnerabilità delle applicazioni di terze parti installate nei dispositivi client.

  Per salvare le vulnerabilità in un file, selezionare le caselle di controllo accanto alle vulnerabilità che si desidera salvare, quindi fare clic sul pulsante **Esporta in CSV** o sul pulsante **Esporta in TXT**.

  Questa sezione contiene le seguenti impostazioni:

  - **Mostra solo le vulnerabilità che possono essere risolte**

    Se questa opzione è abilitata, nella sezione verranno visualizzate le vulnerabilità che è possibile correggere tramite una patch.

    Se questa opzione è disabilitata, nella sezione verranno visualizzate sia le vulnerabilità che è possibile correggere tramite una patch che quelle per cui non è disponibile alcuna patch.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Proprietà vulnerabilità**

    Fare clic sul nome di una vulnerabilità del software nell'elenco per visualizzare le proprietà della vulnerabilità del software selezionata in una finestra separata. Nella finestra è possibile eseguire le seguenti operazioni:

    - Ignorare la vulnerabilità del software in questo dispositivo gestito (in Administration Console o in Kaspersky Security Center Web Console).
    - Visualizzare l'elenco delle correzioni consigliate per la vulnerabilità.
    - Specificare manualmente gli aggiornamenti software per correggere la vulnerabilità (in Administration Console o in Kaspersky Security Center Web Console).
    - Visualizzare le istanze della vulnerabilità.
    - Visualizzare l'elenco delle attività esistenti per correggere la vulnerabilità e creare nuove attività per correggere la vulnerabilità.

- **Diagnostica remota**. In questa sezione, è possibile eseguire la diagnostica remota dei dispositivi client.

Se si utilizza un DBMS PostgreSQL, MariaDB o MySQL, la scheda **Eventi** potrebbe mostrare un elenco incompleto di eventi per il dispositivo client selezionato. Questo si verifica quando il DBMS archivia una quantità molto elevata di eventi. È possibile aumentare il numero di eventi visualizzati effettuando una delle seguenti operazioni:

- Rimozione degli eventi non necessari.
- Riduzione del periodo di archiviazione per gli eventi non necessari.

Per visualizzare un elenco completo degli eventi registrati in Administration Server per il dispositivo, utilizzare Rapporti.

Creazione dei gruppi di amministrazione

Subito dopo l'installazione di Kaspersky Security Center, la gerarchia dei gruppi di amministrazione contiene un solo gruppo di amministrazione, denominato **Dispositivi gestiti**. Durante la creazione di una gerarchia di gruppi di amministrazione è possibile aggiungere dispositivi, incluse le macchine virtuali, al gruppo **Dispositivi gestiti**, nonché aggiungere gruppi nidificati (vedere la figura di seguito).



Visualizzazione della gerarchia di gruppi di amministrazione

Per creare un gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nella struttura di gruppi di amministrazione selezionare il gruppo di amministrazione che deve includere il nuovo gruppo di amministrazione.
3. Fare clic sul pulsante **Aggiungi**.
4. Nella finestra **Nome del nuovo gruppo di amministrazione** visualizzata immettere un nome per il gruppo, quindi fare clic sul pulsante **Aggiungi**.

   Un nuovo gruppo di amministrazione con il nome specificato viene visualizzato nella gerarchia dei gruppi di amministrazione.

L'applicazione consente di creare una gerarchia di gruppi di amministrazione basata sulla struttura di Active Directory o sulla struttura della rete di dominio. È inoltre possibile creare una struttura di gruppi a partire da un file di testo.

Per creare una struttura di gruppi di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Fare clic sul pulsante **Importa**.

Verrà avviata la Creazione guidata nuova struttura dei gruppi di amministrazione. Seguire le istruzioni della procedura guidata.

Aggiunta manuale dei dispositivi a un gruppo di amministrazione

È possibile spostare automaticamente i dispositivi nei gruppi di amministrazione creando regole di spostamento dei dispositivi o manualmente spostando i dispositivi da un gruppo di amministrazione a un altro oppure aggiungendo dispositivi a un gruppo di amministrazione selezionato. Questa sezione descrive come aggiungere manualmente i dispositivi a un gruppo di amministrazione.

Per aggiungere manualmente uno o più dispositivi a un gruppo di amministrazione selezionato:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul collegamento **Percorso corrente:** `<percorso corrente>` sopra l'elenco.
3. Nella finestra visualizzata selezionare il gruppo di amministrazione al quale si desidera aggiungere i dispositivi.
4. Fare clic sul pulsante **Aggiungi dispositivi**.
   Verrà avviato lo Spostamento guidato dispositivi.
5. Creare un elenco dei dispositivi che si desidera aggiungere al gruppo di amministrazione.

   > È possibile aggiungere solo i dispositivi per cui sono già state aggiunte informazioni al database di Administration Server durante la connessione del dispositivo o dopo la device discovery.

   Selezionare il modo in cui aggiungere dispositivi all'elenco:

   - Fare clic sul pulsante **Aggiungi dispositivi** e specificare i dispositivi in uno dei seguenti modi:
     - Selezionare i dispositivi dall'elenco dei dispositivi rilevati da Administration Server.
     - Specificare l'indirizzo IP o l'intervallo IP di un dispositivo.

       > L'intervallo IP non deve contenere più di 1.048.576 indirizzi.

     - Specificare il nome NetBIOS o il nome DNS di un dispositivo.

       > Il campo relativo al nome del dispositivo non deve contenere né spazi né i seguenti caratteri proibiti: \ / * : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

   - Fare clic sul pulsante **Importa dispositivi da file** per importare un elenco di dispositivi da un file .txt. È necessario specificare il nome o l'indirizzo di ciascun dispositivo in una riga separata.

     > Il file non deve contenere né spazi né i seguenti caratteri proibiti: \ / * : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. Visualizzare l'elenco dei dispositivi da aggiungere al gruppo di amministrazione. È possibile modificare l'elenco aggiungendo o rimuovendo i dispositivi.

7. Dopo essersi accertati che l'elenco è corretto, fare clic sul pulsante **Avanti**.

La procedura guidata elabora l'elenco dei dispositivi e visualizza il risultato. I dispositivi elaborati correttamente vengono aggiunti al gruppo di amministrazione e visualizzati nell'elenco dei dispositivi con i nomi generati da Administration Server.

Spostamento manuale dei dispositivi o dei cluster in un gruppo di amministrazione

È possibile spostare i dispositivi da un gruppo di amministrazione a un altro o dal gruppo dei dispositivi non assegnati a un gruppo di amministrazione.

È anche possibile spostare cluster o array di server da un gruppo di amministrazione all'altro. Quando si sposta un cluster o un array di server in un altro gruppo, tutti i suoi nodi vengono spostati con esso, perché un cluster e uno qualsiasi dei suoi nodi appartengono sempre allo stesso gruppo di amministrazione. Quando si seleziona un singolo nodo del cluster nella scheda **Dispositivi**, il pulsante **Sposta nel gruppo** diventa non disponibile.

Per spostare uno o più dispositivi o cluster in un gruppo di amministrazione selezionato:

1. Aprire il gruppo di amministrazione da cui si desidera spostare i dispositivi. A tale scopo, eseguire una delle operazioni seguenti:

   - Per aprire un gruppo di amministrazione, nel menu principale, accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**, fare clic sul collegamento al percorso nel campo **Percorso corrente** e selezionare un gruppo di amministrazione nel riquadro a sinistra che si apre.

   - Per aprire il gruppo **Dispositivi non assegnati**, nel menu principale passare a **Individuazione e distribuzione** → **Dispositivi non assegnati**.

2. Se il gruppo di amministrazione contiene cluster o array di server, la sezione **Dispositivi gestiti** è divisa in due schede: la scheda **Dispositivi** e la scheda **Cluster e array di server**. Aprire la scheda dell'oggetto che si desidera spostare.

3. Selezionare le caselle di controllo accanto ai dispositivi o ai cluster che si desidera spostare in un altro gruppo.

4. Fare clic sul pulsante **Sposta nel gruppo**.

5. Nella gerarchia dei gruppi di amministrazione, selezionare la casella di controllo accanto al gruppo di amministrazione in cui si desidera spostare i dispositivi o i cluster selezionati.

6. Fare clic sul pulsante **Sposta**.

I dispositivi o i cluster selezionati verranno spostati nel gruppo di amministrazione selezionato.

Creazione delle regole di spostamento dei dispositivi

È possibile impostare regole di spostamento dei dispositivi, ovvero regole che allocano automaticamente i dispositivi ai gruppi di amministrazione.

Per creare una regola di spostamento:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Regole di spostamento**.
2. Fare clic su **Aggiungi**.
3. Nella finestra visualizzata specificare le seguenti impostazioni nella scheda **Generale**:

   - Nome regola

     Immettere un nome per la nuova regola.

     Se si sta copiando una regola, alla nuova regola è assegnato lo stesso nome della regola di origine, ma al nome viene aggiunto un indice in formato (), ad esempio: (1).

   - Gruppo di amministrazione

     Selezionare il gruppo di amministrazione in cui devono essere spostati automaticamente i dispositivi.

   - Regola attiva

     Se questa opzione è abilitata, la regola è abilitata e inizia a funzionare dopo il salvataggio.

     Se questa opzione è disabilitata, la regola viene creata, ma non abilitata. Non funzionerà finché non si abilita questa opzione.

   - Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione

     Se questa opzione è abilitata, solo i dispositivi non assegnati verranno spostati nel gruppo selezionato.

     Se questa opzione è disabilitata, i dispositivi che appartengono già ad altri gruppi di amministrazione, nonché i dispositivi non assegnati, verranno spostati nel gruppo selezionato.

   - Applica regola

     È possibile selezionare una delle seguenti opzioni:

     - **Esegui una volta per ciascun dispositivo**

       La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri.

     - **Esegui una volta per ciascun dispositivo, quindi a ogni reinstallazione di Network Agent**

       La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri, quindi solo quando Network Agent viene reinstallato in questi dispositivi.

     - **Applica regola in modo continuativo**

       La regola viene applicata in base alla pianificazione impostata automaticamente da Administration Server (in genere, con una frequenza di alcune ore).

4. Nella scheda **Condizioni delle regole**, specificare almeno un criterio in base al quale i dispositivi vengono spostati in un gruppo di amministrazione.
5. Fare clic su **Salva**.

Verrà creata la regola di spostamento. La regola è visualizzata nell'elenco delle regole di spostamento.

Maggiore è la posizione nell'elenco, maggiore sarà la priorità della regola. Per aumentare o diminuire la priorità di una regola di spostamento, spostare la regola rispettivamente in alto o in basso nell'elenco utilizzando il mouse.

Se l'opzione **Applica regola in modo continuativo** è selezionata, la regola di spostamento viene applicata indipendentemente dalle impostazioni di priorità. Tali regole vengono applicate in base alla pianificazione impostata automaticamente da Administration Server.

Se gli attributi del dispositivo soddisfano le condizioni di più regole, il dispositivo viene spostato nel gruppo di destinazione della regola con la priorità più alta (al livello più alto nell'elenco delle regole).

Copia delle regole di spostamento dei dispositivi

È possibile copiare le regole di spostamento, ad esempio se si desidera disporre di più regole identiche per diversi gruppi di amministrazione di destinazione.

Per copiare una regola di spostamento esistente:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale accedere a **Risorse (dispositivi)** → **Regole di spostamento**.
   - Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Regole di spostamento**.

   Verrà visualizzato l'elenco delle regole di spostamento.

2. Selezionare la casella di controllo accanto alla regola da copiare.
3. Fare clic su **Copia**.

4. Nella finestra visualizzata modificare le seguenti informazioni nella scheda **Generale** (o non apportare modifiche se si desidera solo copiare la regola senza modificarne le impostazioni):

   - Nome regola

     Immettere un nome per la nuova regola.

     Se si sta copiando una regola, alla nuova regola è assegnato lo stesso nome della regola di origine, ma al nome viene aggiunto un indice in formato (), ad esempio: (1).

   - Gruppo di amministrazione

     Selezionare il gruppo di amministrazione in cui devono essere spostati automaticamente i dispositivi.

   - Regola attiva

     Se questa opzione è abilitata, la regola è abilitata e inizia a funzionare dopo il salvataggio.

     Se questa opzione è disabilitata, la regola viene creata, ma non abilitata. Non funzionerà finché non si abilita questa opzione.

   - Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione

     Se questa opzione è abilitata, solo i dispositivi non assegnati verranno spostati nel gruppo selezionato.

     Se questa opzione è disabilitata, i dispositivi che appartengono già ad altri gruppi di amministrazione, nonché i dispositivi non assegnati, verranno spostati nel gruppo selezionato.

   - Applica regola

     È possibile selezionare una delle seguenti opzioni:

     - **Esegui una volta per ciascun dispositivo**

       La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri.

     - **Esegui una volta per ciascun dispositivo, quindi a ogni reinstallazione di Network Agent**

       La regola viene applicata una volta per ogni dispositivo che corrisponde ai criteri, quindi solo quando Network Agent viene reinstallato in questi dispositivi.

     - **Applica regola in modo continuativo**

       La regola viene applicata in base alla pianificazione impostata automaticamente da Administration Server (in genere, con una frequenza di alcune ore).

5. Nella scheda **Condizioni delle regole**, specificare almeno un criterio per i dispositivi che si desidera spostare automaticamente.

6. Fare clic su **Salva**.

Verrà creata la nuova regola di spostamento. La regola è visualizzata nell'elenco delle regole di spostamento.

Condizioni di una regola di spostamento dei dispositivi

Quando si crea o copia una regola per spostare i dispositivi client nei gruppi di amministrazione, nella scheda **Condizioni delle regole** si impostano le condizioni per lo spostamento dei dispositivi. Per determinare quali dispositivi spostare, è possibile utilizzare i seguenti criteri:

- Tag assegnati ai dispositivi client.
- Parametri di rete. Ad esempio, è possibile spostare dispositivi con indirizzi IP da un intervallo specificato.
- Applicazioni gestite installate nei dispositivi client, ad esempio Network Agent o Administration Server.
- Macchine virtuali, che sono i dispositivi client.
- Informazioni sull'unità organizzativa di Active Directory con i dispositivi client.
- Informazioni su un segmento cloud con i dispositivi client.

Di seguito è possibile trovare la descrizione su come specificare queste informazioni in una regola di spostamento dei dispositivi.

Se si specificano più condizioni nella regola, l'operatore logico AND funziona e tutte le condizioni si applicano contemporaneamente. Se non si seleziona alcuna opzione o alcuni campi vengono lasciati vuoti, tali condizioni non si applicano.

Scheda Tag

Nella scheda, è possibile configurare una regola di spostamento dei dispositivi in base ai tag dei dispositivi aggiunti in precedenza alle descrizioni dei dispositivi client. A tale scopo, selezionare i tag richiesti. Inoltre, è possibile abilitare le seguenti opzioni:

- **Applica ai dispositivi senza i tag specificati**

  Se questa opzione è abilitata, tutti i dispositivi con i tag specificati vengono esclusi da una regola di spostamento dei dispositivi. Se questa opzione è disabilitata, la regola di spostamento dei dispositivi si applica ai dispositivi con tutti i tag selezionati.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Applica se almeno uno dei tag specificati corrisponde**

  Se questa opzione è abilitata, una regola di spostamento dei dispositivi si applica ai dispositivi client con almeno uno dei tag selezionati. Se questa opzione è disabilitata, la regola di spostamento dei dispositivi si applica ai dispositivi con tutti i tag selezionati.

  Per impostazione predefinita, questa opzione è disabilitata.

Scheda Rete

In questa scheda, è possibile specificare i dati di rete dei dispositivi considerati da una regola di spostamento dei dispositivi:

- **Nome dispositivo nella rete Windows**

  Nome di rete Windows (nome NetBIOS) del dispositivo o indirizzo IPv4 o IPv6.

- **Dominio Windows**

  Una regola di spostamento dei dispositivi si applica a tutti i dispositivi inclusi nel dominio Windows specificato.

- **Nome DNS del dispositivo**

  Nome dominio DNS del dispositivo client che si desidera spostare. Compilare questo campo se la rete include un server DNS.

  Se per il database utilizzato per Kaspersky Security Center sono impostate regole di confronto con distinzione tra maiuscole e minuscole, mantenere le maiuscole e le minuscole quando si specifica un nome DNS del dispositivo. In caso contrario, la regola di spostamento del dispositivo non funzionerà.

- **Dominio DNS**

  Una regola di spostamento dei dispositivi si applica a tutti i dispositivi inclusi nel suffisso DNS principale specificato. Compilare questo campo se la rete include un server DNS.

- **Intervallo IP**

  Se questa opzione è abilitata, è possibile immettere gli indirizzi IP iniziale e finale dell'intervallo IP in cui i dispositivi rilevanti devono essere inclusi.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Indirizzo IP per la connessione ad Administration Server**

  Se questa opzione è abilitata, è possibile impostare gli indirizzi IP tramite i quali i dispositivi client sono collegati all'Administration Server. A tale scopo, specificare l'intervallo IP che include tutti gli indirizzi IP necessari.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Il dispositivo si trova nell'intervallo IP**

  Se questa opzione è abilitata, è possibile selezionare un intervallo IP aggiunto in precedenza nella sezione **Intervalli IP**. I dispositivi interessati devono essere inclusi nell'intervallo IP selezionato.

  Per impostazione predefinita, questa opzione è disabilitata.

- Profilo connessione modificato

  Selezionare uno dei seguenti valori:

  - **Sì**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi client con un profilo di connessione modificato.
  - **No**. La regola di spostamento dei dispositivi si applica solo ai dispositivi client il cui profilo di connessione non è cambiato.
  - **Nessun valore selezionato**. La condizione non si applica.

- Gestito da un altro Administration Server

  Selezionare uno dei seguenti valori:

  - **Sì**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti da altri Administration Server. Questi server sono diversi dal server su cui si configura la regola di spostamento dei dispositivi.
  - **No**. La regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti dall'Administration Server corrente.
  - **Nessun valore selezionato**. La condizione non si applica.

Scheda Applicazioni

In questa scheda, è possibile configurare una regola di spostamento dei dispositivi in base alle applicazioni gestite e ai sistemi operativi installati nei dispositivi client:

- Network Agent installato

  Selezionare uno dei seguenti valori:

  - **Sì**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi client con Network Agent installato.
  - **No**. La regola di spostamento dei dispositivi si applica solo ai dispositivi client in cui Network Agent non è installato.
  - **Nessun valore selezionato**. La condizione non si applica.

- Applicazioni

  Specificare quali applicazioni gestite devono essere installate nei dispositivi client, in modo da applicare una regola di spostamento dei dispositivi a tali dispositivi. Ad esempio, è possibile selezionare **Kaspersky Security Center 15.1 Network Agent** o **Kaspersky Security Center 15.1 Administration Server**.

  Se non si seleziona alcuna applicazione gestita, la condizione non si applica.

- Versione del sistema operativo

  È possibile eliminare i dispositivi client in base alla versione del sistema operativo. A tale scopo, specificare i sistemi operativi che devono essere installati nei dispositivi client. Di conseguenza, una regola di spostamento dei dispositivi si applica ai dispositivi client con i sistemi operativi selezionati.

  Se questa opzione non viene abilitata, la condizione non si applica. Per impostazione predefinita, l'opzione è disabilitata.

- Dimensioni in bit del sistema operativo

  È possibile selezionare i dispositivi client in base alle dimensioni in bit del sistema operativo. Nel campo **Dimensioni in bit del sistema operativo**, è possibile selezionare uno dei seguenti valori:

  - **Sconosciuto**
  - **x86**
  - **AMD64**
  - **IA64**

  Per controllare le dimensioni in bit del sistema operativo dei dispositivi client:

  1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
  2. Fare clic sul pulsante **Impostazioni colonne** (⚙) a destra.
  3. Selezionare l'opzione **Dimensioni in bit del sistema operativo**, quindi fare clic sul pulsante **Salva**.

     Successivamente, vengono visualizzate le dimensioni in bit del sistema operativo di ogni dispositivo gestito.

- Versione Service Pack del sistema operativo

  In questo campo è possibile specificare la versione del pacchetto del sistema operativo (nel formato *X.Y*), da cui dipenderà l'applicazione della regola di spostamento al dispositivo. Per impostazione predefinita, non è specificato alcun valore per la versione.

- Certificato utente

  Selezionare uno dei seguenti valori:

  - **Installato**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi mobili con un certificato mobile.
  - **Non installato**. La regola di spostamento dei dispositivi si applica solo ai dispositivi mobili senza un certificato mobile.
  - **Nessun valore selezionato**. La condizione non si applica.

- **Build del sistema operativo**

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  È possibile specificare se il sistema operativo selezionato deve avere un numero di build uguale, precedente o successivo. È inoltre possibile configurare una regola di spostamento dei dispositivi per tutti i numeri di build ad eccezione di quello specificato.

- **Numero di rilascio del sistema operativo**

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  È possibile specificare se il sistema operativo selezionato deve avere un numero di rilascio uguale, precedente o successivo. È inoltre possibile configurare una regola di spostamento dei dispositivi per tutti i numeri di rilascio ad eccezione di quello specificato.

Scheda Macchine virtuali

In questa scheda, è possibile configurare una regola di spostamento dei dispositivi a seconda che i dispositivi client siano macchine virtuali o facciano parte di una VDI (Virtual Desktop Infrastructure):

- **Questa è una macchina virtuale**

  Nell'elenco a discesa, è possibile selezionare una delle seguenti opzioni:
  - **N/D**. La condizione non si applica.
  - **No**. I dispositivi che non sono macchine virtuali vengono spostati.
  - **Sì**. I dispositivi che sono macchine virtuali vengono spostati.

- **Tipo di macchina virtuale**

- **Parte di Virtual Desktop Infrastructure**

  Nell'elenco a discesa, è possibile selezionare una delle seguenti opzioni:
  - **N/D**. La condizione non si applica.
  - **No**. I dispositivi che non fanno parte della VDI vengono spostati.
  - **Sì**. I dispositivi che fanno parte della VDI vengono spostati.

Scheda Controller di dominio

In questa scheda, è possibile specificare che è necessario spostare i dispositivi inclusi nell'unità organizzativa del dominio. È inoltre possibile spostare i dispositivi da tutte le unità organizzative secondarie dell'unità organizzativa del dominio specificato:

- **Il dispositivo è incluso nella seguente unità organizzativa**

  Se questa opzione è abilitata, viene applicata una regola di spostamento dei dispositivi ai dispositivi dell'unità organizzativa di dominio specificato nell'elenco sotto l'opzione.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Includi unità organizzative secondarie**

  Se questa opzione è abilitata, la selezione includerà i dispositivi in tutte le unità organizzative secondarie dell'unità organizzativa del dominio specificato.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Sposta i dispositivi dalle unità figlio ai sottogruppi corrispondenti**
- **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati**
- **Elimina sottogruppi non presenti nel dominio**
- **Il dispositivo è incluso nel seguente gruppo di sicurezza del dominio**

  Se questa opzione è abilitata, viene applicata una regola di spostamento dei dispositivi ai dispositivi del gruppo di protezione dei domini specificata nell'elenco sotto l'opzione.

  Per impostazione predefinita, questa opzione è disabilitata.

Scheda Segmenti cloud

In questa scheda, è possibile specificare che è necessario spostare i dispositivi che appartengono a specifici segmenti cloud:

- **Il dispositivo si trova in un segmento cloud**

  Se si seleziona questa opzione, viene applicata una regola di spostamento del dispositivo ai dispositivi client che appartengono a un segmento cloud. È possibile selezionare il segmento cloud richiesto fino a una sottorete nell'elenco sotto l'opzione.

  Per impostazione predefinita, l'opzione è disabilitata.

- **Includi gli oggetti figlio**

  Se si seleziona questa opzione, viene applicata una regola di spostamento del dispositivo non solo al segmento cloud selezionato, ma anche agli oggetti secondari di questo segmento.

  Per impostazione predefinita, l'opzione è disabilitata.

- **Sposta i dispositivi dagli oggetti nidificati nei sottogruppi corrispondenti**
- **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati**
- **Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud**
- **Dispositivo rilevato tramite l'API**

  Nell'elenco a discesa, è possibile selezionare se un dispositivo deve essere rilevato o meno dagli strumenti API:

  - **AWS**. Il dispositivo viene rilevato tramite l'API AWS, quindi si trova senz'altro nell'ambiente cloud AWS.
  - **Azure**. Il dispositivo viene rilevato tramite l'API Azure, quindi si trova senz'altro nell'ambiente cloud Azure.
  - **Google Cloud.** Il dispositivo viene rilevato tramite l'API Google, quindi si trova senz'altro nell'ambiente cloud Google.
  - **No**. Il dispositivo non può essere rilevato tramite l'API AWS, Azure o Google, ad esempio perché si trova all'esterno dell'ambiente cloud oppure si trova nell'ambiente cloud ma non può essere rilevato tramite un'API.
  - **Nessun valore**. Questa condizione non viene applicata.

Informazioni sui cluster e sugli array di server

Kaspersky Security Center supporta la tecnologia cluster. Se Network Agent invia ad Administration Server informazioni che confermano che l'applicazione installata in un dispositivo client fa parte di un array di server, il dispositivo client diventa un nodo del cluster.

Se un gruppo di amministrazione contiene cluster o array di server, la pagina **Dispositivi gestiti** mostra due schede: una per i singoli dispositivi e una per i cluster e gli array di server. Dopo che i dispositivi gestiti vengono rilevati come nodi del cluster, il cluster viene aggiunto come oggetto singolo alla scheda **Cluster e array di server**.

I nodi del cluster o dell'array di server sono elencati nella scheda **Dispositivi**, insieme ad altri dispositivi gestiti. È possibile visualizzare le proprietà dei nodi come dispositivi singoli ed eseguire altre operazioni, ma non è possibile eliminare un nodo del cluster o spostarlo in un altro gruppo di amministrazione separatamente dal relativo cluster. È solo possibile eliminare o spostare un intero cluster.

È possibile eseguire le seguenti operazioni con cluster o array di server:

- Visualizzare le proprietà
- Spostare il cluster o l'array di server in un altro gruppo di amministrazione

  Quando si sposta un cluster o un array di server in un altro gruppo, tutti i suoi nodi vengono spostati con esso, perché un cluster e uno qualsiasi dei suoi nodi appartengono sempre allo stesso gruppo di amministrazione.
- Elimina

  È ragionevole eliminare un cluster o un array di server solo quando il cluster o l'array di server non esiste più nella rete dell'organizzazione. Se un cluster è ancora visibile nella rete e Network Agent e l'applicazione di protezione Kaspersky sono ancora installati nei nodi del cluster, Kaspersky Security Center restituisce automaticamente il cluster eliminato e i relativi nodi all'elenco dei dispositivi gestiti.

Proprietà di un cluster o di un array di server

Per visualizzare le impostazioni di un cluster o di un array di server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti** → **Cluster e array di server**.
   Viene visualizzato l'elenco dei cluster e degli array di server.
2. Fare clic sul nome del cluster o dell'array di server richiesto.

Verrà visualizzata la finestra delle proprietà del cluster o dell'array di server selezionato.

Generale

La sezione **Generale** mostra informazioni generali sul cluster o sull'array di server. Le informazioni sono fornite in base ai dati ricevuti durante l'ultima sincronizzazione dei nodi del cluster con Administration Server:

- **Nome**
- **Descrizione**
- Dominio Windows

  Dominio o gruppo di lavoro di Windows, che contiene il cluster o l'array di server.

- Nome NetBIOS

  Nome di rete Windows del cluster o dell'array di server.

- Nome DNS

  Nome del dominio DNS del cluster o dell'array di server.

Attività

Nella scheda **Attività**, è possibile gestire le attività assegnate al cluster o all'array di server: visualizzare l'elenco delle attività esistenti, creare nuove attività, rimuovere, avviare e arrestare le attività, modificare le impostazioni delle attività e visualizzare i risultati dell'esecuzione. Le attività elencate si riferiscono all'applicazione di protezione Kaspersky installata nei nodi del cluster. Kaspersky Security Center riceve l'elenco delle attività e i dettagli sullo stato delle attività dai nodi del cluster. Se non viene stabilita una connessione, lo stato non viene visualizzato.

Nodi

Questa scheda mostra un elenco di nodi inclusi nel cluster o nell'array di server. È possibile fare clic sul nome di un nodo per visualizzare la finestra delle proprietà del dispositivo.

Applicazione Kaspersky

La finestra delle proprietà può contenere anche schede aggiuntive con le informazioni e le impostazioni relative all'applicazione di protezione Kaspersky installata nei nodi del cluster.

Visualizzazione e configurazione delle azioni per i dispositivi inattivi

È possibile ottenere notifiche relative ai dispositivi client all'interno di un gruppo che risultano inattivi. È anche possibile eliminare automaticamente tali dispositivi.

Per visualizzare o configurare le azioni eseguite quando i dispositivi nel gruppo risultano inattivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Fare clic sul nome del gruppo di amministrazione desiderato.

   Verrà visualizzata la finestra delle proprietà dal gruppo di amministrazione.
3. Nella finestra delle proprietà passare alla scheda **Impostazioni**.
4. Nella sezione **Ereditarietà** abilitare o disabilitare le seguenti opzioni:

   - **Eredita da gruppo padre**

     Le impostazioni di questa sezione saranno ereditate dal gruppo padre di cui fa parte il dispositivo client. Se questa opzione è abilitata, le impostazioni in **Attività dei dispositivi nella rete** sono bloccate dalle modifiche.

     Questa opzione è disponibile solo se il gruppo di amministrazione ha un gruppo padre.

     Per impostazione predefinita, questa opzione è abilitata.

   - **Forza ereditarietà delle impostazioni nei gruppi figlio**

     I valori delle impostazioni vengono distribuiti ai gruppi figlio, ma nelle proprietà dei gruppi figlio tali impostazioni sono bloccate.

     Per impostazione predefinita, questa opzione è disabilitata.

5. Nella sezione **Attività dei dispositivi** abilitare o disabilitare le seguenti opzioni:

- **Avvisa l'amministratore se il dispositivo è inattivo da più di (giorni)**

  Se questa opzione è abilitata, l'amministratore riceve le notifiche sui dispositivi inattivi. È possibile specificare l'intervallo di tempo al termine del quale verrà creato l'evento **Il dispositivo risulta inattivo nella rete da molto tempo**. L'intervallo di tempo predefinito è 7 giorni.

  Per impostazione predefinita, questa opzione è abilitata.

- **Rimuovi il dispositivo dal gruppo se è inattivo da più di (giorni)**

  Se questa opzione è abilitata, è possibile specificare l'intervallo di tempo al termine del quale il dispositivo viene rimosso automaticamente dal gruppo. L'intervallo di tempo predefinito è 60 giorni.

  Per impostazione predefinita, questa opzione è abilitata.

6. Fare clic su **Salva**.

Le modifiche verranno salvate e applicate.

Informazioni sugli stati dei dispositivi

Kaspersky Security Center assegna uno stato a ciascun dispositivo gestito. Lo stato specifico dipende dal rispetto delle condizioni definite dall'utente. In alcuni casi, durante l'assegnazione di uno stato a un dispositivo, Kaspersky Security Center prende in considerazione il flag di visibilità del dispositivo nella rete (vedere la tabella seguente). Ad esempio, se a un dispositivo gestito è stato assegnato lo stato *Critico* perché è stata soddisfatta la condizione *I database non sono aggiornati* e successivamente è stato impostato il flag di visibilità per il dispositivo, al dispositivo viene assegnato lo stato *OK*. Se Kaspersky Security Center non rileva un dispositivo nella rete entro due ore, il flag di visibilità del dispositivo è impostato su *Non visibile*.

Gli stati sono i seguenti:

- *Critico* o *Critico / Visibile*
- *Avviso* o *Avviso / Visibile*
- *OK* o *OK / Visibile*

La tabella seguente elenca le condizioni predefinite da soddisfare per assegnare a un dispositivo lo stato *Critico* o *Avviso*, con tutti i possibili valori.

Condizioni per l'assegnazione di uno stato a un dispositivo

Condizione	Descrizione della condizione	Valori disponibili
Applicazione di protezione non installata	Network Agent è installato nel dispositivo, ma un'applicazione di protezione non è installata.	• L'interruttore è attivato. • L'interruttore è disattivato.
Troppi virus rilevati	Nel dispositivo sono stati rilevati alcuni virus da parte di un'attività per il rilevamento dei virus, ad esempio l'attività *Scansione malware*, e il numero di virus trovati supera il valore specificato.	Più di 0.

Condizione	Descrizione della condizione	Valori disponibili
Livello protezione in tempo reale diverso da quello impostato dall'amministratore	Il dispositivo è visibile nella rete, ma il livello della protezione in tempo reale è diverso dal livello impostato (nella condizione) dall'amministratore per lo stato del dispositivo.	• Arrestata. • Sospesa. • In esecuzione.
Scansione malware non eseguita da molto tempo	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma né l'attività *Scansione malware* né un'attività di scansione locale sono state eseguite nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server 7 giorni o più di 7 giorni prima.	Più di 1 giorno.
I database non sono aggiornati	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma i database anti-virus non vengono aggiornati nel dispositivo nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server un giorno o più di un giorno prima.	Più di 1 giorno.
Connessione non eseguita da molto tempo	Network Agent è installato nel dispositivo, ma il dispositivo non viene connesso a un Administration Server nell'intervallo di tempo specificato, perché il dispositivo era spento.	Più di 1 giorno.
Rilevate minacce attive	Il numero di oggetti non elaborati nella cartella **Minacce attive** è superiore al valore specificato.	Più di 0 elementi.
È necessario il riavvio	Il dispositivo è visibile nella rete, ma un'applicazione richiede il riavvio del dispositivo da un periodo superiore all'intervallo di tempo specificato e per uno dei motivi selezionati.	Più di 0 minuti.
Applicazioni incompatibili installate	Il dispositivo è visibile nella rete, ma l'inventario software eseguito tramite Network Agent ha rilevato applicazioni incompatibili installate nel dispositivo.	• L'interruttore è disattivato. • L'interruttore è attivato.
Rilevate vulnerabilità del software	Il dispositivo è visibile nella rete e Network Agent è installato nel dispositivo, ma l'attività *Trova vulnerabilità e aggiornamenti richiesti* ha rilevato vulnerabilità con il livello di criticità specificato nelle applicazioni installate nel dispositivo.	• Critico. • Alto. • Medio. • Ignora se non è possibile correggere il tipo di vulnerabilità. • Ignora se un aggiornamento è assegnato per l'installazione.
La licenza è scaduta	Il dispositivo è visibile nella rete, ma la licenza è scaduta.	• L'interruttore è disattivato. • L'interruttore è attivato.
La licenza sta per scadere	Il dispositivo è visibile nella rete, ma la licenza nel dispositivo scadrà tra un numero di giorni inferiore rispetto a quello specificato.	Meno di 0 giorni.
Verifica disponibilità aggiornamenti di Windows Update non eseguita da molto tempo	Il dispositivo è visibile nella rete, ma l'attività *Esegui sincronizzazione di Windows Update* non viene eseguita nell'intervallo di tempo specificato.	Più di 1 giorno.

Condizione	Descrizione della condizione	Valori disponibili
Stato criptaggio non valido	Network Agent è installato nel dispositivo, ma il risultato del criptaggio dispositivo è uguale al valore specificato.	• Non è conforme al criterio a causa di un rifiuto dell'utente (solo per i dispositivi esterni). • Non è conforme al criterio a causa di un errore. • È richiesto il riavvio per l'applicazione del criterio. • Non è specificato alcun criterio di criptaggio. • Non supportato. • Quando viene applicato il criterio.
Impostazioni dispositivo mobile non conformi al criterio	Le impostazioni del dispositivo mobile sono diverse dalle impostazioni specificate nel criterio di Kaspersky Endpoint Security for Android durante il controllo delle regole di conformità.	• L'interruttore è disattivato. • L'interruttore è attivato.
Problemi di sicurezza non elaborati rilevati	Sono stati rilevati nel dispositivo alcuni problemi di sicurezza non elaborati. I problemi di sicurezza possono essere creati automaticamente, tramite le applicazioni gestite Kaspersky installate nel dispositivo client, o manualmente, dall'amministratore.	• L'interruttore è disattivato. • L'interruttore è attivato.
Stato dispositivo definito dall'applicazione	Lo stato del dispositivo è definito dall'applicazione gestita. I dispositivi gestiti possono avere uno stato definito dallr applicazioni gestite indipendentemente dalle impostazioni di Kaspersky Security Center. Dopo che questo stato restituisce uno degli stati definiti da Kaspersky Security Center, Administration Server assegna a un dispositivo gestito lo stato più critico tra quelli restituiti dall'applicazione gestita e assegnati da Administration Server. Gli stati definiti dalle applicazioni gestite hanno descrizioni trasferite dalle applicazioni gestite. È possibile visualizzare le descrizioni nell'elenco dei dispositivi gestiti, colonna **Descrizione stato**.	• L'interruttore è disattivato. • L'interruttore è attivato.
Spazio su disco esaurito nel dispositivo	Lo spazio disponibile sul disco nel dispositivo è inferiore al valore specificato o il dispositivo non può essere sincronizzato con Administration Server. Lo stato *Critico* o *Avviso* diventa *OK* quando il dispositivo viene sincronizzato con Administration Server e lo spazio disponibile nel dispositivo è maggiore o uguale al valore specificato.	Più di 0 MB.
Il dispositivo è diventato non gestito	Durante la device discovery, il dispositivo è stato riconosciuto come visibile nella rete, ma più di tre tentativi di sincronizzazione con Administration Server hanno avuto esito negativo.	• L'interruttore è disattivato. • L'interruttore è attivato.
Protezione disattivata	Il dispositivo è visibile nella rete, ma l'applicazione di protezione nel dispositivo è stata disabilitata per un periodo superiore all'intervallo di tempo specificato. In questo caso, lo stato dell'applicazione di protezione è *interrotto* o *non riuscito* e differisce dai seguenti: *avvio*, *esecuzione* o *sospensione*.	Più di 0 minuti.
Applicazione di protezione non in esecuzione	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma non è in esecuzione.	• L'interruttore è disattivato. • L'interruttore è attivato.

Kaspersky Security Center consente di configurare la selezione automatica dello stato di un dispositivo in un gruppo di amministrazione quando vengono soddisfatte le condizioni specificate. Quando vengono soddisfatte le condizioni specificate, al dispositivo client viene assegnato uno dei seguenti stati: *Critico* o *Avviso*. Quando le condizioni specificate non vengono soddisfatte, al dispositivo client viene assegnato lo stato *OK*.

Diversi stati possono corrispondere ai diversi valori di una condizione. Ad esempio, per impostazione predefinita, se alla condizione **I database non sono aggiornati** è associato il valore **Più di 3 giorni**, al dispositivo client sarà assegnato lo stato *Avviso*; se il valore è **Più di 7 giorni**, verrà assegnato lo stato *Critico*.

Se si esegue l'upgrade di Kaspersky Security Center dalla versione precedente, i valori della condizione **I database non sono aggiornati** per l'assegnazione dello stato *Critico* o *Avviso* restano invariati.

Configurazione del passaggio degli stati del dispositivo

È possibile modificare le condizioni per assegnare lo stato *Critico* o *Avviso* a un dispositivo.

Per abilitare la modifica dello stato del dispositivo in Critico:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.
4. Nel riquadro sinistro selezionare **Critico**.
5. Nel riquadro destro, nella sezione **Imposta su Critico se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Critico*.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio principale.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.
7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.
8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.

9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Critico*.

Per abilitare la modifica dello stato del dispositivo in Avviso:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.

4. Nel riquadro sinistro selezionare **Avviso**.

5. Nel riquadro destro, nella sezione **Imposta su Avviso se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Avviso*.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio principale.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.

7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.

8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.

9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Avviso*.

Connessione remota al desktop di un dispositivo client

L'amministratore può accedere in remoto al desktop di un dispositivo client attraverso Network Agent installato nel dispositivo client. La connessione remota a un dispositivo tramite Network Agent è possibile anche se le porte TCP e UDP del dispositivo client sono chiuse.

Dopo avere stabilito la connessione con il dispositivo, l'amministratore ottiene l'accesso completo alle informazioni memorizzate in tale dispositivo e può gestire le applicazioni installate.

La connessione remota deve essere consentita nelle impostazioni del sistema operativo del dispositivo gestito di destinazione. Ad esempio, in Windows 10, questa opzione è denominata **Consenti connessioni di Assistenza remota al computer** (questa opzione è anche disponibile in **Pannello di controllo** → **Sistema e sicurezza** → **Sistema** → **Impostazioni di connessione remota**). Se si dispone di una licenza per la funzionalità Vulnerability e patch management, è possibile forzare l'abilitazione di questa opzione quando si stabilisce la connessione a un dispositivo gestito. Se non si dispone della licenza, abilitare questa opzione in locale nel dispositivo gestito di destinazione. Se questa opzione è disabilitata, la connessione remota non è possibile.

Per stabilire una connessione remota a un dispositivo, è necessario disporre di due utilità:

- Utilità Kaspersky denominata klsctunnel. Questa utilità deve essere archiviata nella workstation dell'amministratore. Questa utilità viene utilizzata per eseguire il tunneling della connessione tra un dispositivo client e Administration Server.

  Kaspersky Security Center consente il tunneling delle connessioni TCP da Administration Console tramite l'Administration Server e quindi tramite Network Agent su una porta specificata in un dispositivo gestito. Il tunneling è progettato per la connessione di un'applicazione client su un dispositivo con Administration Console installato a una porta TCP in un dispositivo gestito, se non è possibile la connessione diretta tra Administration Console e il dispositivo di destinazione.

  Il tunneling della connessione tra un dispositivo client remoto e Administration Server è richiesto se la porta utilizzata per la connessione ad Administration Server non è disponibile nel dispositivo. La porta nel dispositivo potrebbe non essere disponibile nei seguenti casi:

  - Il dispositivo remoto è connesso a una rete locale che utilizza il meccanismo NAT.
  - Il dispositivo remoto fa parte della rete locale di Administration Server, ma la relativa porta è chiusa da un firewall.

- Componente standard di Microsoft Windows denominato Connessione Desktop remoto. La connessione a un desktop remoto viene stabilita attraverso l'utilità standard di Windows mstsc.exe in base alle impostazioni dell'utilità.

  La connessione alla sessione di desktop remoto corrente dell'utente viene stabilita senza che l'utente ne sia a conoscenza. Una volta che l'amministratore si è connesso alla sessione, l'utente del dispositivo viene disconnesso dalla sessione senza preavviso.

Per stabilire la connessione al desktop di un dispositivo client:

1. In Administration Console basata su MMC, nel menu di scelta rapida di Administration Server selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server visualizzata passare a **Impostazioni di connessione di Administration Server → Porte di connessione**.
3. Assicurarsi che l'opzione **Apri porta RDP per Kaspersky Security Center Web Console** sia abilitata.
4. In Kaspersky Security Center Web Console, passare a **Risorse (dispositivi) → Dispositivi gestiti**.
5. Nel campo **Percorso corrente** sopra l'elenco dei dispositivi gestiti, fare clic sul collegamento del percorso.
6. Nel riquadro visualizzato a sinistra, selezionare il gruppo di amministrazione che contiene il dispositivo a cui si desidera ottenere l'accesso.
7. Selezionare la casella di controllo accanto al nome del dispositivo a cui si desidera ottenere l'accesso.
8. Fare clic sul pulsante **Connetti a desktop remoto**

   Verrà aperta la finestra Desktop remoto (solo Windows).

9. Abilitare l'opzione **Consenti connessione Desktop remoto nel dispositivo gestito**. In questo caso, la connessione verrà stabilita anche se le connessioni remote non sono attualmente consentite nelle impostazioni del sistema operativo nel dispositivo gestito.

   Questa opzione è disponibile solo se si dispone di una licenza per la funzionalità Vulnerability e patch management.

10. Fare clic sul pulsante **Scarica** per scaricare l'utilità klsctunnel.

11. Fare clic sul pulsante **Copia negli Appunti** per copiare il testo dal campo di testo. Questo testo è un BLOB (Binary Large OBject) che contiene le impostazioni necessarie per stabilire una connessione tra Administration Server e il dispositivo gestito.

    Un BLOB è valido per 3 minuti. Se è scaduto, riaprire la finestra Desktop remoto (solo Windows) per generare un nuovo BLOB.

12. Eseguire l'utilità klsctunnel.

    Verrà visualizzata la finestra dell'utilità.

13. Incollare il testo copiato nel campo di testo.

14. Se si utilizza un server proxy, selezionare la casella di controllo **Usa server proxy**, quindi specificare le impostazioni di connessione del server proxy.

15. Fare clic sul pulsante **Apri porta**.

    Verrà visualizzata la finestra di accesso a Connessione Desktop remoto.

16. Specificare le credenziali dell'account con cui si è attualmente connessi a Kaspersky Security Center Web Console.

17. Fare clic sul pulsante **Connetti**.

Quando viene stabilita la connessione con il dispositivo, il desktop è disponibile nella finestra Connessione Desktop remoto di Microsoft Windows.

Connessione ai dispositivi tramite Condivisione desktop Windows

L'amministratore può accedere in remoto al desktop di un dispositivo client attraverso Network Agent installato nel dispositivo client. La connessione remota a un dispositivo tramite Network Agent è possibile anche se le porte TCP e UDP del dispositivo client sono chiuse.

L'amministratore può connettersi a una sessione esistente in un dispositivo client senza disconnettere l'utente in questa sessione. In questo caso, l'amministratore e l'utente della sessione nel dispositivo condividono l'accesso al desktop.

Per stabilire una connessione remota a un dispositivo, è necessario disporre di due utilità:

- Utilità Kaspersky denominata klsctunnel. Questa utilità deve essere archiviata nella workstation dell'amministratore. Questa utilità viene utilizzata per eseguire il tunneling della connessione tra un dispositivo client e Administration Server.

  Kaspersky Security Center consente il tunneling delle connessioni TCP da Administration Console tramite l'Administration Server e quindi tramite Network Agent su una porta specificata in un dispositivo gestito. Il tunneling è progettato per la connessione di un'applicazione client su un dispositivo con Administration Console installato a una porta TCP in un dispositivo gestito, se non è possibile la connessione diretta tra Administration Console e il dispositivo di destinazione.

  Il tunneling della connessione tra un dispositivo client remoto e Administration Server è richiesto se la porta utilizzata per la connessione ad Administration Server non è disponibile nel dispositivo. La porta nel dispositivo potrebbe non essere disponibile nei seguenti casi:

  - Il dispositivo remoto è connesso a una rete locale che utilizza il meccanismo NAT.
  - Il dispositivo remoto fa parte della rete locale di Administration Server, ma la relativa porta è chiusa da un firewall.

- Condivisione desktop Windows. Quando ci si connette a una sessione esistente di desktop remoto, l'utente della sessione nel dispositivo client riceve una richiesta per la connessione dall'amministratore. Nei rapporti creati da Kaspersky Security Center non sarà salvata alcuna informazione sull'attività remota nel dispositivo né sui relativi risultati.

  L'amministratore può configurare un controllo dell'attività dell'utente in un dispositivo client remoto. Durante il controllo, l'applicazione salva le informazioni sui file nel dispositivo client che sono stati aperti e/o modificati dall'amministratore.

Per connettersi al desktop di un dispositivo client tramite Condivisione desktop Windows, devono essere soddisfatte le seguenti condizioni:

- Microsoft Windows Vista o versione successiva è installato nella workstation dell'amministratore. Il tipo di sistema operativo del dispositivo che contiene Administration Server non impone alcuna limitazione alla connessione tramite Condivisione desktop Windows.

  Per verificare se la funzionalità Condivisione desktop Windows è inclusa nella versione di Windows in uso, assicurarsi che la chiave CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} sia presente nel Registro di sistema di Windows.

- Microsoft Windows Vista o versione successiva è installato nel dispositivo client.
- Kaspersky Security Center utilizza una licenza per Vulnerability e patch management.

Per connettersi al desktop di un dispositivo client tramite Condivisione desktop Windows:

1. In Administration Console basata su MMC, nel menu di scelta rapida di Administration Server selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server visualizzata passare a **Impostazioni di connessione di Administration Server → Porte di connessione**.
3. Assicurarsi che l'opzione **Apri porta RDP per Kaspersky Security Center Web Console** sia abilitata.
4. In Kaspersky Security Center Web Console, passare a **Risorse (dispositivi) → Dispositivi gestiti**.
5. Nel campo **Percorso corrente** sopra l'elenco dei dispositivi gestiti, fare clic sul collegamento del percorso.

6. Nel riquadro visualizzato a sinistra, selezionare il gruppo di amministrazione che contiene il dispositivo a cui si desidera ottenere l'accesso.

7. Selezionare la casella di controllo accanto al nome del dispositivo a cui si desidera ottenere l'accesso.

8. Fare clic sul pulsante **Condivisione desktop Windows**.

   Viene aperta la procedura guidata Condivisione desktop Windows.

9. Fare clic sul pulsante **Scarica** per scaricare l'utilità klsctunnel e attendere il completamento del processo di download.

   Se si dispone già dell'utilità klsctunnel, ignorare questo passaggio.

10. Fare clic sul pulsante **Avanti**.

11. Selezionare la sessione nel dispositivo a cui si desidera eseguire la connessione, quindi fare clic sul pulsante **Avanti**.

12. Nel dispositivo di destinazione, l'utente deve consentire una sessione di condivisione desktop nella finestra di dialogo visualizzata. In caso contrario, la sessione non è possibile.

    Dopo che l'utente del dispositivo ha confermato la sessione di condivisione del desktop, viene aperta la pagina successiva della procedura guidata.

13. Fare clic sul pulsante **Copia negli Appunti** per copiare il testo dal campo di testo. Questo testo è un BLOB (Binary Large OBject) che contiene le impostazioni necessarie per stabilire una connessione tra Administration Server e il dispositivo gestito.

    Un BLOB è valido per 3 minuti. Se è scaduto, generare un nuovo BLOB.

14. Eseguire l'utilità klsctunnel.

    Verrà visualizzata la finestra dell'utilità.

15. Incollare il testo copiato nel campo di testo.

16. Se si utilizza un server proxy, selezionare la casella di controllo **Usa server proxy**, quindi specificare le impostazioni di connessione del server proxy.

17. Fare clic sul pulsante **Apri porta**.

La condivisione del desktop viene avviata in una nuova finestra. Se si desidera interagire con il dispositivo, fare clic sull'icona Menu () nell'angolo superiore sinistro della finestra, quindi selezionare **Modalità interattiva**.

Selezioni dispositivi

Le *selezioni dispositivi* sono uno strumento per filtrare i dispositivi in base a condizioni specifiche. È possibile utilizzare le selezioni dispositivi per gestire diversi dispositivi, ad esempio per visualizzare un rapporto solo su questi dispositivi o per spostare tutti questi dispositivi in un altro gruppo.

Kaspersky Security Center offre un'ampia gamma di *selezioni predefinite* (ad esempio, **Dispositivi con stato Critico**, **Protezione disattivata**, **Rilevate minacce attive**). Le selezioni predefinite non possono essere eliminate. È inoltre possibile creare e configurare ulteriori *selezioni definite dall'utente*.

Nelle selezioni definite dall'utente è possibile impostare l'ambito di ricerca e selezionare tutti i dispositivi, i dispositivi gestiti o i dispositivi non assegnati. I parametri di ricerca sono specificati nelle condizioni. Nella selezione dispositivi è possibile creare diverse condizioni con parametri di ricerca differenti. È ad esempio possibile creare due condizioni e specificare intervalli IP diversi in ciascuna di esse. Se vengono specificate più condizioni, una selezione visualizza i dispositivi che soddisfano una qualsiasi delle condizioni. Al contrario, i parametri di ricerca in una condizione vengono sovrapposti. Se in una condizione si specificano sia un intervallo IP che il nome di un'applicazione installata, verranno visualizzati solo i dispositivi in cui è installata l'applicazione e con un indirizzo IP che appartiene all'intervallo specificato.

Visualizzazione dell'elenco dei dispositivi da una selezione di dispositivi

Kaspersky Security Center consente di visualizzare l'elenco dei dispositivi da una selezione di dispositivi.

Per visualizzare l'elenco dei dispositivi dalla selezione di dispositivi:

1. Nel menu principale, passare alla sezione **Risorse (dispositivi)** → **Selezioni dispositivi** o **Individuazione e distribuzione** → **Selezioni dispositivi**.
2. Nell'elenco delle selezioni fare clic sul nome della selezione di dispositivi.

   La pagina mostra una tabella con le informazioni sui dispositivi inclusi nella selezione di dispositivi.
3. È possibile raggruppare e filtrare i dati della tabella dei dispositivi come segue:
   - Fare clic sull'icona delle impostazioni ( ), quindi selezionare le colonne da visualizzare nella tabella.
   - Fare clic sull'icona del filtro ( ), quindi specificare e applicare il criterio di filtro nel menu richiamato.

     Viene visualizzata la tabella filtrata dei dispositivi.

È possibile selezionare uno o più dispositivi nella selezione di dispositivi e fare clic sul pulsante **Nuova attività** per creare un'attività che verrà applicata a tali dispositivi.

Per spostare i dispositivi selezionati della selezione di dispositivi in un altro gruppo di amministrazione, fare clic sul pulsante **Sposta nel gruppo**, quindi selezionare il gruppo di amministrazione di destinazione.

Creazione di una selezione dispositivi

Per creare una selezione dispositivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Selezioni dispositivi**.

   Verrà visualizzata una pagina con un elenco di selezioni dispositivi.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra **Impostazioni della selezione dispositivi**.
3. Immettere il nome della nuova selezione.

4. Specificare il gruppo che contiene i dispositivi da includere nella selezione di dispositivi:

   - **Trova qualsiasi dispositivo**: ricerca dei dispositivi che soddisfano i criteri di selezione e inclusi nel gruppo **Dispositivi gestiti** o **Dispositivi non assegnati**.
   - **Trova dispositivi gestiti**: ricerca dei dispositivi che soddisfano i criteri di selezione e inclusi nel gruppo **Dispositivi gestiti**.
   - **Trova dispositivi non assegnati**: ricerca dei dispositivi che soddisfano i criteri di selezione e inclusi nel gruppo **Dispositivi non assegnati**.

   È possibile abilitare la casella di controllo **Includi i dati degli Administration Server secondari** per abilitare la ricerca dei dispositivi che soddisfano i criteri di selezione e gestiti dagli Administration Server secondari.

5. Fare clic sul pulsante **Aggiungi**.
6. Nella finestra visualizzata specificare le condizioni che devono essere soddisfatte per includere i dispositivi in questa selezione, quindi fare clic sul pulsante **OK**.
7. Fare clic sul pulsante **Salva**.

La selezione dispositivi viene creata e aggiunta all'elenco delle selezioni dispositivi.

Configurazione di una selezione dispositivi

Per configurare una selezione dispositivi:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Selezioni dispositivi**.

   Verrà visualizzata una pagina con un elenco di selezioni dispositivi.

2. Selezionare la selezione di dispositivi definita dall'utente pertinente e fare clic sul pulsante **Proprietà**.

   Verrà visualizzata la finestra **Impostazioni della selezione dispositivi**.

3. Nella scheda **Generale**, fare clic sul collegamento **Nuova condizione**.
4. Specificare le condizioni da soddisfare per l'inclusione dei dispositivi nella selezione.
5. Fare clic sul pulsante **Salva**.

Le impostazioni verranno applicate e salvate.

Di seguito sono descritte le condizioni per l'assegnazione dei dispositivi a una selezione. Le condizioni vengono combinate tramite l'operatore logico OR: la selezione conterrà i dispositivi conformi ad almeno una delle condizioni elencate.

Generale

Nella sezione **Generale** è possibile modificare il nome della condizione di selezione e specificare se tale condizione deve essere invertita:

Inverti condizione selezione

Per impostazione predefinita, questa opzione è disabilitata.

Se si abilita questa opzione, la condizione di selezione specificata verrà invertita. La selezione includerà tutti i dispositivi che non soddisfano la condizione.

L'esempio seguente mostra la logica del lavoro di inversione:

- **Condizione**: nel dispositivo è presente un sistema operativo con il tipo Linux e il numero di build 00.0.000.
- **Condizione invertita**: nel dispositivo è presente un sistema operativo con NOT (il tipo Linux e il numero di build 00.0.000), che equivale a quanto segue:

  È presente un sistema operativo con il tipo NOT Linux OR numero di build NOT 00.0. 000.

Pertanto, la selezione includerà i dispositivi con un sistema operativo, ad esempio di tipo Windows e numero di build 00.0.000, o di tipo Linux e qualsiasi numero di build diverso da 00.0.000.

Infrastruttura di rete

Nella sottosezione **Rete**, è possibile specificare i criteri che verranno utilizzati per includere i dispositivi nella selezione in base ai dati della rete:

- Nome dispositivo

  Nome di rete Windows (nome NetBIOS) del dispositivo o indirizzo IPv4 o IPv6.

- Dominio

  Visualizza tutti i dispositivi inclusi nel dominio Windows specificato.

- Gruppo di amministrazione

  Visualizza i dispositivi inclusi nel gruppo di amministrazione specificato.

- **Descrizione**

  Testo contenuto nella finestra delle proprietà del dispositivo: nel campo **Descrizione** della sezione **Generale**.

  Per inserire il testo nel campo **Descrizione**, è possibile utilizzare i seguenti caratteri:

  - All'interno di una parola:

    - *****. Sostituisce qualsiasi stringa con qualsiasi numero di caratteri.

    Esempio:

    Per descrivere parole come **Server** o **Server's**, è possibile immettere **Server***.

    - **?.** Sostituisce qualsiasi carattere singolo.

    Esempio:

    Per descrivere parole come **Finestra** o **Finestre**, è possibile immettere **Finestr?**.

    Non è possibile utilizzare l'asterisco (*****) o il punto interrogativo (**?**) come primo carattere nella query.

  - Per trovare più parole:

    - Spazio. Visualizza tutti i dispositivi le cui descrizioni contengono una delle parole elencate.

    Esempio:

    Per trovare una frase contenente le parole **Secondario** o **Virtuale**, è possibile includere la riga **Secondario Virtuale** nella query.

    - **+**. Quando una parola è preceduta dal segno +, tutti i risultati della ricerca conterranno tale parola.

    Esempio:

    Per trovare una frase contenente sia **Secondario** che **Virtuale**, immettere la query **+Secondario+Virtuale**.

    - **-**. Quando una parola è preceduta dal segno -, nessun risultato della ricerca conterrà tale parola.

    Esempio:

    Per trovare una frase contenente **Secondario** e non contenente **Virtuale**, immettere la query **+Secondario-Virtuale**.

    - **"<testo>"**. Verranno visualizzati i risultati che contengono il testo racchiuso tra virgolette.

    Esempio:

    Per trovare una frase contenente la combinazione di parole **Server secondario**, è possibile immettere **"Server secondario"** nella query.

- Intervallo IP

  Se questa opzione è abilitata, è possibile immettere gli indirizzi IP iniziale e finale dell'intervallo IP in cui i dispositivi rilevanti devono essere inclusi.

  Per impostazione predefinita, questa opzione è disabilitata.

- Gestito da un altro Administration Server

  Selezionare uno dei seguenti valori:

  - **Sì**. Una regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti da altri Administration Server. Questi server sono diversi dal server su cui si configura la regola di spostamento dei dispositivi.
  - **No**. La regola di spostamento dei dispositivi si applica solo ai dispositivi client gestiti dall'Administration Server corrente.
  - **Nessun valore selezionato**. La condizione non si applica.

Nella sottosezione **Controller di dominio**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'appartenenza a un dominio:

- Il dispositivo si trova in un'unità organizzativa del dominio

  Se questa opzione è abilitata, la selezione includerà i dispositivi dell'unità organizzativa del dominio specificata nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il dispositivo fa parte del gruppo di sicurezza del dominio

  Se questa opzione è abilitata, la selezione includerà i dispositivi del gruppo di sicurezza del dominio specificato nel campo di immissione.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Attività di rete**, è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base alle relative attività della rete:

- Funge da punto di distribuzione

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione include i dispositivi che operano come punti di distribuzione.
  - **No**. I dispositivi che operano come punti di distribuzione non sono inclusi nella selezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Non eseguire la disconnessione da Administration Server

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Abilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è selezionata.
  - **Disabilitata**. La selezione includerà i dispositivi in cui la casella di controllo **Non eseguire la disconnessione da Administration Server** è deselezionata.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Profilo connessione cambiato

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. La selezione includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **No**. La selezione non includerà i dispositivi che hanno eseguito la connessione ad Administration Server dopo la modifica del profilo di connessione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- Ultima connessione ad Administration Server

  È possibile utilizzare questa casella di controllo per impostare un criterio di ricerca per i dispositivi in base all'ora dell'ultima connessione ad Administration Server.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stata stabilita l'ultima connessione tra Network Agent installato nel dispositivo client e Administration Server. La selezione includerà i dispositivi che rientrano nell'intervallo specificato.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Rilevati nuovi dispositivi durante il polling della rete

  Cerca nuovi dispositivi rilevati dal polling della rete negli ultimi giorni.

  Se questa opzione è abilitata, la selezione includerà soltanto i nuovi dispositivi rilevati dalla device discovery nel numero di giorni specificato nel campo **Periodo di rilevamento (giorni)**.

  Se questa opzione è disabilitata, la selezione includerà tutti i dispositivi rilevati dalla device discovery.

  Per impostazione predefinita, questa opzione è disabilitata.

- Il dispositivo è visibile

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi nella selezione durante l'esecuzione di una ricerca:

  - **Sì**. L'applicazione include nella selezione i dispositivi attualmente visibili nella rete.
  - **No**. L'applicazione include nella selezione i dispositivi attualmente invisibili nella rete.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Nella sottosezione **Segmenti cloud**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base ai rispettivi segmenti cloud:

- Il dispositivo si trova in un segmento cloud

  Se questa opzione è abilitata, è possibile scegliere i dispositivi dai segmenti cloud AWS, Azure e Google.

  Se anche l'opzione **Includi gli oggetti figlio** è abilitata, la ricerca viene eseguita in tutti gli oggetti figlio del segmento selezionato.

  I risultati di ricerca includono solo i dispositivi del segmento selezionato.

- Dispositivo rilevato tramite l'API

  Nell'elenco a discesa, è possibile selezionare se un dispositivo deve essere rilevato o meno dagli strumenti API:

  - **Sì**. Il dispositivo viene rilevato tramite l'API AWS, Azure o Google.
  - **No**. Il dispositivo non può essere rilevato tramite l'API AWS, Azure o Google. In altre parole, il dispositivo si trova all'esterno dell'ambiente cloud o si trova nell'ambiente cloud ma non può essere rilevato tramite un'API.
  - Nessun valore. Questa condizione non viene applicata.

Stati dispositivi

Nella sottosezione **Stato del dispositivo gestito**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base alla descrizione dello stato dei dispositivi ottenuta da un'applicazione gestita:

- **Stato dispositivo**

  Elenco a discesa in cui è possibile selezionare uno degli stati del dispositivo: *OK*, *Critico* o *Avviso*.

- **Stato protezione in tempo reale**

  Elenco a discesa in cui è possibile selezionare lo stato della protezione in tempo reale. I dispositivi con lo stato della protezione in tempo reale specificato vengono inclusi nella selezione.

- **Descrizione stato del dispositivo**

  In questo campo è possibile selezionare le caselle di controllo accanto alle condizioni che, se soddisfatte, assegnano al dispositivo uno dei seguenti stati: *OK*, *Critico* o *Avviso*.

Nella sezione **Stato dei componenti nelle applicazioni gestite**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base agli stati dei componenti nelle applicazioni gestite:

- **Stato prevenzione fughe di dati**

  Cercare i dispositivi in base allo stato di prevenzione della perdita dei dati (*Sconosciuto, Arrestata, Avvio in corso, Sospesa, In esecuzione, Non riuscito*).

- **Stato protezione server di collaborazione**

  Cercare i dispositivi in base allo stato della protezione della collaborazione server (*Sconosciuto*, *Arrestata*, *Avvio in corso, Sospesa*, *In esecuzione*, *Non riuscito*).

- **Stato protezione anti-virus server di posta**

  Cercare i dispositivi in base allo stato della protezione dei server di posta (*Sconosciuto, Arrestata, Avvio in corso, Sospesa, In esecuzione, Non riuscito*).

- **Stato Endpoint Sensor**

  Cercare i dispositivi in base allo stato del componente Sensore Endpoint (*Sconosciuto, Arrestata, Avvio in corso, Sospesa, In esecuzione, Non riuscito*).

Nella sezione **Problemi che influiscono sullo stato nelle applicazioni gestite** è possibile specificare i criteri per l'inclusione dei dispositivi nella selezione in base all'elenco dei possibili problemi rilevati da un'applicazione gestita. Se è presente almeno un problema selezionato in un dispositivo, il dispositivo verrà incluso nella selezione. Quando si seleziona un problema elencato per diverse applicazioni, è possibile selezionare automaticamente questo problema in tutti gli elenchi.

È possibile selezionare le caselle di controllo relative alle descrizioni degli stati dall'applicazione gestita. Alla ricezione di questi stati, i dispositivi verranno inclusi nella selezione. Quando si seleziona uno stato elencato per diverse applicazioni, è possibile selezionare automaticamente questo stato in tutti gli elenchi.

Dettagli di sistema

Nella sezione **Sistema operativo** è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base al tipo di sistema operativo.

- Tipo di piattaforma

  Se la casella di controllo è selezionata, è possibile selezionare un sistema operativo dall'elenco. I dispositivi in cui sono installati i sistemi operativi specificati saranno inclusi nei risultati della ricerca.

- Versione Service Pack del sistema operativo

  In questo campo è possibile specificare la versione del pacchetto del sistema operativo (nel formato *X.Y*), da cui dipenderà l'applicazione della regola di spostamento al dispositivo. Per impostazione predefinita, non è specificato alcun valore per la versione.

- Dimensioni in bit del sistema operativo

  Nell'elenco a discesa è possibile selezionare l'architettura del sistema operativo da cui dipenderà l'applicazione della regola di spostamento al dispositivo (**Sconosciuto**, **x86**, **AMD64** o **IA64**). Per impostazione predefinita, non è selezionata alcuna opzione nell'elenco, pertanto l'architettura del sistema operativo non è definita.

- Build del sistema operativo

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Numero di build del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un numero di build uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti i numeri di build ad eccezione di quello specificato.

- Numero di rilascio del sistema operativo

  Questa impostazione è applicabile solo ai sistemi operativi Windows.

  Identificatore della versione (ID) del sistema operativo. È possibile specificare se il sistema operativo selezionato deve avere un ID di rilascio uguale, precedente o successivo. È anche possibile configurare la ricerca di tutti gli ID di rilascio ad eccezione di quello specificato.

Nella sezione **Macchine virtuali** è possibile configurare i criteri per l'inclusione dei dispositivi nella selezione in base al fatto che siano macchine virtuali o che facciano parte di Microsoft Virtual Desktop Infrastructure (VDI):

- Questa è una macchina virtuale

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Indefinito**.
  - **No**. I dispositivi che non sono macchine virtuali vengono trovati.
  - **Sì**. Vengono trovati i dispositivi che sono macchine virtuali.

- Tipo di macchina virtuale

  Nell'elenco a discesa è possibile selezionare il produttore della macchina virtuale.

  Questo elenco a discesa è disponibile se è selezionato il valore **Sì** o **Non importante** nell'elenco a discesa **Questa è una macchina virtuale**.

- Parte di Virtual Desktop Infrastructure

  Dall'elenco a discesa è possibile selezionare le seguenti opzioni:

  - **Indefinito**.
  - **No**. Vengono trovati i dispositivi che non fanno parte di Virtual Desktop Infrastructure.
  - **Sì**. Vengono trovati i dispositivi che fanno parte di Microsoft Virtual Desktop Infrastructure (VDI).

Nella sottosezione **Registro hardware**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'hardware installato:

Assicurarsi che l'utilità lshw sia installata nei dispositivi Linux da cui si desidera recuperare i dettagli dell'hardware. I dettagli dell'hardware recuperati dalle macchine virtuali potrebbero essere incompleti a seconda dell'hypervisor utilizzato.

- Dispositivo

  Nell'elenco a discesa è possibile selezionare un tipo di unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- Fornitore

  Nell'elenco a discesa è possibile selezionare il nome di un produttore dell'unità. Tutti i dispositivi con questa unità verranno inclusi nei risultati della ricerca.

  Il campo supporta la ricerca full-text.

- **Nome dispositivo**

  Nome del dispositivo nella rete Windows. Il dispositivo con il nome specificato verrà incluso nella selezione.

- **Descrizione**

  Descrizione del dispositivo o dell'unità hardware. I dispositivi con la descrizione specificata in questo campo verranno inclusi nella selezione.

  La descrizione di un dispositivo in qualsiasi formato può essere immessa nella finestra delle proprietà del dispositivo. Il campo supporta la ricerca full-text.

- **Produttore dispositivo**

  Nome del produttore del dispositivo. I dispositivi del produttore specificato in questo campo verranno inclusi nella selezione.

  È possibile inserire il nome del produttore nella finestra delle proprietà di un dispositivo.

- **Numero di serie**

  Tutte le unità hardware con il numero di serie specificato in questo campo verranno incluse nella selezione.

- **Numero di inventario**

  L'apparecchiatura con il numero di inventario specificato in questo campo verrà inclusa nella selezione.

- **Utente**

  Tutte le unità hardware dell'utente specificato in questo campo verranno incluse nella selezione.

- **Posizione**

  Posizione del dispositivo o dell'unità hardware (ad esempio nella sede principale o in una filiale). I computer o gli altri dispositivi distribuiti al percorso specificato in questo campo verranno inclusi nella selezione.

  È possibile descrivere il percorso di un dispositivo in qualsiasi formato nella finestra delle proprietà del dispositivo.

- **Frequenza di clock della CPU (in MHz) da**

  La frequenza di clock minima di una CPU. I dispositivi con una CPU che corrisponde all'intervallo di frequenza di clock specificati nei campi di immissione (compresi) verranno inclusi nella selezione.

- **Frequenza di clock della CPU (in MHz) a**

  La frequenza di clock massima di una CPU. I dispositivi con una CPU che corrisponde all'intervallo di frequenza di clock specificati nei campi di immissione (compresi) verranno inclusi nella selezione.

- Numero di core CPU virtuali, da

  Il numero minimo di core CPU virtuali. I dispositivi con una CPU che corrisponde all'intervallo del numero di core virtuali specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

- Numero di core CPU virtuali, a

  Il numero massimo di core CPU virtuali. I dispositivi con una CPU che corrisponde all'intervallo del numero di core virtuali specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

- Volume disco rigido (GB) da

  Il volume minimo del disco rigido sul dispositivo. I dispositivi con un disco rigido che corrisponde all'intervallo di volumi nei campi di immissione (compresi) verranno inclusi nella selezione.

- Volume disco rigido (GB) a

  Il volume massimo del disco rigido sul dispositivo. I dispositivi con un disco rigido che corrisponde all'intervallo di volumi nei campi di immissione (compresi) verranno inclusi nella selezione.

- Dimensione RAM (MB) da

  La dimensione minima della RAM del dispositivo. I dispositivi con una RAM che corrisponde all'intervallo di dimensione specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

- Dimensione RAM (MB) a

  La dimensione massima della RAM del dispositivo. I dispositivi con una RAM che corrisponde all'intervallo di dimensione specificato nei campi di immissione (compresi) verranno inclusi nella selezione.

Dettagli software di terze parti

Nella sottosezione **Registro delle applicazioni**, è possibile impostare i criteri di ricerca dei dispositivi in base alle applicazioni installate:

- Nome applicazione

  Elenco a discesa da cui è possibile selezionare un'applicazione. I dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- Versione applicazione

  Campo di immissione in cui è possibile specificare la versione dell'applicazione selezionata.

- Fornitore

  Elenco a discesa da cui è possibile selezionare il produttore di un'applicazione installata nel dispositivo.

- Stato applicazione

  Elenco a discesa da cui è possibile selezionare lo stato di un'applicazione (*Installata*, *Non installata*). Verranno inclusi nella selezione i dispositivi in cui è installata o non è installata l'applicazione specificata, in base allo stato selezionato.

- Trova per aggiornamento

  Se questa opzione è abilitata, la ricerca verrà eseguita utilizzando i dettagli degli aggiornamenti per le applicazioni installate nei dispositivi. Dopo aver selezionato la casella di controllo, i campi **Nome applicazione**, **Versione applicazione** e **Stato applicazione** diventano rispettivamente **Nome aggiornamento**, **Versione aggiornamento** e **Stato**.

  Per impostazione predefinita, questa opzione è disabilitata.

- Nome dell'applicazione di protezione incompatibile

  Elenco a discesa da cui è possibile selezionare applicazioni di protezione di terze parti. Durante la ricerca, i dispositivi in cui è installata l'applicazione specificata sono inclusi nella selezione.

- Tag applicazione

  Nell'elenco a discesa è possibile selezionare il tag di un'applicazione. Tutti i dispositivi che hanno applicazioni installate con il tag selezionato nella descrizione sono inclusi nella selezione dispositivi.

- Applica ai dispositivi senza i tag specificati

  Se questa opzione è abilitata, la selezione includerà i dispositivi con descrizioni che non contengono alcuno dei tag selezionati.

  Se questa opzione è disabilitata, il criterio non viene applicato.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Vulnerabilità e aggiornamenti**, è possibile specificare i criteri per l'inclusione dei dispositivi nella selezione in base all'origine di Windows Update:

WUA è passato ad Administration Server

È possibile selezionare una delle seguenti opzioni di ricerca nell'elenco a discesa:

- **Sì**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da Administration Server.
- **No**. Se questa opzione è selezionata, i risultati di ricerca includeranno i dispositivi che ricevono gli aggiornamenti tramite Windows Update da altre origini.

Dettagli delle applicazioni Kaspersky

Nella sottosezione **Applicazioni Kaspersky**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base all'applicazione gestita selezionata:

- Nome applicazione

  Nell'elenco a discesa è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome di un'applicazione Kaspersky.

  L'elenco contiene solo i nomi delle applicazioni con plug-in di gestione installati nella workstation dell'amministratore.

  Se non è selezionata alcuna applicazione, il criterio non verrà applicato.

- Versione applicazione

  Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al numero versione di un'applicazione Kaspersky.

  Se non è specificato alcun numero di versione, il criterio non verrà applicato.

- Nome aggiornamento critico

  Elenco a discesa da cui è possibile selezionare lo stato di un'applicazione (*Installata*, *Non installata*). Verranno inclusi nella selezione i dispositivi in cui è installata o non è installata l'applicazione specificata, in base allo stato selezionato.

  Nel campo di immissione è possibile impostare un criterio per l'inclusione dei dispositivi in una selezione quando la ricerca viene eseguita in base al nome dell'applicazione o al numero del pacchetto di aggiornamento.

  Se il campo è vuoto, il criterio non verrà applicato.

- Selezionare il periodo dell'ultimo aggiornamento dei moduli

  È possibile utilizzare questa opzione per impostare un criterio per la ricerca dei dispositivi in base all'ora dell'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare l'intervallo di tempo (data e ora) durante il quale è stato eseguito l'ultimo aggiornamento dei moduli delle applicazioni installate in tali dispositivi.

  Se questa casella di controllo è deselezionata, il criterio non verrà applicato.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Il dispositivo è gestito tramite Administration Server

  Nell'elenco a discesa è possibile includere nella selezione i dispositivi gestiti tramite Kaspersky Security Center:

  - **Sì**. L'applicazione include nella selezione i dispositivi gestiti tramite Kaspersky Security Center.
  - **No**. L'applicazione include nella selezione i dispositivi non gestiti tramite Kaspersky Security Center.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

- L'applicazione di protezione è installata

  Nell'elenco a discesa è possibile includere nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione:

  - **Sì**. L'applicazione include nella selezione tutti i dispositivi in cui è installata l'applicazione di protezione.
  - **No**. L'applicazione include nella selezione tutti i dispositivi in cui non è installata un'applicazione di protezione.
  - **Nessun valore selezionato**. Il criterio non verrà applicato.

Nella sottosezione **Protezione anti-virus**, è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base allo stato della protezione:

- Data rilascio database

  Se questa opzione è selezionata, è possibile eseguire la ricerca dei dispositivi client in base alla data di rilascio del database anti-virus. Nei campi di immissione è possibile impostare l'intervallo di tempo in base al quale eseguire la ricerca.

  Per impostazione predefinita, questa opzione è disabilitata.

- Conteggio record database

  Se questa opzione è abilitata, è possibile eseguire la ricerca di dispositivi client in base al numero di record del database. Nei campi di immissione è possibile impostare i valori di soglia inferiore e superiore per i record del database anti-virus.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Ultima scansione**

  Se questa opzione è abilitata, è possibile eseguire la ricerca dei dispositivi client in base all'ora dell'ultima scansione malware. Nei campi di immissione è possibile specificare il periodo di tempo entro il quale è stata eseguita l'ultima scansione malware.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Minacce**

  Se questa opzione è abilitata, è possibile eseguire la ricerca di dispositivi client in base al numero di virus rilevati. Nei campi di immissione è possibile impostare i valori di soglia inferiore e superiore per il numero di virus trovati.

  Per impostazione predefinita, questa opzione è disabilitata.

Nella sottosezione **Criptaggio**, è possibile configurare il criterio per l'inclusione dei dispositivi in una selezione in base all'algoritmo di criptaggio selezionato:

Algoritmo di criptaggio

Algoritmo di cifratura a blocchi AES (Advanced Encryption Standard). Nell'elenco a discesa è possibile selezionare le dimensioni della chiave di criptaggio (56 bit, 128 bit, 192 bit o 256 bit).

Valori disponibili: *AES56*, *AES128*, *AES192* e *AES256*.

La sottosezione **Componenti dell'applicazione** contiene un elenco dei componenti delle applicazioni per cui sono installati plug-in di gestione corrispondenti in Kaspersky Security Center Web Console.

Nella sottosezione **Componenti dell'applicazione**, è possibile specificare i criteri per l'inclusione dei dispositivi in una selezione in base agli stati e ai numeri di versione dei componenti che fanno riferimento all'applicazione selezionata:

- **Stato**

  Ricerca dei dispositivi in base allo stato dei componenti inviato da un'applicazione all'Administration Server. È possibile selezionare uno dei seguenti stati: *N/D, Arrestato*, *Sospeso*, *Avvio in corso*, *In esecuzione, Non riuscito, Non installato, Non supportato dalla licenza*. Se il componente selezionato dell'applicazione installata in un dispositivo gestito presenta lo stato specificato, il dispositivo viene incluso nella selezione dispositivi.

  Stati inviati dalle applicazioni:

  - *Arrestato* - Il componente è disabilitato e al momento non è in esecuzione.
  - *Sospeso* - Il componente è sospeso, ad esempio dopo che l'utente ha sospeso la protezione nell'applicazione gestita.
  - *Avvio in corso* - Il componente è attualmente in fase di inizializzazione.
  - *In esecuzione* - Il componente è abilitato e correttamente in esecuzione.
  - *Non riuscito* - Si è verificato un errore durante l'esecuzione del componente.
  - *Non installato* - L'utente non ha selezionato il componente per l'installazione durante la configurazione dell'installazione personalizzata dell'applicazione.
  - *Non supportato dalla licenza* - La licenza non copre il componente selezionato.

  A differenza degli altri stati, lo stato *N/D* non viene inviato dalle applicazioni. Questa opzione indica che le applicazioni non dispongono di alcuna informazione sullo stato del componente selezionato. Ciò può ad esempio verificarsi quando il componente selezionato non appartiene ad alcuna delle applicazioni installate nel dispositivo o quando il dispositivo è spento.

- **Versione**

  Ricerca dei dispositivi in base al numero di versione del componente selezionato nell'elenco. È possibile digitare un numero di versione, ad esempio `3.4.1.0`, e quindi specificare se il componente selezionato deve avere una versione uguale, precedente o successiva. È anche possibile configurare la ricerca di tutte le versioni ad eccezione di quella specificata.

Tag

Nella sezione **Tag** è possibile configurare i criteri per l'inclusione dei dispositivi in una selezione in base alle parole chiave (tag) che sono state aggiunte in precedenza alle descrizioni dei dispositivi gestiti:

Applica se almeno uno dei tag specificati corrisponde

Se questa opzione è abilitata, i risultati di ricerca visualizzeranno i dispositivi con descrizioni contenenti almeno uno dei tag selezionati.

Se questa opzione è disabilitata, i risultati di ricerca visualizzeranno solo i dispositivi con descrizioni contenenti tutti i tag selezionati.

Per impostazione predefinita, questa opzione è disabilitata.

Per aggiungere tag al criterio, fare clic sul pulsante **Aggiungi** e selezionare i tag facendo clic sul campo di immissione **Tag**. Specificare se includere o escludere i dispositivi con i tag selezionati nella selezione di dispositivi.

- **Tutti i dispositivi con questo tag**

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

  Per impostazione predefinita, questa opzione è selezionata.

- **Tutti i dispositivi senza questo tag**

  Se questa opzione è selezionata, i risultati di ricerca visualizzeranno i dispositivi le cui descrizioni non contengono il tag selezionato. Per trovare i dispositivi è possibile utilizzare l'asterisco, che rappresenta qualsiasi stringa con qualsiasi numero di caratteri.

Utenti

Nella sezione **Utenti** è possibile impostare i criteri per l'inclusione dei dispositivi nella selezione in base agli account degli utenti che hanno eseguito l'accesso al sistema operativo.

- **Ultimo utente che ha eseguito l'accesso al sistema**

  Se questa opzione è abilitata, è possibile selezionare l'account utente per configurare il criterio. I risultati della ricerca includeranno i dispositivi in cui l'utente selezionato ha eseguito l'ultimo accesso al sistema.

- **Utente che ha eseguito l'accesso al sistema almeno una volta**

  Se questa opzione è abilitata, fare clic sul pulsante **Sfoglia** per specificare un account utente. I risultati della ricerca includeranno i dispositivi in cui l'utente specificato ha eseguito l'accesso al sistema almeno una volta.

Esportazione dell'elenco dei dispositivi da una selezione di dispositivi

Kaspersky Security Center consente di salvare le informazioni sui dispositivi da una selezione di dispositivi ed esportarle in un file CSV o TXT.

Per esportare l'elenco dei dispositivi dalla selezione di dispositivi:

1. Aprire la tabella con i dispositivi dalla selezione di dispositivi.
2. Utilizzare uno dei seguenti metodi per selezionare i dispositivi che si desidera esportare:
   - Per selezionare dispositivi specifici, selezionare le caselle di controllo accanto ad essi.
   - Per selezionare tutti i dispositivi dalla pagina della tabella corrente, selezionare la casella di controllo nell'intestazione della tabella dei dispositivi, quindi selezionare la casella di controllo **Seleziona tutto nella pagina corrente**.
   - Per selezionare tutti i dispositivi dalla tabella, selezionare la casella di controllo nell'intestazione della tabella dei dispositivi, quindi selezionare la casella di controllo **Seleziona tutto**.
3. Fare clic sul pulsante **Esporta in CSV** o **Esporta in TXT**. Tutte le informazioni sui dispositivi selezionati inclusi nella tabella verranno esportate.

Si noti che se è stato applicato un criterio di filtraggio alla tabella dei dispositivi, solo i dati filtrati dalle colonne visualizzate verranno esportati.

Rimozione di dispositivi dai gruppi di amministrazione in una selezione

Durante l'utilizzo di una selezione dispositivi, è possibile rimuovere i dispositivi dai gruppi di amministrazione in questa selezione senza passare ai gruppi di amministrazione da cui devono essere rimossi i dispositivi.

Per rimuovere dispositivi dai gruppi di amministrazione:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Selezioni dispositivi** o **Individuazione e distribuzione** → **Selezioni dispositivi**.
2. Nell'elenco delle selezioni fare clic sul nome della selezione di dispositivi.

   La pagina mostra una tabella con le informazioni sui dispositivi inclusi nella selezione di dispositivi.
3. Selezionare i dispositivi che si desidera rimuovere, quindi fare clic su **Elimina**.

   I dispositivi selezionati verranno rimossi dai gruppi di amministrazione corrispondenti.

Tag dispositivo

Kaspersky Security Center consente di eseguire il *tagging* dei dispositivi. Un tag è l'etichetta di un dispositivo che può essere utilizzato per raggruppare, descrivere o cercare i dispositivi. I tag assegnati ai dispositivi possono essere utilizzati per la creazione di selezioni, per il rilevamento dei dispositivi e per la distribuzione dei dispositivi tra i gruppi di amministrazione.

È possibile assegnare tag ai dispositivi in modalità manuale o automatica. Se si desidera assegnare tag a un singolo dispositivo, è possibile utilizzare l'assegnazione di tag manuale. L'assegnazione di tag automatica viene eseguita da Kaspersky Security Center in uno dei seguenti modi:

- In conformità con le regole di assegnazione di tag specificate.
- Da un'applicazione.

Non è consigliabile utilizzare modi diversi di assegnazione di tag per assegnare lo stesso tag. Ad esempio, se il tag è assegnato dalla regola, non è consigliabile assegnarlo manualmente ai dispositivi.

Se i tag sono assegnati dalle regole, i dispositivi vengono taggati automaticamente quando vengono soddisfatte le regole specificate. A ogni tag corrisponde una regola individuale. Le regole vengono applicate alle proprietà di rete del dispositivo, al sistema operativo, alle applicazioni installate nel dispositivo e ad altre proprietà del dispositivo. Se ad esempio si dispone di un'infrastruttura ibrida di macchine fisiche, istanze Amazon EC2 e macchine virtuali Microsoft Azure, è possibile impostare una regola che assegnerà il tag `[Azure]` a tutte le macchine virtuali Microsoft Azure. Sarà quindi possibile utilizzare il tag durante la creazione di una selezione dispositivi. Questo consentirà di ordinare tutte le macchine virtuali Microsoft Azure e di assegnare loro un'attività.

È possibile aggiungere solo una regola di tagging automatico per tag. Se si crea una nuova regola per lo stesso tag, la precedente verrà sostituita.

Un tag viene rimosso automaticamente da un dispositivo nei seguenti casi:

- Quando il dispositivo smette di soddisfare le condizioni della regola per l'assegnazione del tag.
- Quando la regola per l'assegnazione del tag viene disabilitata o eliminata.

L'elenco dei tag e l'elenco delle regole in ciascun Administration Server sono indipendenti da tutti gli altri Administration Server, inclusi un Administration Server primario o gli Administration Server virtuali subordinati. Una regola viene applicata solo ai dispositivi nello stesso Administration Server in cui viene creata la regola.

Creazione di un tag dispositivo

Per creare un tag dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Fare clic su **Aggiungi**.

   Verrà visualizzata una finestra per il nuovo tag.
3. Nel campo **Tag** immettere il nome del tag.
4. Fare clic su **Salva** per salvare le modifiche.

Il nuovo tag verrà visualizzato nell'elenco dei tag dispositivo.

Ridenominazione di un tag dispositivo

Per rinominare un tag dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Fare clic sul nome del tag che si desidera rinominare.

   Verrà visualizzata una finestra delle proprietà del tag.
3. Nel campo **Tag** modificare il nome del tag.
4. Fare clic su **Salva** per salvare le modifiche.

Il tag aggiornato verrà visualizzato nell'elenco dei tag dispositivo.

Eliminazione di un tag dispositivo

Per eliminare un tag dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Selezionare dall'elenco il tag dispositivo da eliminare.
3. Fare clic sul pulsante **Elimina**.
4. Nella finestra visualizzata fare clic su **Sì**.

Il tag dispositivo verrà eliminato. Il tag eliminato viene rimosso automaticamente da tutti i dispositivi a cui è stato assegnato.

Il tag eliminato non viene rimosso automaticamente dalle regole di tagging automatico. Una volta eliminato, il tag verrà assegnato a un nuovo dispositivo solo quando il dispositivo soddisfa per la prima volta le condizioni di una regola per l'assegnazione del tag.

Il tag eliminato non viene rimosso automaticamente dal dispositivo se è assegnato al dispositivo da un'applicazione o da Network Agent. Per rimuovere il tag dal dispositivo, usare l'utilità klscflag.

Visualizzazione dei dispositivi a cui è assegnato un tag

Per visualizzare i dispositivi a cui è assegnato un tag:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**.
2. Fare clic sul collegamento **Visualizza dispositivi** accanto al tag per cui si desidera visualizzare i dispositivi assegnati.

   Si verrà reindirizzati alla sezione **Dispositivi gestiti** del menu principale, con i dispositivi filtrati in base al tag per cui si è fatto clic sul collegamento **Visualizza dispositivi**.
3. Se si desidera tornare all'elenco dei tag dispositivo, fare clic sul pulsante **Indietro** del browser.

Dopo aver visualizzato i dispositivi a cui è assegnato il tag, è possibile creare e assegnare un nuovo tag o assegnare il tag esistente ad altri dispositivi. In questo caso, è necessario rimuovere il filtro in base al tag, selezionare i dispositivi e quindi assegnare il tag.

Visualizzazione dei tag assegnati a un dispositivo

Per visualizzare i tag assegnati a un dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo di cui si desidera visualizzare i tag.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Tag**.

   Verrà visualizzato l'elenco dei tag assegnati al dispositivo selezionato. Nella colonna **Tag assegnato** è possibile visualizzare come è stato assegnato il tag.

Nella barra degli strumenti è possibile eseguire le seguenti operazioni:

- Assegnare un altro tag al dispositivo.
- Rimuovere un tag già assegnato.
- Visualizzare tutti i tag dispositivo presenti in Administration Server.

Non è possibile visualizzare i tag assegnati in locale nel dispositivo.

Tagging manuale di un dispositivo

Per assegnare manualmente un tag a un dispositivo:

1. Visualizzare i tag assegnati al dispositivo a cui si desidera assegnare un altro tag.
2. Fare clic su **Aggiungi**.

3. Nella finestra visualizzata eseguire una delle seguenti operazioni:

   - Per creare e assegnare un nuovo tag, selezionare **Crea nuovo tag** e quindi specificare il nome del nuovo tag.
   - Per selezionare un tag esistente, selezionare **Assegna tag esistente** e quindi selezionare il tag desiderato nell'elenco a discesa.

4. Fare clic su **OK** per applicare le modifiche.
5. Fare clic su **Salva** per salvare le modifiche.

Il tag selezionato verrà assegnato al dispositivo.

Rimozione di un tag assegnato a un dispositivo

Per rimuovere un tag da un dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo di cui si desidera visualizzare i tag.
3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Tag**.
4. Selezionare la casella di controllo accanto al tag da rimuovere.
5. Nella parte superiore dell'elenco, fare clic sul pulsante **Annullare assegnazione tag?**.
6. Nella finestra visualizzata fare clic su **Sì**.

Il tag viene rimosso dal dispositivo.

Il tag del dispositivo di cui è stata annullata l'assegnazione non viene eliminato. Se si desidera, è possibile eliminarlo manualmente.

Non è possibile rimuovere manualmente i tag assegnati al dispositivo dalle applicazioni o da Network Agent. Per gestire questi tag, utilizzare l'utilità klscflag.

Visualizzazione delle regole per il tagging automatico dei dispositivi

Per visualizzare le regole per il tagging automatico dei dispositivi:

Eseguire una delle seguenti operazioni:

- Nel menu principale accedere a **Risorse (dispositivi)** → **Tag** → **Regole di tagging automatico**.
- Nel menu principale, passare a **Risorse (dispositivi)** → **Tag** → **Tag dispositivo**, quindi fare clic sul collegamento **Configura regole di tagging automatico**.
- Visualizzare i tag assegnati a un dispositivo e fare clic sul pulsante **Impostazioni**.

Verrà visualizzato l'elenco delle regole per il tagging automatico dei dispositivi.

Modifica di una regola per il tagging automatico dei dispositivi

Per modificare una regola per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Fare clic sul nome della regola che si desidera modificare.
   Verrà visualizzata una finestra delle impostazioni della regola.
3. Modificare le proprietà generali della regola:
   a. Nel campo **Nome regola** modificare il nome della regola.
      Il nome non può contenere più di 256 caratteri.
   b. Eseguire una delle seguenti operazioni:
      - Abilitare la regola spostando l'interruttore su **Regola abilitata**.
      - Disabilitare la regola spostando l'interruttore su **Regola disabilitata**.
4. Eseguire una delle seguenti operazioni:
   - Se si desidera aggiungere una nuova condizione, fare clic sul pulsante **Aggiungi** e specificare le impostazioni della nuova condizione nella finestra visualizzata.
   - Per modificare una condizione esistente, fare clic sul nome della condizione che si desidera modificare, quindi modificare le impostazioni della condizione.
   - Per eliminare una condizione, selezionare la casella di controllo accanto al nome della condizione da eliminare, quindi fare clic su **Elimina**.
5. Fare clic su **OK** nella finestra delle impostazioni delle condizioni.
6. Fare clic su **Salva** per salvare le modifiche.

La regola modificata verrà visualizzata nell'elenco.

Creazione di una regola per il tagging automatico dei dispositivi

Per creare una regola per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Fare clic su **Aggiungi**.
   Verrà visualizzata una finestra delle impostazioni della nuova regola.

3. Configurare le proprietà generali della regola:

   a. Nel campo **Nome regola** immettere il nome della regola.

      Il nome non può contenere più di 256 caratteri.

   b. Eseguire una delle seguenti operazioni:

      - Abilitare la regola spostando l'interruttore su **Regola abilitata**.
      - Disabilitare la regola spostando l'interruttore su **Regola disabilitata**.

   c. Nel campo **Tag** immettere il nome del nuovo tag dispositivo o selezionare uno dei tag dispositivo esistenti dall'elenco.

      Il nome non può contenere più di 256 caratteri.

4. Nella sezione delle condizioni fare clic sul pulsante **Aggiungi** per aggiungere una nuova condizione.

   Verrà visualizzata una finestra delle impostazioni della nuova condizione.

5. Immettere il nome della condizione.

   Il nome non può contenere più di 256 caratteri. Il nome deve essere univoco all'interno di una regola.

6. Configurare l'attivazione della regola in base alle seguenti condizioni. È possibile selezionare più condizioni.

   - **Rete** - Proprietà di rete del dispositivo, ad esempio il nome del dispositivo nella rete Windows o l'inclusione del dispositivo in un dominio o in una subnet IP.

     Se per il database utilizzato per Kaspersky Security Center sono impostate regole di confronto con distinzione tra maiuscole e minuscole, mantenere le maiuscole e le minuscole quando si specifica un nome DNS del dispositivo. In caso contrario, la regola di tagging automatico non funzionerà.

   - **Applicazioni** - Presenza di Network Agent nel dispositivo, tipo di sistema operativo, versione e architettura.
   - **Macchine virtuali** - Il dispositivo appartiene a un tipo specifico di macchina virtuale.
   - **Controller di dominio** - Presenza del dispositivo in un'unità organizzativa di Active Directory e appartenenza del dispositivo a un gruppo di Active Directory.
   - **Registro delle applicazioni** - Presenza di applicazioni di vari produttori nel dispositivo.

7. Fare clic su **OK** per salvare le modifiche.

   Se necessario, è possibile impostare più condizioni per una singola regola. In questo caso, il tag verrà essere assegnato a un dispositivo se soddisfa almeno una condizione.

8. Fare clic su **Salva** per salvare le modifiche.

La nuova regola creata viene applicata ai dispositivi gestiti dall'Administration Server selezionato. Se le impostazioni di un dispositivo soddisfano le condizioni della regola, al dispositivo viene assegnato il tag.

Successivamente, la regola viene applicata nei seguenti casi:

- Automaticamente e periodicamente, a seconda del carico di lavoro del server
- Dopo aver modificato la regola
- Quando si esegue la regola manualmente
- Dopo che Administration Server rileva una modifica delle impostazioni di un dispositivo che soddisfa le condizioni della regola o delle impostazioni di un gruppo che contiene tale dispositivo

È possibile creare diverse regole di tagging. A un singolo dispositivo possono essere assegnati diversi tag se sono state create più regole di tagging e se vengono contemporaneamente soddisfatte le rispettive condizioni di tali regole. È possibile visualizzare l'elenco di tutti i tag assegnati nelle proprietà del dispositivo.

Esecuzione di regole per il tagging automatico dei dispositivi

Quando viene eseguita una regola, il tag specificato nelle proprietà di questa regola è assegnato ai dispositivi che soddisfano le condizioni specificate nelle proprietà della regola. È possibile eseguire solo regole attive.

Per eseguire le regole per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Selezionare le caselle di controllo accanto alle regole attive che si desidera eseguire.
3. Fare clic sul pulsante **Esegui regola**.

Le regole selezionate verranno eseguite.

Eliminazione di una regola per il tagging automatico dei dispositivi

Per eliminare una regola per il tagging automatico dei dispositivi:

1. Visualizzare le regole per il tagging automatico dei dispositivi.
2. Selezionare la casella di controllo accanto alla regola che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Nella finestra visualizzata fare di nuovo clic su **Elimina**.

La regola selezionata verrà eliminata. L'assegnazione del tag specificato nelle proprietà di questa regola viene annullata da tutti i dispositivi a cui il tag è stato assegnato.

Il tag del dispositivo di cui è stata annullata l'assegnazione non viene eliminato. Se si desidera, è possibile eliminarlo manualmente.

Gestione dei tag del dispositivo tramite l'utilità klscflag

Per assegnare un set di tag a un dispositivo, è necessario eseguire l'utilità klscflag nel dispositivo client a cui si desidera assegnare i tag.

L'utilità klscflag sovrascrive i tag esistenti assegnati al dispositivo. Ciò significa che è possibile aggiungere o rimuovere tag specificando il set di tag desiderato nel comando. L'utilità non dispone di comandi separati per aggiungere o rimuovere singoli tag. Invece, si modifica l'intero set di tag.

Quando si specificano i nomi dei tag in comandi come klscflag, si consiglia di utilizzare un approccio coerente per quanto riguarda le maiuscole e le minuscole, ad esempio usando solo lettere maiuscole. L'utilizzo di lettere maiuscole può aiutare a evitare potenziali problemi con i tag che differiscono solo per le maiuscole e le minuscole, a seconda della configurazione del DBMS.

Per assegnare tag al dispositivo utilizzando l'utilità klscflag:

1. Eseguire il prompt dei comandi di Windows con diritti di amministratore, quindi modificare la directory corrente nella directory con l'utilità klscflag. L'utilità klscflag si trova nella cartella in cui è installato Network Agent. Il percorso di installazione predefinito è <Disk>:\Program Files (x86)\Kaspersky Lab\NetworkAgent.

2. Immettere uno dei seguenti comandi:

   - Per assegnare un set di tag:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NOME TAG 1\",\"NOME TAG 2\",\"NOME TAG 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     dove `[\"NOME TAG 1\",\"NOME TAG 2\",\"NOME TAG 3\"]` è l'elenco dei tag che si desidera assegnare al dispositivo.

     Se si lasciano vuote le parentesi quadre, verranno rimossi tutti i tag dal dispositivo:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

   - Per assegnare un nuovo tag a un set di tag esistente:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NUOVO NOME TAG\",\"NOME TAG 1\",\"NOME TAG 2\",\"NOME TAG 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     dove `NEW TAG NAME` è il nome del tag che si desidera assegnare al dispositivo e `TAG NAME 1`, `TAG NAME 2`, `TAG NAME 3` sono i nomi dei tag già assegnati al dispositivo.

   - Per rimuovere un tag specifico senza rimuovere gli altri tag già assegnati al dispositivo, eseguire il comando con il set di tag aggiornato.

     Ad esempio, se i tag correnti sono `TAG NAME 1`, `TAG NAME 2`, `TAG NAME 3` e si desidera rimuovere `TAG NAME 2`, eseguire il seguente comando:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\"NOME TAG 1\",\"NOME TAG 3\"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. Riavviare il servizio Network Agent.

   L'utilità klscflag assegna i tag specificati al dispositivo.

4. Se si desidera accertarsi che l'utilità klscflag abbia assegnato correttamente i tag specificati, visualizzare i tag assegnati al dispositivo.

In alternativa, è possibile assegnare i tag del dispositivo manualmente.

Criteri e profili criterio

In Kaspersky Security Center Web Console è possibile creare criteri per le applicazioni Kaspersky. Questa sezione descrive i criteri e i profili criterio e fornisce istruzioni per crearli e modificarli.

Informazioni su criteri e profili criterio

Un *criterio* è un set di impostazioni dell'applicazione Kaspersky che vengono applicate a un gruppo di amministrazione e ai relativi sottogruppi. È possibile installare diverse applicazioni Kaspersky nei dispositivi di un gruppo di amministrazione. Kaspersky Security Center fornisce un singolo criterio per ogni applicazione Kaspersky in un gruppo di amministrazione. Un criterio ha uno dei seguenti stati (vedere la seguente tabella):

Lo stato del criterio

Stato	Descrizione
Attivo	Il criterio corrente applicato al dispositivo. Può essere attivo un solo criterio per un'applicazione Kaspersky in ogni gruppo di amministrazione. I dispositivi applicano i valori delle impostazioni di un criterio attivo per un'applicazione Kaspersky.
Inattivo	Un criterio che non è attualmente applicato a un dispositivo.
Fuori sede	Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.

I criteri funzionano secondo le seguenti regole:

- È possibile configurare diversi criteri con differenti impostazioni per una singola applicazione.
- Un solo criterio può essere attivo per l'applicazione corrente.
- È possibile attivare un criterio inattivo quando si verifica un evento specifico. È ad esempio possibile applicare impostazioni di protezione anti-virus più rigide durante le epidemie di virus.
- Un criterio può avere criteri secondari.

In generale è possibile utilizzare i criteri in preparazione a situazioni di emergenza, come un attacco virus. Ad esempio in caso di attacco tramite unità flash, è possibile attivare un criterio che blocca l'accesso alle unità flash. In questo caso il criterio attivo corrente diventa automaticamente inattivo.

Per evitare di dover gestire più criteri, ad esempio quando diverse occasioni presuppongono solo la modifica di più impostazioni, è possibile utilizzare i profili criterio.

Un *profilo criterio* è un sottoinsieme denominato di valori delle impostazioni dei criteri che sostituisce i valori delle impostazioni di un criterio. Un profilo criterio influisce sulla creazione delle impostazioni ottimizzate in un dispositivo gestito. Per *impostazioni effettive* si intende un insieme di impostazioni dei criteri, impostazioni dei profili criterio e impostazioni delle applicazioni locali attualmente applicate nel dispositivo.

I profili criterio funzionano secondo le seguenti regole:

- Un profilo criterio assume validità quando si verifica una condizione di attivazione specifica.
- I profili criterio contengono valori delle impostazioni che differiscono dalle impostazioni dei criteri.
- L'attivazione di un profilo criterio modifica le impostazioni effettive del dispositivo gestito.
- Un criterio può includere al massimo 100 profili criterio.

Informazioni su blocco e impostazioni bloccate

Ogni impostazione dei criteri ha un'icona a forma di lucchetto (). La tabella seguente mostra gli stati dei pulsanti a forma di lucchetto:

Stati dei pulsanti a forma di lucchetto

Stato	Descrizione
Indefinito	Se accanto a un'impostazione viene visualizzato un lucchetto aperto e l'interruttore è disabilitato, l'impostazione non è specificata nel criterio. Un utente può modificare queste impostazioni nell'interfaccia dell'applicazione gestita. Questa tipologia di impostazioni è denominata *sbloccata*.
Applica	Se accanto a un'impostazione viene visualizzato un lucchetto chiuso e l'interruttore è abilitato, l'impostazione viene applicata ai dispositivi ai quali si applica il criterio. Un utente non può modificare i valori di queste impostazioni nell'interfaccia dell'applicazione gestita. Questa tipologia di impostazioni è denominata *bloccata*.

È consigliabile bloccare le impostazioni dei criteri che si desidera applicare ai dispositivi gestiti. Le impostazioni dei criteri sbloccate possono essere riassegnate dalle impostazioni dell'applicazione Kaspersky in un dispositivo gestito.

È possibile utilizzare un pulsante a forma di lucchetto per eseguire le seguenti azioni:

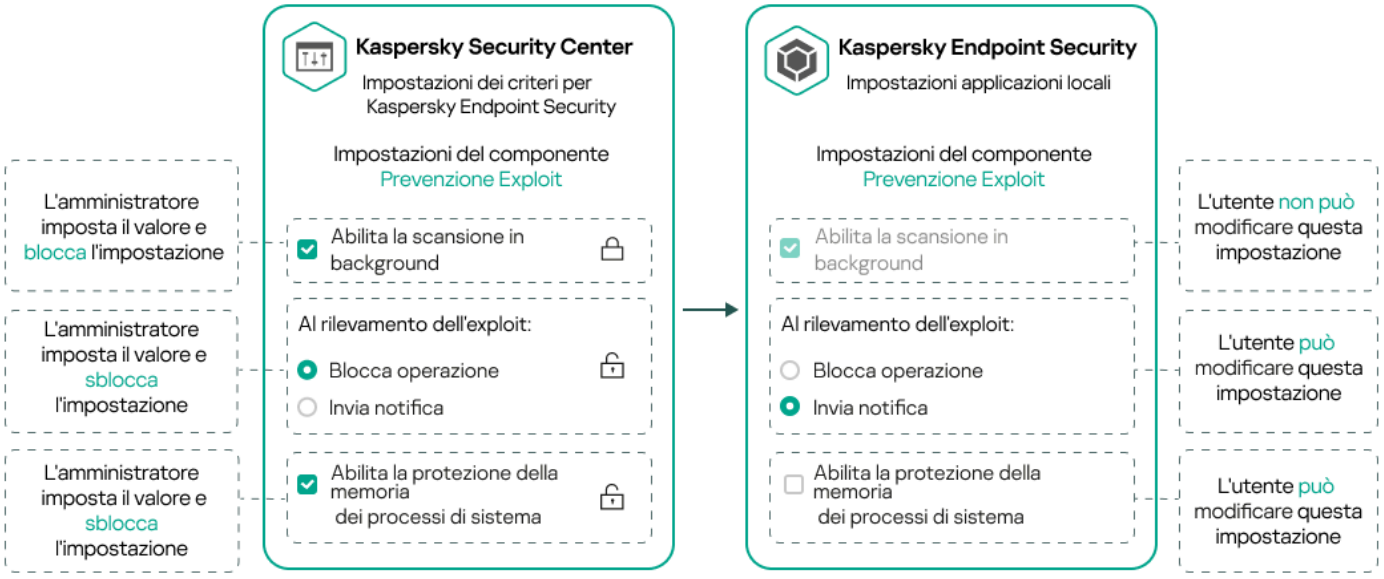
- Blocco delle impostazioni per il criterio di un sottogruppo di amministrazione
- Blocco delle impostazioni di un'applicazione Kaspersky in un dispositivo gestito

Un'impostazione bloccata viene pertanto utilizzata per implementare impostazioni ottimizzate in un dispositivo gestito.

Un processo di implementazione delle impostazioni ottimizzate include le seguenti azioni:

- Il dispositivo gestito applica i valori delle impostazioni dell'applicazione Kaspersky.
- Il dispositivo gestito applica i valori delle impostazioni bloccate di un criterio.

Un criterio e un'applicazione Kaspersky gestita contengono lo stesso set di impostazioni. Quando si configurano le impostazioni dei criteri, le impostazioni dell'applicazione Kaspersky assumono valori differenti in un dispositivo gestito. Non è possibile regolare le impostazioni bloccate in un dispositivo gestito (vedere la figura seguente):



Blocchi e impostazioni delle applicazioni Kaspersky

Ereditarietà di criteri e profili criterio

Questa sezione fornisce informazioni sulla gerarchia e sull'ereditarietà dei criteri e dei profili criterio.

Gerarchia dei criteri

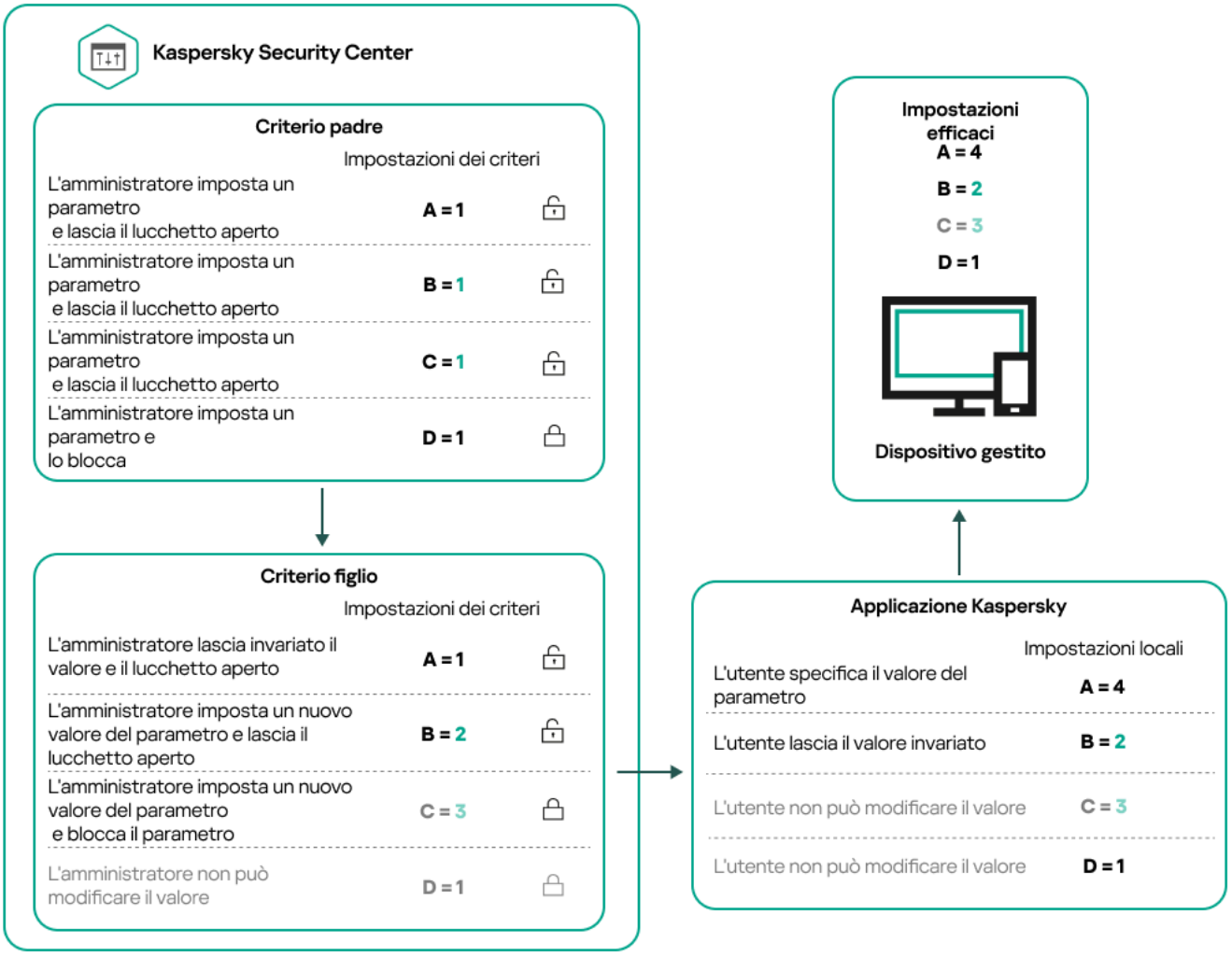
Se dispositivi diversi richiedono impostazioni diverse, è possibile organizzare i dispositivi in gruppi di amministrazione.

È possibile specificare un criterio per un singolo gruppo di amministrazione. Le impostazioni dei criteri possono essere *ereditate*. Ereditarietà significa ricevere i valori delle impostazioni dei criteri nei sottogruppi (gruppi secondari) di un criterio di un gruppo di amministrazione (principale) di livello superiore.

Da questo momento in poi, un criterio per un gruppo padre viene denominato anche *criterio principale*. Un criterio per un sottogruppo (gruppo figlio) viene inoltre denominato *criterio secondario*.

Per impostazione predefinita, esiste almeno un gruppo di dispositivi gestiti in Administration Server. Se si desidera creare gruppi personalizzati, questi vengono creati come sottogruppi (gruppi figlio) all'interno del gruppo di dispositivi gestiti.

I criteri della stessa applicazione si influenzano reciprocamente in base a una gerarchia di gruppi di amministrazione. Le impostazioni bloccate di un criterio di un gruppo di amministrazione di livello superiore (padre) riassegneranno i valori delle impostazioni dei criteri di un sottogruppo (vedere la figura seguente).

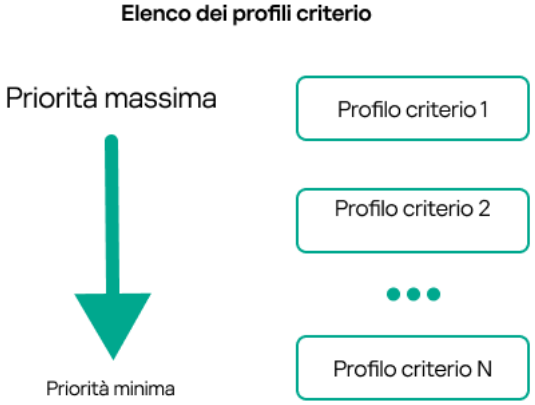


Gerarchia dei criteri

Profili criterio in una gerarchia di criteri

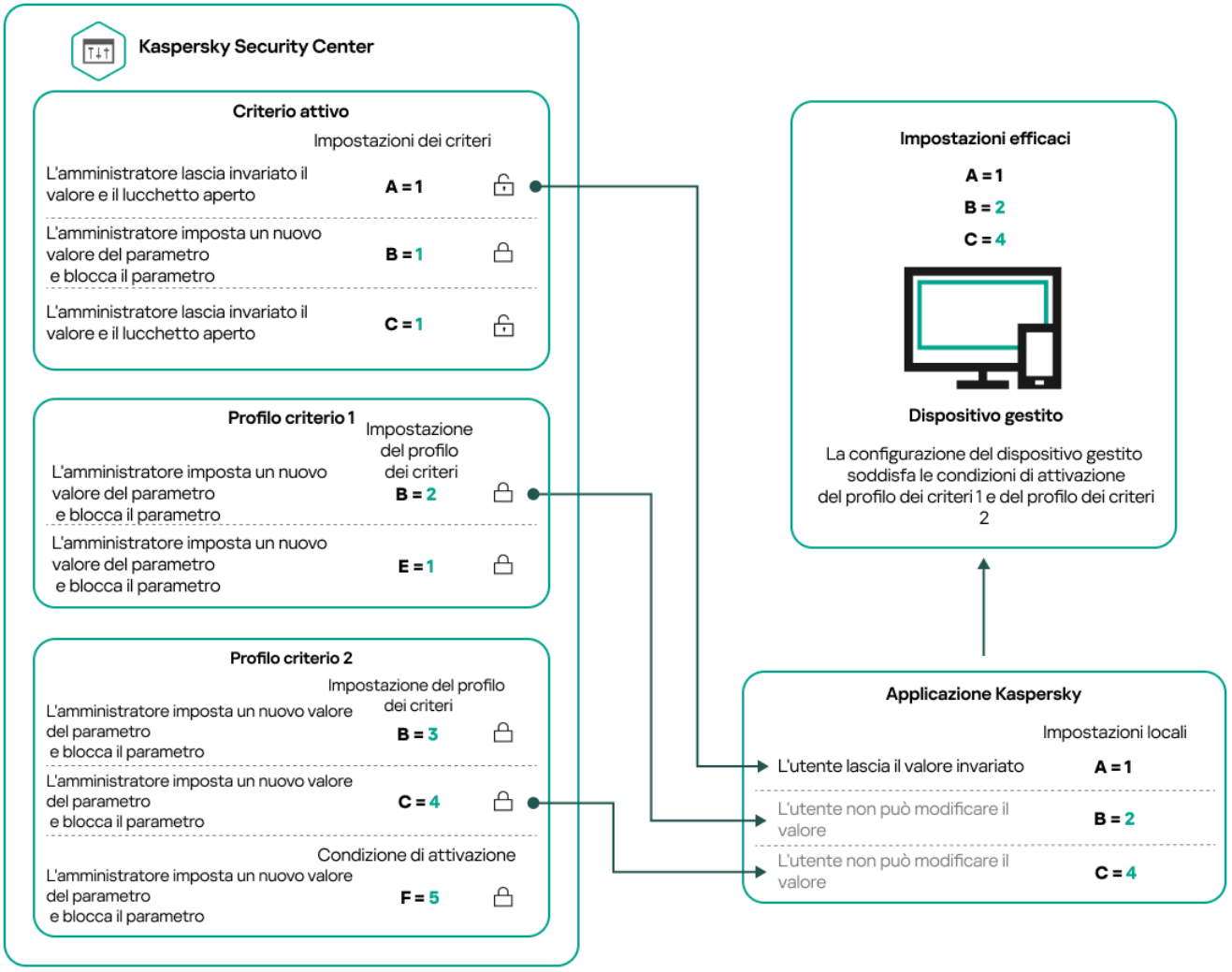
I profili criterio hanno le seguenti condizioni di assegnazione della priorità:

- La posizione di un profilo in un elenco di profili criterio indica la relativa priorità. È possibile modificare la priorità di un profilo criterio. La posizione più elevata in un elenco indica la massima priorità (vedere la figura seguente).



Definizione della priorità di un profilo criterio

- Le condizioni di attivazione dei profili criterio non dipendono l'una dall'altra. È possibile attivare più profili criterio contemporaneamente. Se più profili criterio influiscono sulla stessa impostazione, il dispositivo acquisisce il valore dell'impostazione dal profilo criterio con la priorità più elevata (vedere la figura seguente).

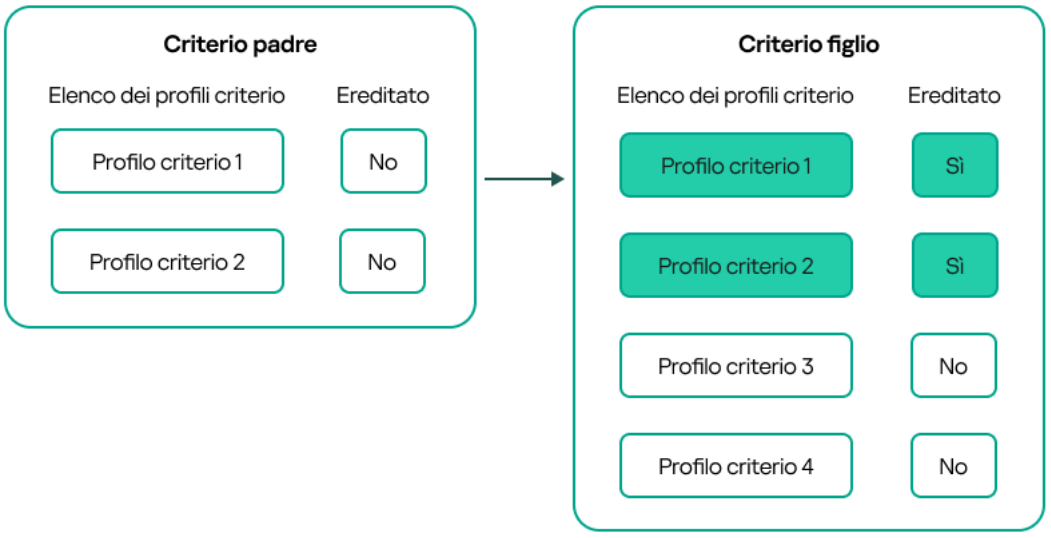


La configurazione del dispositivo gestito soddisfa le condizioni di attivazione di diversi profili criterio

Profili criterio in una gerarchia di ereditarietà

I profili criterio di diversi criteri di livello gerarchico soddisfano le seguenti condizioni:

- Un criterio di livello inferiore eredita i profili criterio da un criterio di livello superiore. Un profilo criterio ereditato da un criterio di livello superiore ottiene una priorità più elevata rispetto al livello del profilo criterio originale.
- Non è possibile modificare la priorità di un profilo criterio ereditato (vedere la figura seguente).

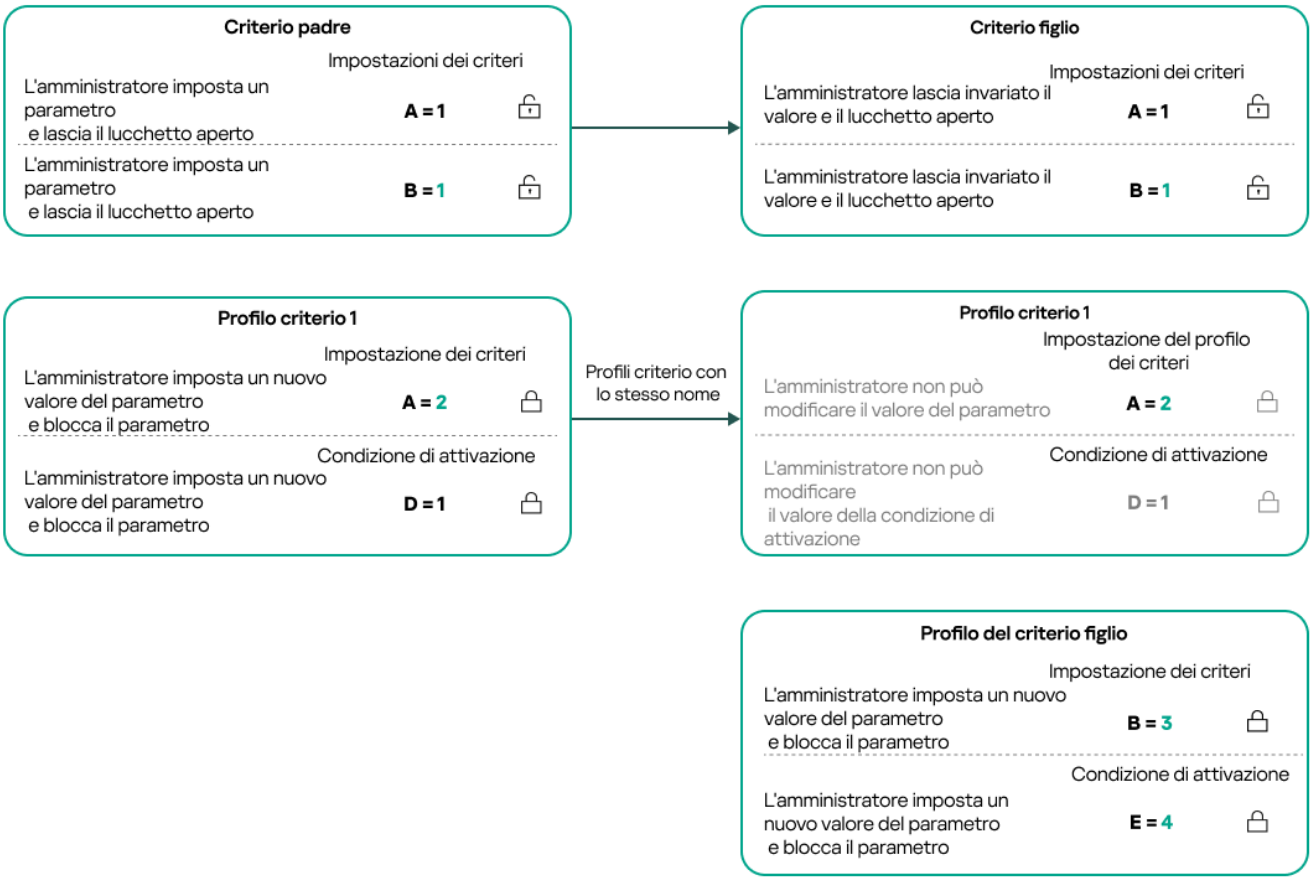


Ereditarietà dei profili criterio

Profili criterio con lo stesso nome

Se sono presenti due criteri con lo stesso nome in diversi livelli della gerarchia, questi criteri funzionano in base alle seguenti regole:

- Le impostazioni bloccate e la condizione di attivazione di un profilo criterio di livello superiore modificano le impostazioni e la condizione di attivazione di un profilo criterio di livello inferiore (vedere la figura seguente).



Il profilo figlio eredita i valori delle impostazioni da un profilo criterio principale

- Le impostazioni sbloccate e la condizione di attivazione di un profilo criterio di livello superiore non modificano le impostazioni e la condizione di attivazione di un profilo criterio di livello inferiore.

Modalità di implementazione delle impostazioni in un dispositivo gestito

L'implementazione di impostazioni ottimizzate in un dispositivo gestito può essere descritta come segue:

- I valori di tutte le impostazioni non bloccate vengono acquisiti dal criterio.
- Quindi vengono sovrascritti con i valori delle impostazioni dell'applicazione gestita.
- Vengono applicati i valori delle impostazioni bloccate del criterio ottimizzato. I valori delle impostazioni bloccate modificano i valori delle impostazioni ottimizzate sbloccate.

Gestione dei criteri

Questa sezione descrive i criteri di gestione e fornisce informazioni sulla visualizzazione dell'elenco dei criteri, sulla creazione di un criterio, sulla modifica di un criterio, sulla copia di un criterio, sullo spostamento di un criterio, sulla sincronizzazione forzata, sulla visualizzazione del grafico dello stato di distribuzione dei criteri e sull'eliminazione di un criterio.

Visualizzazione dell'elenco di criteri

È possibile visualizzare elenchi dei criteri creati per Administration Server o per qualsiasi gruppo di amministrazione.

Per visualizzare un elenco di criteri:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nella struttura dei gruppi di amministrazione selezionare il gruppo di amministrazione per cui si desidera visualizzare l'elenco di criteri.

L'elenco di criteri viene visualizzato in formato di tabella. Se non sono presenti criteri, la tabella è vuota. È possibile mostrare o nascondere le colonne della tabella, modificarne l'ordine, visualizzare solo le righe che contengono un valore specificato o utilizzare la ricerca.

Creazione di un criterio

È possibile creare criteri, nonché modificare ed eliminare i criteri esistenti.

Per creare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare il gruppo di amministrazione per cui creare il criterio:
   - Per il gruppo radice.

     In questo caso, è possibile procedere al passaggio successivo.
   - Per un sottogruppo:

     a. Fare clic sul collegamento del percorso corrente nella parte superiore della finestra.

     b. Nel pannello visualizzato, fare clic sul collegamento con il nome del sottogruppo desiderato.

     Il percorso corrente cambia per riflettere il sottogruppo selezionato.
3. Fare clic su **Aggiungi**.

   Verrà aperta la finestra **Selezionare l'applicazione**.
4. Selezionare l'applicazione per cui si desidera creare un criterio.

5. Fare clic su **Avanti**.

   Verrà visualizzata la finestra delle impostazioni del nuovo criterio, con la scheda **Generale** selezionata.

6. Se si desidera, modificare il nome predefinito, lo stato predefinito e le impostazioni di ereditarietà predefinite del criterio.

7. Selezionare la scheda **Impostazioni applicazione**.

   In alternativa, fare clic su **Salva** e uscire. Il criterio verrà visualizzato nell'elenco dei criteri e sarà possibile modificarne le impostazioni in un secondo momento.

8. Nella scheda **Impostazioni applicazione**, nel riquadro a sinistra selezionare la categoria desiderata e nel riquadro dei risultati a destra modificare le impostazioni del criterio. È possibile modificare le impostazioni del criterio in ciascuna categoria (sezione).

   Il set di impostazioni dipende dall'applicazione per cui si crea un criterio. Per i dettagli, fare riferimento ai seguenti elementi:

   - Configurazione di Administration Server
   - Impostazioni del criterio di Network Agent
   - Documentazione di Kaspersky Endpoint Security for Windows

   Per informazioni dettagliate sulle impostazioni delle altre applicazioni di protezione, fare riferimento alla documentazione relativa all'applicazione corrispondente.

   Quando si modificano le impostazioni, è possibile fare clic su **Annulla** per annullare l'ultima operazione.

9. Fare clic su **Salva** per salvare il criterio.

Il criterio verrà visualizzato nell'elenco dei criteri.

Modifica di un criterio

Per modificare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

2. Fare clic sul criterio che si desidera modificare.

   Verrà visualizzata la finestra delle impostazioni del criterio.

3. Specificare le impostazioni generali e le impostazioni dell'applicazione per cui si crea un criterio. Per i dettagli, fare riferimento ai seguenti elementi:

   - Configurazione di Administration Server
   - Impostazioni del criterio di Network Agent
   - Documentazione di Kaspersky Endpoint Security for Windows

   Per informazioni dettagliate sulle impostazioni delle altre applicazioni di protezione, fare riferimento alla documentazione relativa a tale applicazione.

4. Fare clic su **Salva**.

Le modifiche apportate al criterio saranno salvate nelle proprietà del criterio e verranno visualizzate nella sezione **Cronologia revisioni**.

Impostazioni generali dei criteri

Generale

Nella scheda **Generale** è possibile modificare lo stato del criterio e specificare l'ereditarietà delle impostazioni criterio:

- Nella sezione **Stato criterio** è possibile selezionare una modalità criterio:
  - **Attivo**

    Se questa opzione è selezionata, il criterio diventa attivo.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Fuori sede**

    Se questa opzione è selezionata, il criterio diventa attivo quando il dispositivo lascia la rete aziendale.

  - **Inattivo**

    Se questa opzione è selezionata, il criterio diventa inattivo, ma viene comunque salvato nella cartella **Criteri**. Se necessario, il criterio può essere attivato.

- Nel gruppo di impostazioni **Ereditarietà impostazioni** è possibile configurare l'ereditarietà del criterio:
  - **Eredita impostazioni dal criterio padre**

    Se questa opzione è abilitata, i valori delle impostazioni del criterio vengono ereditati dal criterio di gruppo di livello superiore e pertanto vengono bloccati.

    Per impostazione predefinita, questa opzione è abilitata.

  - **Forza ereditarietà impostazioni nei criteri figlio**

    Se questa opzione è abilitata, una volta applicate le modifiche ai criteri, verranno eseguite le seguenti azioni:

    - I valori delle impostazioni dei criteri saranno propagati ai criteri dei sottogruppi di amministrazione, ovvero ai criteri secondari.
    - Nel gruppo **Ereditarietà impostazioni** della sezione **Generale** nella finestra delle proprietà di ogni criterio secondario, l'opzione **Eredita impostazioni dal criterio principale** sarà abilitata automaticamente.

    Se questa opzione è abilitata, le impostazioni dei criteri secondari vengono bloccate.

    Per impostazione predefinita, questa opzione è disabilitata.

Configurazione eventi

La scheda **Configurazione eventi** consente di configurare la registrazione degli eventi e le notifiche degli eventi. Gli eventi vengono distribuiti nelle seguenti schede in base al livello di importanza:

- **Critico**

  La sezione **Critico** non è visualizzata nelle proprietà del criterio di Network Agent.

- **Errore funzionale**
- **Avviso**
- **Informazioni**

In ogni sezione, l'elenco mostra i tipi di eventi e il periodo di archiviazione predefinito per gli eventi in Administration Server (in giorni). Facendo clic su un tipo di evento, è possibile specificare le seguenti impostazioni:

- **Registrazione eventi**

  È possibile specificare per quanti giorni archiviare l'evento e selezionare dove archiviarlo:

  - **Esporta nel sistema SIEM utilizzando Syslog**
  - **Archivia nel registro eventi del sistema operativo del dispositivo**
  - **Archivia nel registro eventi del sistema operativo in Administration Server**

- **Notifiche eventi**

  È possibile selezionare se si desidera essere informati dell'evento in uno dei seguenti modi:

  - **Notifica tramite e-mail**
  - **Notifica tramite SMS**
  - **Notifica tramite l'esecuzione di file eseguibile o script**
  - **Notifica tramite SNMP**

  Per impostazione predefinita, vengono utilizzate le impostazioni di notifica specificate nella scheda delle proprietà di Administration Server (ad esempio l'indirizzo del destinatario). Se si desidera, è possibile modificare queste impostazioni nelle schede **E-mail**, **SMS** e **File eseguibile da avviare**.

Cronologia revisioni

La scheda **Cronologia revisioni** consente di visualizzare l'elenco delle revisioni del criterio ed eseguire il rollback delle modifiche apportate al criterio, se necessario.

Abilitazione e disabilitazione di un'opzione di ereditarietà dei criteri

Per abilitare o disabilitare l'opzione di ereditarietà in un criterio:

1. Aprire il criterio richiesto.
2. Aprire la scheda **Generale**.
3. Abilitare o disabilitare l'ereditarietà dei criteri:
   - Se si abilita **Eredita impostazioni dal criterio padre** in un criterio secondario e un amministratore blocca alcune impostazioni nel criterio principale, non è possibile modificare queste impostazioni nel criterio secondario.
   - Se si disabilita **Eredita impostazioni dal criterio padre** in un criterio secondario, è possibile modificare tutte le impostazioni nel criterio secondario, anche se alcune impostazioni sono bloccate nel criterio principale.
   - Se si abilita **Forza ereditarietà impostazioni nei criteri figlio** nel gruppo padre, viene abilitata l'opzione **Eredita impostazioni dal criterio padre** per tutti i criteri secondari. In questo caso, non è possibile disabilitare questa opzione per nessun criterio secondario. Tutte le impostazioni bloccate nel criterio principale vengono ereditate forzatamente nei gruppi figlio e non è possibile modificare queste impostazioni nei gruppi figlio.
4. Fare clic sul pulsante **Salva** per salvare le modifiche o fare clic sul pulsante **Annulla** per rifiutare le modifiche.

Per impostazione predefinita, l'opzione **Eredita impostazioni dal criterio padre** è abilitata per un nuovo criterio.

Se un criterio dispone di profili, tutti i criteri secondari ereditano tali profili.

Copia di un criterio

È possibile copiare i criteri da un gruppo di amministrazione a un altro.

Per copiare un criterio in un altro gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio (o ai criteri) che si desidera copiare.
3. Fare clic sul pulsante **Copia**.

   Sul lato destro dello schermo verrà visualizzata la struttura dei gruppi di amministrazione.
4. Nella struttura selezionare il gruppo di destinazione, ovvero il gruppo in cui si desidera copiare il criterio (o i criteri).
5. Fare clic sul pulsante **Copia** nella parte inferiore dello schermo.
6. Fare clic su **OK** per confermare l'operazione.

I criteri verranno copiati nel gruppo di destinazione con tutti i relativi profili. Lo stato di ciascun criterio copiato nel gruppo di destinazione sarà **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

Se un criterio con lo stesso nome del nuovo criterio spostato è già incluso nel gruppo di destinazione, al nome del nuovo criterio spostato viene aggiunto l'indice (<numero progressivo successivo>), ad esempio: (1).

Spostamento di un criterio

È possibile spostare i criteri da un gruppo di amministrazione a un altro. Ad esempio, si desidera eliminare un gruppo, ma utilizzare i relativi criteri per un altro gruppo. In questo caso, è possibile spostare il criterio dal gruppo precedente a quello nuovo prima di eliminare il gruppo precedente.

Per spostare un criterio in un altro gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio (o ai criteri) che si desidera spostare.
3. Fare clic sul pulsante **Sposta**.

   Sul lato destro dello schermo verrà visualizzata la struttura dei gruppi di amministrazione.
4. Nella struttura selezionare il gruppo di destinazione, ovvero il gruppo in cui si desidera spostare il criterio (o i criteri).
5. Fare clic sul pulsante **Sposta** nella parte inferiore dello schermo.
6. Fare clic su **OK** per confermare l'operazione.

   Se un criterio non è ereditato dal gruppo di origine, verrà spostato nel gruppo di destinazione con tutti i relativi profili. Lo stato del criterio nel gruppo di destinazione è **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

   Se un criterio è ereditato dal gruppo di origine, rimane nel gruppo di origine. Viene copiato nel gruppo di destinazione con tutti i relativi profili. Lo stato del criterio nel gruppo di destinazione è **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

Se un criterio con lo stesso nome del nuovo criterio spostato è già incluso nel gruppo di destinazione, al nome del nuovo criterio spostato viene aggiunto l'indice (<numero progressivo successivo>), ad esempio: (1).

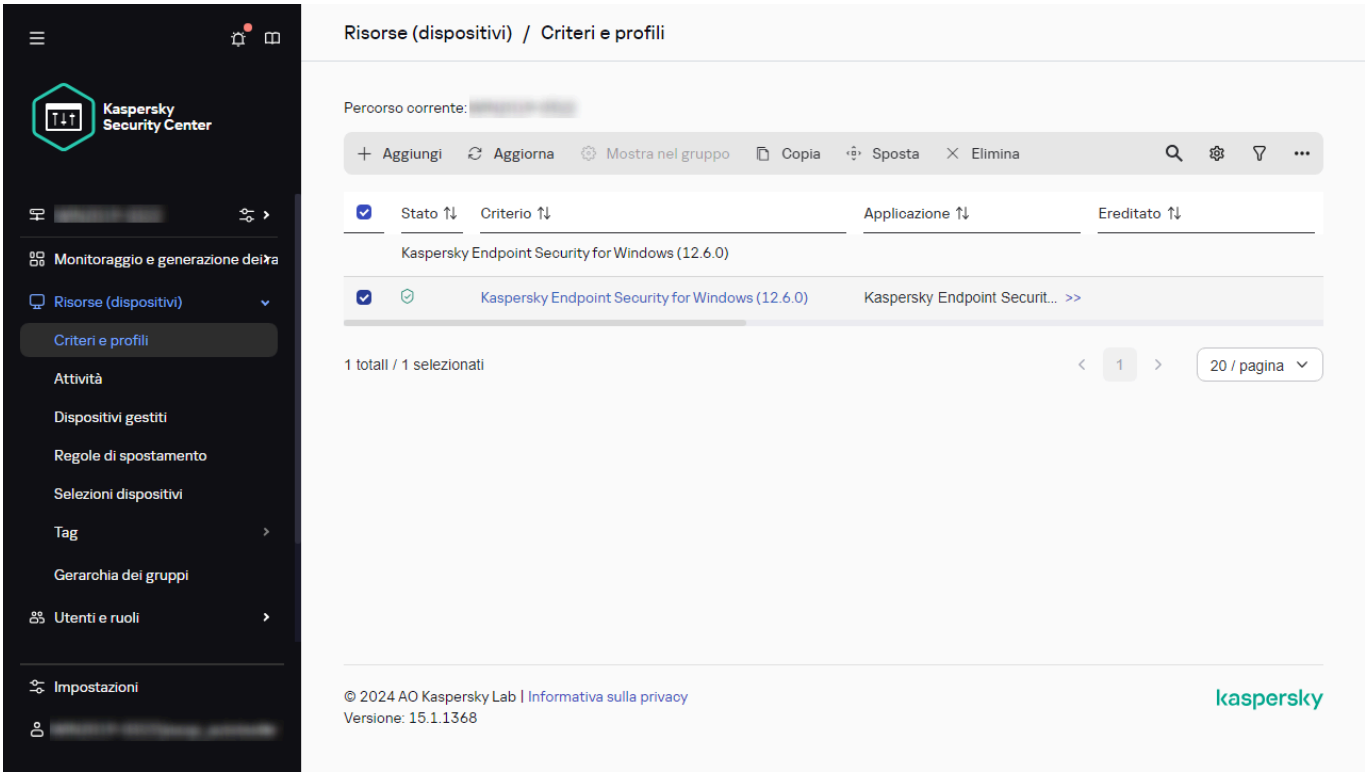
Esportazione di un criterio

Kaspersky Security Center consente di salvare un criterio, le relative impostazioni e i profili dei criteri in un file KLP. È possibile utilizzare questo file KLP per importare il criterio salvato sia per Kaspersky Security Center Windows che per Kaspersky Security Center Linux.

Per esportare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio che si desidera esportare.

   Non è possibile esportare più criteri contemporaneamente. Se si selezionano più criteri, il pulsante **Esporta** verrà disabilitato.



3. Fare clic sul pulsante **Esporta**.
4. Nella finestra **Salva con nome** visualizzata, specificare il percorso e il nome del file di criteri. Fare clic sul pulsante **Salva**.

   La finestra **Salva con nome** viene visualizzata solo se si utilizza Google Chrome, Microsoft Edge oppure Opera. Se si utilizza un altro browser, il criterio di attività viene salvato automaticamente nella cartella **Download**.

Importazione di un criterio

Kaspersky Security Center consente di importare un criterio da un file KLP. Il file KLP contiene il criterio esportato, le relative impostazioni e i profili dei criteri.

Per importare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul pulsante **Importa**.
3. Fare clic sul pulsante **Sfoglia** per scegliere un file di criteri da importare.
4. Nella finestra visualizzata, specificare il percorso del file di criteri KLP, quindi fare clic sul pulsante **Apri**. Si noti che è possibile selezionare solo un file di criteri.

   Viene avviata l'elaborazione del criterio.

5. Dopo che il criterio è stato elaborato correttamente, selezionare il gruppo di amministrazione a cui si desidera applicare il criterio.

6. Fare clic sul pulsante **Completa** per completare l'importazione del criterio.

Viene visualizzata la notifica con i risultati dell'importazione. Se il criterio viene importato correttamente, è possibile fare clic sul collegamento **Dettagli** per visualizzare le proprietà del criterio.

Dopo un'importazione riuscita, il criterio viene visualizzato nell'elenco dei criteri. Vengono importati anche le impostazioni e i profili del criterio. Indipendentemente dallo stato del criterio selezionato durante l'esportazione, il criterio importato è inattivo. È possibile modificare lo stato del criterio nelle proprietà del criterio.

Se il criterio appena importato ha un nome identico a quello di un criterio esistente, il nome del criterio importato viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Visualizzazione del grafico dello stato di distribuzione dei criteri

In Kaspersky Security Center è possibile visualizzare lo stato dell'applicazione dei criteri in ogni dispositivo in un grafico dello stato di distribuzione dei criteri.

Per visualizzare lo stato di distribuzione dei criteri in ogni dispositivo:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

2. Selezionare la casella di controllo accanto al nome del criterio per cui si desidera visualizzare lo stato di distribuzione nei dispositivi.

3. Nel menu visualizzato selezionare il collegamento **Distribuzione**.

   Verrà visualizzata la finestra **Risultati della distribuzione di <Nome criterio>**.

4. Nella finestra **Risultati della distribuzione di <Nome criterio>** visualizzata viene visualizzata la **descrizione dello stato** del criterio.

È possibile modificare il numero di risultati visualizzati nell'elenco con la distribuzione dei criteri. Il numero massimo di dispositivi è 100.000.

Per modificare il numero dei dispositivi visualizzati nell'elenco con i risultati di distribuzione dei criteri:

1. Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Opzioni di interfaccia**.

2. In **Limite di dispositivi visualizzati nei risultati di distribuzione criteri**, immettere il numero di dispositivi (fino a 100.000).

   Il numero predefinito è 5000.

3. Fare clic su **Salva**.

   Le impostazioni verranno salvate e applicate.

Eliminazione di un criterio

È possibile eliminare un criterio se non è più necessario. Può essere eliminato solo un criterio che non viene ereditato nel gruppo di amministrazione specificato. Se un criterio viene ereditato, è possibile eliminarlo solo nel gruppo di livello superiore per cui è stato creato.

Per eliminare un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Selezionare la casella di controllo accanto al criterio che si desidera eliminare e fare clic su **Elimina**.

   Il pulsante **Elimina** diventa non disponibile (visualizzato in grigio) se si seleziona un criterio ereditato.
3. Fare clic su **OK** per confermare l'operazione.

Il criterio verrà eliminato insieme a tutti i relativi profili.

Gestione dei profili criterio

Questa sezione illustra la gestione dei profili criterio e fornisce informazioni sulla visualizzazione dei profili di un criterio, sulla modifica della priorità di un profilo criterio, sulla creazione di un profilo criterio, sulla modifica di un profilo criterio, sulla copia di un profilo criterio, sulla creazione di una regola di attivazione del profilo criterio e sull'eliminazione di un profilo criterio.

Visualizzazione dei profili di un criterio

Per visualizzare i profili di un criterio:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul nome del criterio di cui si desidera visualizzare i profili.

   Verrà visualizzata la finestra delle proprietà del criterio, con la scheda **Generale** selezionata.
3. Aprire la scheda **Profili criterio**.

L'elenco dei profili criterio viene visualizzato in formato di tabella. Se il criterio non dispone di profili, viene visualizzata una tabella vuota.

Modifica della priorità di un profilo criterio

Per modificare la priorità di un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.
2. Nella scheda **Profili criterio** selezionare la casella di controllo accanto al profilo criterio per cui si desidera modificare la priorità.

3. Impostare una nuova posizione del profilo criterio nell'elenco facendo clic su **Assegna priorità** o **Annulla priorità**.

   Più in alto è posizionato un profilo criterio nell'elenco, maggiore è la relativa priorità.

4. Fare clic sul pulsante **Salva**.

La priorità del profilo criterio selezionato verrà modificata e applicata.

Creazione di un profilo criterio

Per creare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio. Se il criterio non dispone di profili, viene visualizzata una tabella vuota.

2. Fare clic su **Aggiungi**.

3. Se si desidera, modificare il nome predefinito e le impostazioni di ereditarietà predefinite del profilo.

4. Selezionare la scheda **Impostazioni applicazione**.

   In alternativa, fare clic su **Salva** e uscire. Il profilo che è stato creato viene visualizzato nell'elenco dei profili criterio e sarà possibile modificarne le impostazioni in un secondo momento.

5. Nella scheda **Impostazioni applicazione**, nel riquadro a sinistra selezionare la categoria desiderata e nel riquadro dei risultati a destra modificare le impostazioni per il profilo. È possibile modificare le impostazioni del profilo criterio in ciascuna categoria (sezione).

   Quando si modificano le impostazioni, è possibile fare clic su **Annulla** per annullare l'ultima operazione.

6. Fare clic su **Salva** per salvare il profilo.

Il profilo verrà visualizzato nell'elenco dei profili criterio.

Modifica di un profilo criterio

La possibilità di modificare un profilo criterio è disponibile solo per i criteri di Kaspersky Endpoint Security for Windows.

Per modificare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.

2. Nella scheda **Profili criterio** fare clic sul profilo criterio che si desidera modificare.

   Verrà visualizzata la finestra delle proprietà del profilo criterio.

3. Configurare il profilo nella finestra delle proprietà:

   - Se necessario, nella scheda **Generale** modificare il nome del profilo e abilitare o disabilitare il profilo.
   - Modificare le regole di attivazione del profilo.
   - Modificare le impostazioni dell'applicazione.

   Per informazioni dettagliate sulle impostazioni delle applicazioni di protezione, consultare la documentazione dell'applicazione corrispondente.

4. Fare clic su **Salva**.

Le impostazioni modificate diventeranno effettive dopo la sincronizzazione del dispositivo con Administration Server (se il profilo criterio è attivo) o dopo l'esecuzione di una regola di attivazione (se il profilo criterio è inattivo).

Copia di un profilo criterio

È possibile copiare un profilo criterio nel criterio corrente o in un altro, ad esempio se si desidera avere profili identici per criteri diversi. È anche possibile utilizzare la copia per disporre di due o più profili che differiscono solo per un numero limitato di impostazioni.

Per copiare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio. Se il criterio non dispone di profili, viene visualizzata una tabella vuota.

2. Nella scheda **Profili criterio** selezionare il profilo criterio che si desidera copiare.
3. Fare clic su **Copia**.
4. Nella finestra visualizzata selezionare il criterio in cui si desidera copiare il profilo.

   È possibile copiare un profilo criterio nello stesso criterio o in un criterio specificato.

5. Fare clic su **Copia**.

Il profilo criterio verrà copiato nel criterio selezionato. Il nuovo profilo copiato ha la priorità più bassa. Se si copia il profilo nello stesso criterio, al nome del nuovo profilo copiato viene aggiunto l'indice (), ad esempio: (1), (2).

Successivamente, è possibile modificare le impostazioni del profilo, inclusi il nome e la priorità. In questo caso, il profilo criterio originale non verrà modificato.

Creazione di una regola di attivazione del profilo criterio

Per creare una regola di attivazione per un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.

2. Nella scheda **Profili criterio** fare clic sul profilo criterio per cui è necessario creare una regola di attivazione.

   Se l'elenco dei profili criterio è vuoto, è possibile creare un profilo criterio.

3. Nella scheda **Regole di attivazione** fare clic sul pulsante **Aggiungi**.

   Verrà visualizzata la finestra con le regole di attivazione del profilo criterio.

4. Specificare un nome per la regola.

5. Selezionare le caselle di controllo accanto alle condizioni che devono determinare l'attivazione del profilo criterio che si sta creando:

- **Regole generali per l'attivazione del profilo criterio**

  Selezionare questa casella di controllo per configurare le regole di attivazione del profilo criterio nel dispositivo in base allo stato della modalità offline del dispositivo, alla regola per la connessione ad Administration Server e ai tag assegnati al dispositivo.

  Per questa opzione, specificare al passaggio successivo:

  - **Stato dispositivo**

    Definisce la condizione per la presenza del dispositivo nella rete:

    - **Online** - Il dispositivo è presente nella rete, pertanto Administration Server è disponibile.
    - **Offline** - Il dispositivo si trova in una rete esterna, pertanto Administration Server non è disponibile.
    - **N/D** - Il criterio non verrà applicato.

  - **La regola per la connessione ad Administration Server è attiva su questo dispositivo**

    Scegliere la condizione di attivazione del profilo criterio (se la regola viene eseguita o meno) e selezionare il nome della regola.

    La regola definisce il percorso di rete del dispositivo per la connessione ad Administration Server, le cui condizioni devono essere soddisfatte (o non devono essere soddisfatte) per l'attivazione del profilo criterio.

    È possibile creare o configurare una descrizione del percorso di rete dei dispositivi per la connessione a un Administration Server in una regola per il passaggio di Network Agent.

- **Regole per il proprietario di un dispositivo specifico**

  Per questa opzione, specificare al passaggio successivo:

  - **Proprietario dispositivo**

    Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al proprietario. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

    - Il dispositivo appartiene al proprietario specificato (segno "=").
    - Il dispositivo non appartiene al proprietario specificato (segno "#").

      Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il proprietario dispositivo quando l'opzione è abilitata. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

  - **Il proprietario dispositivo fa parte di un gruppo di protezione interno**

Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base all'appartenenza del proprietario a un gruppo di protezione interno di Kaspersky Security Center. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:

- Il proprietario dispositivo è un membro del gruppo di protezione specificato (segno "=").
- Il proprietario dispositivo non è un membro del gruppo di protezione specificato (segno "#").

  Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare un gruppo di protezione di Kaspersky Security Center. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Regole per le specifiche hardware**

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base al volume della memoria e al numero di processori logici.

  Per questa opzione, specificare al passaggio successivo:

  - **Dimensione RAM (MB)**

    Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al volume della RAM disponibile in tale dispositivo. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:
    - Le dimensioni della RAM del dispositivo sono inferiori al valore specificato (segno "<").
    - Le dimensioni della RAM del dispositivo sono superiori al valore specificato (segno ">").

    Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il volume della RAM nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

  - **Numero di processori logici**

    Abilitare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo in base al numero di processori logici nel dispositivo. Nell'elenco a discesa sotto la casella di controllo è possibile selezionare un criterio per l'attivazione del profilo:
    - Il numero di processori logici nel dispositivo è inferiore o uguale al valore specificato (segno "<").
    - Il numero di processori logici nel dispositivo è superiore o uguale al valore specificato (segno ">").

    Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato. È possibile specificare il numero di processori logici nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Regole per l'assegnazione dei ruoli**

  Per questa opzione, specificare al passaggio successivo:

Attiva il profilo criterio in base allo specifico ruolo del proprietario del dispositivo

Selezionare questa opzione per configurare e abilitare la regola di attivazione del profilo nel dispositivo a seconda del ruolo del proprietario. Aggiungere manualmente il ruolo dall'elenco dei ruoli esistenti.

Se questa opzione è abilitata, il profilo viene attivato nel dispositivo in base al criterio configurato.

- Regole per l'utilizzo dei tag

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base ai tag assegnati al dispositivo. È possibile attivare il profilo criterio nei dispositivi che dispongono o che non dispongono dei tag selezionati.

  Per questa opzione, specificare al passaggio successivo:

  - Tag

    Nell'elenco di tag specificare una regola per l'inclusione dei dispositivi nel profilo criterio selezionando le caselle di controllo accanto ai tag appropriati.

    È possibile aggiungere nuovi tag all'elenco immettendoli nel campo sopra l'elenco e facendo clic sul pulsante **Aggiungi**.

    Il profilo criterio include i dispositivi con descrizioni che contengono tutti i tag selezionati. Se le caselle di controllo sono deselezionate, il criterio non viene applicato. Per impostazione predefinita, queste caselle di controllo sono deselezionate.

  - Applica ai dispositivi senza i tag specificati

    Abilitare questa opzione se è necessario invertire la selezione di tag.

    Se questa opzione è abilitata, il profilo criterio include i dispositivi con descrizioni che non contengono alcuno dei tag selezionati. Se questa opzione è disabilitata, il criterio non viene applicato.

    Per impostazione predefinita, questa opzione è disabilitata.

- Regole per l'utilizzo di Active Directory

  Selezionare questa casella di controllo per configurare le regole per l'attivazione del profilo criterio nel dispositivo in base alla presenza del dispositivo in un'unità organizzativa di Active Directory o all'appartenenza del dispositivo (o del proprietario) a un gruppo di protezione di Active Directory.

  Per questa opzione, specificare al passaggio successivo:

  - Appartenenza del proprietario del dispositivo a un gruppo di protezione di Active Directory

    Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo il cui proprietario appartiene al gruppo di protezione specificato. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

  - Appartenenza del dispositivo al gruppo di protezione di Active Directory

Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato. Per impostazione predefinita, questa opzione è disabilitata.

- **Allocazione del dispositivo nell'unità organizzativa di Active Directory**

  Se questa opzione è abilitata, il profilo criterio viene attivato nel dispositivo incluso nell'unità organizzativa di Active Directory specificata. Se questa opzione è disabilitata, il criterio di attivazione del profilo non viene applicato.

  Per impostazione predefinita, questa opzione è disabilitata.

Il numero delle pagine aggiuntive della procedura guidata dipende dalle impostazioni selezionate nel primo passaggio. È possibile modificare le regole di attivazione del profilo criterio in un secondo momento.

6. Controllare l'elenco dei parametri configurati. Se l'elenco è corretto, fare clic su **Crea**.

Il profilo verrà salvato. Il profilo sarà attivato nel dispositivo quando vengono attivate le regole di attivazione.

Le regole di attivazione del profilo criterio create per il profilo sono visualizzate nelle proprietà del profilo criterio nella scheda **Regole di attivazione**. È possibile modificare o rimuovere qualsiasi regola di attivazione del profilo criterio.

È possibile attivare contemporaneamente più regole di attivazione.

Eliminazione di un profilo criterio

Per eliminare un profilo criterio:

1. Passare all'elenco dei profili del criterio desiderato.

   Verrà visualizzato l'elenco dei profili criterio.

2. Nella scheda **Profili criterio** selezionare la casella di controllo accanto al profilo criterio da eliminare e fare clic su **Elimina**.

3. Nella finestra visualizzata fare di nuovo clic su **Elimina**.

Il profilo criterio viene eliminato. Se il criterio è ereditato da un gruppo di livello inferiore, il profilo rimane in tale gruppo, ma diventa il profilo criterio di tale gruppo. Questo avviene per eliminare un cambiamento significativo nelle impostazioni delle applicazioni gestite installate nei dispositivi dei gruppi di livello inferiore.

Criptaggio e protezione dei dati

Il criptaggio dei dati riduce il rischio di divulgazione accidentale in caso di furto o smarrimento di un laptop o un disco rigido oppure qualora venga eseguito l'accesso da parte di utenti e applicazioni non autorizzati.

Le seguenti applicazioni Kaspersky supportano il criptaggio:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

È possibile mostrare o nascondere alcuni degli elementi dell'interfaccia relativi alla funzionalità di gestione del criptaggio utilizzando le impostazioni dell'interfaccia utente.

Non è consigliabile abilitare il criptaggio in VDI.

Criptaggio dei dati in Kaspersky Endpoint Security for Windows

È possibile gestire i seguenti tipi di criptaggio:

- Crittografia unità BitLocker nei dispositivi che eseguono un sistema operativo Windows per i server
- Criptaggio disco Kaspersky nei dispositivi che eseguono un sistema operativo Windows per workstation

Utilizzando questi componenti di Kaspersky Endpoint Security for Windows è ad esempio possibile abilitare o disabilitare il criptaggio, visualizzare l'elenco delle unità criptate o generare e visualizzare rapporti sul criptaggio.

È possibile configurare il criptaggio definendo i criteri di Kaspersky Endpoint Security for Windows in Kaspersky Security Center. Kaspersky Endpoint Security for Windows esegue il criptaggio e il decriptaggio in base al criterio attivo. Per istruzioni dettagliate su come configurare le regole e una descrizione delle funzionalità di criptaggio, consultare la Guida di Kaspersky Endpoint Security for Windows.

Criptaggio dei dati in Kaspersky Endpoint Security for Mac

È possibile utilizzare il criptaggio FileVault nei dispositivi che eseguono macOS. Durante l'utilizzo di Kaspersky Endpoint Security for Mac è possibile abilitare o disabilitare questo criptaggio.

È possibile configurare il criptaggio definendo i criteri di Kaspersky Endpoint Security for Mac in Kaspersky Security Center. Kaspersky Endpoint Security for Mac esegue il criptaggio e il decriptaggio in base al criterio attivo. Per una descrizione dettagliata delle funzionalità di criptaggio, consultare la Guida di Kaspersky Endpoint Security for Mac.

Visualizzazione dell'elenco delle unità criptate

In Kaspersky Security Center, è possibile visualizzare i dettagli sulle unità criptate e sui dispositivi criptati a livello di unità. Una volta decriptate le informazioni in un'unità, l'unità viene automaticamente rimossa dall'elenco.

Per visualizzare l'elenco delle unità criptate:

Nel menu principale accedere a **Operazioni** → **Criptaggio e protezione dei dati** → **Unità criptate**.

Se la sezione non è visibile nel menu, significa che è nascosta. Nelle impostazioni dell'interfaccia utente. abilitare l'opzione **Mostra Criptaggio e protezione dei dati** per visualizzare la sezione.

È possibile esportare l'elenco delle unità criptate in un file CSV o TXT. A tale scopo, fare clic sul pulsante **Esporta in CSV** o **Esporta in TXT**.

Visualizzazione dell'elenco degli eventi di criptaggio

Durante l'esecuzione delle attività di criptaggio o decriptaggio dei dati nei dispositivi, Kaspersky Endpoint Security for Windows invia a Kaspersky Security Center informazioni sui seguenti tipi di eventi:

- Impossibile criptare o decriptare un file o creare un archivio criptato perché lo spazio sul disco rigido non è sufficiente.
- Impossibile criptare o decriptare un file o creare un archivio criptato a causa dei problemi di licenza.
- Impossibile criptare o decriptare un file o creare un archivio criptato a causa di diritti di accesso insufficienti.
- All'applicazione è stato negato l'accesso a un file criptato.
- Errori sconosciuti.

Per visualizzare un elenco degli eventi che si sono verificati durante il criptaggio dei dati nei dispositivi:

Nel menu principale accedere a **Operazioni** → **Criptaggio e protezione dei dati** → **Eventi di criptaggio**.

Se la sezione non è visibile nel menu, significa che è nascosta. Nelle impostazioni dell'interfaccia utente. abilitare l'opzione **Mostra Criptaggio e protezione dei dati** per visualizzare la sezione.

È possibile esportare l'elenco delle unità criptate in un file CSV o TXT. A tale scopo, fare clic sul pulsante **Esporta in CSV** o **Esporta in TXT**.

In alternativa è possibile esaminare l'elenco degli eventi di criptaggio per ogni dispositivo gestito.

Per visualizzare gli eventi di criptaggio di un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome di un dispositivo gestito.
3. Nella scheda **Generale**, passare alla sezione **Protezione**.
4. Fare clic sul collegamento **Visualizza errori di criptaggio dei dati**.

Creazione e visualizzazione di rapporti sul criptaggio

È possibile generare i seguenti rapporti:

- Rapporto sullo stato di criptaggio dei dispositivi gestiti. Questo rapporto include informazioni dettagliate sul criptaggio dei dati di vari dispositivi gestiti. Il rapporto mostra ad esempio il numero di dispositivi a cui si applica il criterio con regole di criptaggio configurate. È inoltre possibile scoprire, ad esempio, quanti dispositivi devono essere riavviati. Il rapporto contiene inoltre le informazioni sulla tecnologia di criptaggio e sull'algoritmo di ogni dispositivo.

- Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa. Questo rapporto contiene informazioni simili a quelle del rapporto sullo stato di criptaggio dei dispositivi gestiti, ma fornisce solo i dati relativi a dispositivi di archiviazione di massa e unità rimovibili.

- Rapporto sui diritti di accesso alle unità criptate. Questo rapporto mostra quali account utente hanno accesso alle unità criptate.

- Rapporto sugli errori di criptaggio dei file. Questo rapporto contiene informazioni sugli errori che si sono verificati durante l'esecuzione delle attività di criptaggio o decriptaggio dei dati nei dispositivi.

- Rapporto sul blocco dell'accesso ai file criptati. Questo rapporto contiene informazioni sul blocco dell'accesso delle applicazioni ai file criptati. Questo rapporto è utile se un utente o un'applicazione non autorizzati tentano di accedere a unità o file criptati.

È possibile generare qualsiasi rapporto nella sezione **Monitoraggio e generazione dei rapporti → Rapporti**. In alternativa, nella sezione **Operazioni → Criptaggio e protezione dei dati**, è possibile generare i seguenti rapporti di criptaggio:

- Rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa

- Rapporto sui diritti di accesso alle unità criptate

- Rapporto sugli errori di criptaggio dei file

*Per generare un rapporto sul criptaggio nella sezione **Criptaggio e protezione dei dati**:*

1. Assicurarsi di avere abilitato l'opzione **Mostra Criptaggio e protezione dei dati** in Opzioni di interfaccia.

2. Nelle proprietà del criterio aprire la scheda **Configurazione eventi**.

3. Nella sezione **Critico**, fare clic su **Aggiungi evento** e selezionare la casella di controllo accanto all'evento *Errore durante l'applicazione delle regole di criptaggio/decriptaggio dei file*.

4. Fare clic su **OK**.

5. Nel menu principale accedere a **Operazioni → Criptaggio e protezione dei dati**.

6. Aprire una delle seguenti sezioni:

   - **Unità criptate** genera il rapporto sullo stato di criptaggio dei dispositivi di archiviazione di massa o il rapporto sui diritti di accesso alle unità criptate.

   - **Eventi di criptaggio** genera il rapporto sugli errori di criptaggio dei file.

7. Fare clic sul nome del rapporto che si desidera generare.

Verrà avviata la generazione del rapporto.

Concedere l'accesso a un'unità criptata in modalità offline

Un utente può richiedere l'accesso a un dispositivo criptato, ad esempio quando Kaspersky Endpoint Security for Windows non è installato nel dispositivo gestito. Dopo aver ricevuto la richiesta, è possibile creare un file della chiave di accesso e inviarlo all'utente. Tutti i casi di utilizzo e le istruzioni dettagliate sono disponibili nella Guida di Kaspersky Endpoint Security for Windows.

Per concedere l'accesso a un'unità criptata in modalità offline:

1. Ottenere un file della richiesta di accesso da un utente (un file con estensione FDERTC). Seguire le istruzioni contenute nella Guida di Kaspersky Endpoint Security for Windows per generare il file in Kaspersky Endpoint Security for Windows.

2. Nel menu principale accedere a **Operazioni** → **Criptaggio e protezione dei dati** → **Unità criptate**.

   Verrà visualizzato un elenco di unità criptate.

3. Selezionare l'unità a cui l'utente ha richiesto l'accesso.

4. Fare clic sul pulsante **Concedi l'accesso al dispositivo in modalità offline**.

5. Nella finestra visualizzata selezionare il plug-in corrispondente all'applicazione Kaspersky utilizzata per criptare l'unità selezionata.

   Se un'unità è criptata con un'applicazione Kaspersky non supportata da Kaspersky Security Center Web Console, utilizzare Administration Console basata su Microsoft Management Console per concedere l'accesso offline.

6. Seguire le istruzioni fornite nella Guida di Kaspersky Endpoint Security for Windows (vedere le parti espandibili alla fine della sezione).

Successivamente l'utente applica il file ricevuto per accedere all'unità criptata e leggere i dati archiviati nell'unità.

Utenti e ruoli utente

Questa sezione descrive gli utenti e i ruoli utente e fornisce istruzioni per la creazione e la modifica di questi elementi, per l'assegnazione di ruoli e gruppi agli utenti e per l'associazione dei profili criterio ai ruoli.

Informazioni sui ruoli utente

Un *ruolo utente* (anche denominato *ruolo*) è un oggetto contenente un set di diritti e privilegi. Un ruolo può essere associato alle impostazioni delle applicazioni Kaspersky installate in un dispositivo utente. È possibile assegnare un ruolo a un set di utenti o a un set di gruppi di protezione a qualsiasi livello nella gerarchia dei gruppi di amministrazione, di Administration Server o a livello di oggetti specifici.

Se i dispositivi vengono gestiti tramite una gerarchia di Administration Server che include Administration Server virtuali, si noti che è possibile creare, modificare o eliminare i ruoli utente solo da un Administration Server fisico. È quindi possibile propagare i ruoli utente agli Administration Server secondari, inclusi quelli virtuali.

È possibile associare i ruoli utente ai profili criterio. Se a un utente viene assegnato un ruolo, tale utente ottiene le impostazioni di protezione necessarie per eseguire le funzioni lavorative.

Un ruolo utente può essere associato agli utenti dei dispositivi in un gruppo di amministrazione specifico.

Ambito del ruolo utente

Un *ambito di un ruolo utente* è una combinazione di utenti e gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Vantaggi dell'utilizzo dei ruoli

Un vantaggio dell'utilizzo dei ruoli è che non è necessario specificare le impostazioni di protezione per ciascuno dei dispositivi gestiti o per ciascuno degli utenti separatamente. Il numero di utenti e dispositivi in un'azienda può essere piuttosto elevato, ma il numero delle diverse funzioni lavorative che richiedono differenti impostazioni di protezione è notevolmente inferiore.

Differenze rispetto all'utilizzo dei profili criterio

I profili criterio sono le proprietà di un criterio creato per ciascuna applicazione Kaspersky separatamente. Un ruolo è associato a molti profili criterio creati per diverse applicazioni. Pertanto, un ruolo è un metodo per riunire le impostazioni per un determinato tipo di utente in un'unica posizione.

Visualizzazione degli account utente e delle sessioni

Kaspersky Security Center consente di gestire account utente e gruppi di account. L'applicazione supporta due tipi di account:

- Account dei dipendenti dell'organizzazione. Administration Server recupera i dati degli account degli utenti durante il polling della rete dell'organizzazione.
- Account degli utenti interni. Questi account vengono applicati quando si utilizzano Administration Server virtuali. Gli account degli utenti interni vengono creati e utilizzati solo in Kaspersky Security Center.

È possibile visualizzare l'elenco degli account utente e delle sessioni in uno dei seguenti modi:

- Nel menu principale accedere a **Utenti e ruoli** → **Utenti e gruppi**.
- Nel menu principale, passare a **Risorse (dispositivi)** → **Dispositivi gestiti** → collegamento <nome dispositivo> → scheda **Generale** → sezione **Generale** → blocco **Sessioni**.

  La sezione **Sessioni** mostra gli account utente con sessioni attive nei dispositivi in cui viene eseguito Windows.

L'elenco degli account utente e delle sessioni viene visualizzato correttamente se vengono soddisfatti i seguenti requisiti:

- Utilizzare Network Agent con la stessa versione di Administration Server o successiva.
- Il polling di Active Directory è abilitato per visualizzare gli account degli utenti del dominio.
- Nei dispositivi gestiti in cui viene eseguito Windows, il servizio **Server** (**LanmanServer**) è in esecuzione.

Configurazione dei diritti di accesso alle funzionalità dell'applicazione. Controllo dell'accesso basato sui ruoli

Kaspersky Security Center offre l'accesso in base al ruolo alle funzionalità di Kaspersky Security Center e delle applicazioni Kaspersky gestite.

È possibile configurare i diritti di accesso alle funzionalità dell'applicazione per gli utenti di Kaspersky Security Center in uno dei seguenti modi:

- Attraverso la configurazione dei diritti per ciascun utente o gruppo di utenti singolarmente.
- Attraverso la creazione di ruoli utente standard con un set di diritti predefinito e l'assegnazione di tali ruoli agli utenti sulla base dell'ambito delle relative mansioni lavorative.

L'applicazione dei ruoli utente ha lo scopo di semplificare e abbreviare le procedure di routine per la configurazione dei diritti di accesso degli utenti alle funzionalità dell'applicazione. I diritti di accesso all'interno di un ruolo vengono configurati in base alle attività standard e all'ambito delle mansioni lavorative degli utenti.

Ai ruoli utente possono essere assegnati nomi corrispondenti ai rispettivi scopi. È possibile creare un numero illimitato di ruoli nell'applicazione.

È possibile utilizzare i ruoli utente predefiniti con un set di diritti già configurato oppure creare nuovi ruoli e configurare autonomamente i diritti richiesti.

Diritti di accesso alle funzionalità dell'applicazione

La tabella seguente mostra le funzionalità di Kaspersky Security Center con i diritti di accesso per gestire le attività, i rapporti e le impostazioni associati e per eseguire le azioni utente associate.

Per eseguire le azioni utente elencate nella tabella, un utente deve disporre del diritto specificato accanto all'azione.

I diritti **Read**, **Scrittura** ed **Esecuzione** sono applicabili a qualsiasi attività, rapporto o impostazione. Oltre a questi diritti, un utente deve disporre del diritto **Esegui operazioni per le selezioni dispositivi** per gestire attività, rapporti o impostazioni relativi alle selezioni dispositivi.

Tutte le attività, i rapporti, le impostazioni e i pacchetti di installazione mancanti nella tabella appartengono all'area funzionale **Caratteristiche generali: Funzionalità di base**.

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: **Gestione dei gruppi di amministrazione**	**Scrittura**	• Aggiungere un dispositivo a un gruppo di amministrazione: **Scrittura** • Eliminare un dispositivo da un gruppo di amministrazione: **Scrittura** • Aggiungere un gruppo di amministrazione a un altro gruppo di amministrazione: **Scrittura** • Eliminare un gruppo di amministrazione da un altro gruppo di amministrazione: **Scrittura**	None	None	None
Caratteristiche generali: **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi**	**Lettura**	Ottenere l'accesso in Lettura a tutti gli oggetti: **Lettura**	None	None	L'area funzionale **Caratteristiche generali: Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** è destinata a scopi di controllo. Quando gli utenti ottengono i diritti di **Lettura** in quest'area funzionale, ottengono l'accesso completo in **Lettura** a tutti gli oggetti e sono in grado di eseguire qualsiasi attività creata su selezioni di dispositivi connessi ad Administration Server tramite Network Agent con diritti di amministratore locale (root per Linux). Si consiglia di concedere con attenzione questi diritti a un gruppo limitato di utenti che ne hanno bisogno per svolgere le proprie funzioni ufficiali. L'accesso viene concesso indipendentemente da altri diritti, anche se vietano l'accesso in Lettura a oggetti specifici.

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: **Funzionalità di base**	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Regole di spostamento dei dispositivi (creazione, modifica o eliminazione) per il server virtuale: **Scrittura**, **Esegui operazioni per le selezioni dispositivi** • Ottenere un certificato personalizzato per il protocollo Mobile (LWNGT): **Lettura** • Impostare un certificato personalizzato per il protocollo Mobile (LWNGT): **Scrittura** • Ottenere l'elenco di reti definito da NLA: **Lettura** • Aggiungere, modificare o eliminare l'elenco di reti definito da NLA: **Scrittura** • Visualizzare gli elenchi di controllo di accesso dei gruppi: **Lettura** • Visualizzare il registro eventi Kaspersky: **Lettura** • Visualizzare la chiave di ripristino per ripristinare l'accesso a un disco rigido con Crittografia unità BitLocker: **Esecuzione**	• "Scarica aggiornamenti nell'archivio di Administration Server" • "Invia rapporti" • "Distribuisci pacchetto di installazione" • "Installa l'applicazione negli Administration Server secondari in remoto"	• "Rapporto sullo stato della protezione" • "Rapporto sulle minacce" • "Rapporto sui dispositivi più infetti" • "Rapporto sullo stato dei database anti-virus" • "Rapporto sugli errori" • "Rapporto sugli attacchi di rete" • "Rapporto di riepilogo sulle applicazioni di protezione per il sistema di posta installate" • "Rapporto di riepilogo sulle applicazioni di difesa perimetrale installate" • "Rapporto di riepilogo sui tipi di applicazioni installate" • "Rapporto sugli utenti dei dispositivi infetti" • "Rapporto sugli incidenti" • "Rapporto sugli eventi" • "Rapporto sull'attività dei punti di distribuzione" • "Rapporto sugli Administration Server secondari" • "Rapporto sugli eventi di Controllo Dispositivi" • "Rapporto sulle vulnerabilità" • "Rapporto sulle applicazioni proibite" • "Rapporto su Controllo Web" • "Rapporto sullo stato di criptaggio dei dispositivi gestiti" • "Rapporto sullo stato di criptaggio dei dispositivi di	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
				archiviazione di massa" • "Rapporto sugli errori di criptaggio dei file" • "Rapporto sul blocco dell'accesso ai file criptati" • "Rapporto sui diritti di accesso ai dispositivi criptati" • "Rapporto sulle autorizzazioni utente effettive" • "Rapporto sui diritti"	
Caratteristiche generali: **Oggetti eliminati**	• **Lettura** • **Scrittura**	• Visualizzare gli oggetti eliminati nel Cestino: **Lettura** • Eliminare gli oggetti dal Cestino: **Scrittura**	None	None	None
Caratteristiche generali: **Elaborazione degli eventi**	• **Elimina eventi** • **Modifica impostazioni di notifica eventi** • **Modifica impostazioni registro eventi** • **Scrittura**	• Modificare le impostazioni di registrazione degli eventi: **Modifica impostazioni registro eventi** • Modificare le impostazioni di notifica degli eventi: **Modifica impostazioni di notifica eventi** • Eliminare gli eventi: **Elimina eventi**	None	None	Impostazioni: • Impostazioni Epidemia di virus: numero di rilevamenti di virus necessari per creare un evento Epidemia di virus • Impostazioni Epidemia di virus: periodo di tempo per la valutazione dei rilevamenti di virus • Numero massimo di eventi archiviati nel database • Periodo di tempo per l'archiviazione degli eventi dai dispositivi eliminati

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: Operazioni in Administration Server	• **Lettura** • **Scrittura** • **Esecuzione** • **Modifica elenchi di controllo degli accessi agli oggetti** • **Esegui operazioni per le selezioni dispositivi**	• Specificare le porte dell'Administration Server per la connessione di Network Agent: **Scrittura** • Specificare le porte del proxy di attivazione avviato sull'Administration Server: **Scrittura** • Specificare le porte del proxy di attivazione per i dispositivi mobili avviato sull'Administration Server: **Scrittura** • Specificare le porte del server Web per la distribuzione di pacchetti indipendenti: **Scrittura** • Specificare le porte del server Web per la distribuzione dei profili MDM: **Scrittura** • Specificare le porte SSL di Administration Server per la connessione tramite Kaspersky Security Center Web Console: **Scrittura** • Specificare le porte dell'Administration Server per la connessione mobile: **Scrittura** • Specificare il numero massimo di eventi archiviati nel database dell'Administration Server: **Scrittura** • Specificare il numero massimo di eventi che possono essere inviati dall'Administration Server: **Scrittura** • Specificare il periodo di tempo durante il quale gli eventi possono essere inviati dall'Administration Server: **Scrittura**	• "Backup dei dati di Administration Server" • "Manutenzione database"	None	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: **Distribuzione applicazione Kaspersky**	• **Gestisci patch di Kaspersky** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	Accettare o rifiutare l'installazione della patch: **Gestisci patch di Kaspersky**	None	• "Rapporto sull'utilizzo delle chiavi di licenza da parte dell'Administration Server virtuale" • "Rapporto sulle versioni del software Kaspersky" • "Rapporto sulle applicazioni incompatibili" • "Rapporto sulle versioni degli aggiornamenti dei moduli software Kaspersky" • "Rapporto sulla distribuzione della protezione"	Pacchetto di installazione: "Kaspersky"
Caratteristiche generali: **Gestione delle chiavi di licenza**	• **Esporta file chiave** • **Scrittura**	• Esportare il file chiave: **Esporta file chiave** • Modificare le impostazioni della chiave di licenza di Administration Server: **Scrittura**	None	None	None
Caratteristiche generali: **Gestione dei rapporti forzata**	• **Lettura** • **Scrittura**	• Creare rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Scrittura** • Eseguire rapporti indipendentemente dagli elenchi di controllo degli accessi degli oggetti: **Lettura**	None	None	None
Caratteristiche generali: **Gerarchia di Administration Server**	**Configura gerarchia di Administration Server**	Registrare, aggiornare o eliminare gli Administration Server secondari: **Configura gerarchia di Administration Server**	None	None	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Caratteristiche generali: Autorizzazioni utente	**Modifica elenchi di controllo degli accessi agli oggetti**	• Modificare le proprietà Protezione di qualsiasi oggetto: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire i ruoli utente: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire gli utenti interni: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire i gruppi di protezione: **Modifica elenchi di controllo degli accessi agli oggetti** • Gestire gli alias: **Modifica elenchi di controllo degli accessi agli oggetti**	None	None	None
Caratteristiche generali: Administration Server virtuali	• **Gestisci Administration Server virtuali** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Ottenere l'elenco degli Administration Server virtuali: **Lettura** • Ottenere informazioni sull'Administration Server virtuale: **Lettura** • Creare, aggiornare o eliminare un Administration Server virtuale: **Gestisci Administration Server virtuali** • Spostare un Administration Server virtuale in un altro gruppo: **Gestisci Administration Server virtuali** • Impostare le autorizzazioni dei server virtuali: **Gestisci Administration Server virtuali**	None	"Rapporto sui risultati dell'installazione degli aggiornamenti software di terze parti"	None
Caratteristiche generali: Gestione delle chiavi di criptaggio	**Scrittura**	Importare le chiavi di criptaggio: **Scrittura**	None	None	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Mobile Device Management: Generale	• **Connetti nuovi dispositivi** • **Invia solo comandi informativi ai dispositivi mobili** • **Invia comandi ai dispositivi mobili** • **Gestisci certificati** • **Lettura** • **Scrittura**	• Ottenere dati di ripristino del servizio di gestione delle chiavi: **Lettura** • Eliminare i certificati utente: **Gestisci certificati** • Ottenere la parte pubblica del certificato utente: **Lettura** • Controllare se l'infrastruttura a chiave pubblica (PKI) è abilitata: **Lettura** • Controllare l'account dell'infrastruttura a chiave pubblica (PKI): **Lettura** • Ottenere i modelli dell'infrastruttura a chiave pubblica (PKI): **Lettura** • Ottenere i modelli dell'infrastruttura a chiave pubblica (PKI) tramite il certificato EKU (Extended Key Usage): **Lettura** • Controllare se il certificato dell'infrastruttura a chiave pubblica (PKI) è stato revocato: **Lettura** • Aggiornare le impostazioni di emissione del certificato utente: **Gestisci certificati** • Ottenere le impostazioni di emissione del certificato utente: **Lettura** • Ottenere i pacchetti per nome applicazione e versione: **Lettura** • Impostare o annullare il certificato utente: **Gestisci certificati** • Rinnovare il certificato utente: **Gestisci certificati** • Impostare il tag del certificato utente: **Gestisci certificati** • Eseguire la generazione del pacchetto di installazione MDM; annullare la generazione del	None	None	None

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
		pacchetto di installazione MDM: **Connetti nuovi dispositivi**			
Gestione sistema: Connettività	• **Avvia sessioni RDP** • **Connetti a sessioni RDP esistenti** • **Avvia tunneling** • **Salva i file dei dispositivi nella workstation dell'amministratore** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Creare una sessione di condivisione desktop: **Avvia sessioni RDP** • Creare una sessione RDP: **Connetti a sessioni RDP esistenti** • Creare un tunnel: **Avvia tunneling** • Salvare l'elenco della rete di contenuti: **Salva i file dei dispositivi nella workstation dell'amministratore**	None	"Rapporto sugli utenti dei dispositivi"	None
Gestione sistema: Inventario hardware	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Ottenere o esportare un oggetto dell'inventario hardware: **Lettura** • Aggiungere, impostare o eliminare un oggetto dell'inventario hardware: **Scrittura**	None	• "Rapporto sul registro hardware" • "Rapporto sulle modifiche della configurazione" • "Rapporto sull'hardware"	None
Gestione sistema: Controllo accesso alla rete (NAC)	• **Lettura** • **Scrittura**	• Visualizzare le impostazioni CISCO: **Lettura** • Modificare le impostazioni CISCO: **Scrittura**	None	None	None
Gestione sistema: Distribuzione del sistema operativo	• **Distribuisci server PXE** • **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Distribuire server PXE: **Distribuisci server PXE** • Visualizzare un elenco di server PXE: **Lettura** • Avviare o interrompere il processo di installazione nei client PXE: **Esecuzione** • Gestire i driver per WinPE e le immagini del sistema operativo: **Scrittura**	"Crea pacchetto installazione in base a immagine sistema operativo dispositivo di riferimento"	None	Pacchetto di installazione: "OS Image"

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Gestione sistema: Vulnerability e patch management	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Visualizzare le proprietà delle patch di terzi: **Lettura** • Modificare le proprietà delle patch di terzi: **Scrittura**	• "Esegui sincronizzazione di Windows Update" • "Installa aggiornamenti di Windows Update" • "Correggi vulnerabilità" • "Installa aggiornamenti richiesti e correggi vulnerabilità"	"Rapporto sugli aggiornamenti software"	None
Gestione sistema: Installazione remota	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	• Visualizzazione delle proprietà del pacchetto di installazione basato su Vulnerability e patch management di terzi: **Lettura** • Modifica delle proprietà del pacchetto di installazione basato su Vulnerability e patch management di terzi: **Scrittura**	None	None	Pacchetti di installazione: • "Applicazione personalizzata" • "Pacchetto VAPM"

Area funzionale	Diritto	Azione utente: diritto richiesto per eseguire l'azione	Attività	Rapporto	Altro
Gestione sistema: Inventario software	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	None	None	• "Rapporto sulle applicazioni installate" • "Rapporto sulla cronologia del registro applicazioni" • "Rapporto sullo stato dei gruppi di applicazioni concesse in licenza" • "Rapporto sulle chiavi di licenza del software di terze parti"	None
Gestione sistema: Esegui script da remoto	• **Lettura** • **Scrittura** • **Esecuzione** • **Esegui operazioni per le selezioni dispositivi**	L'utente può visualizzare le proprietà dell'attività: **Lettura** L'utente può creare, eliminare o modificare un pacchetto di installazione: **Scrittura** L'utente può eseguire un'attività: **Scrittura**. Nei dispositivi Linux client, gli script vengono eseguiti con i privilegi di root. L'utente può eseguire un'attività o pianificarne l'esecuzione: **Esecuzione** L'utente può eseguire un'attività su una selezione di dispositivi: **Esegui operazioni per le selezioni dispositivi**	"Esegui script da remoto"	None	None

Ruoli utente predefiniti

I ruoli utente assegnati agli utenti di Kaspersky Security Center forniscono set di diritti di accesso alle funzionalità dell'applicazione.

Agli utenti creati in un server virtuale non può essere assegnato un ruolo in Administration Server.

È possibile utilizzare i ruoli utente predefiniti con un set di diritti già configurato oppure creare nuovi ruoli. Quando si crea un nuovo ruolo, è necessario impostare l'ambito del ruolo e assegnare autonomamente i diritti di accesso alle funzionalità di Kaspersky Security Center. Alcuni dei ruoli utente predefiniti disponibili in Kaspersky Security Center possono essere associati a posizioni lavorative specifiche, ad esempio **Auditor**, **Security Officer** e **Supervisore** (questi ruoli sono presenti in Kaspersky Security Center a partire dalla versione 11). I diritti di accesso di questi ruoli sono preconfigurati in base alle attività standard e all'ambito delle mansioni lavorative delle posizioni associate. La tabella seguente illustra il modo in cui è possibile associare i ruoli a posizioni specifiche.

Esempi di ruoli per posizioni specifiche

Ruolo	Commento
Auditor	Consente tutte le operazioni di visualizzazione e l'esecuzione di qualsiasi attività creata su selezioni di dispositivi connessi all'Administration Server tramite Network Agent con diritti di amministratore locale (radice per Linux). Si consiglia di assegnare questo ruolo a un gruppo con attenzione limitato di utenti che ne hanno bisogno per svolgere le proprie funzioni ufficiali.
Supervisore	Consente tutte le operazioni di visualizzazione; non consente le altre operazioni. È possibile assegnare questo ruolo a un security officer e ad altri manager responsabili della sicurezza IT dell'organizzazione.
Security Officer	Consente tutte le operazioni di visualizzazione e la gestione dei rapporti; concede autorizzazioni limitate per l'area **Gestione sistema**: **Connettività**. È possibile assegnare questo ruolo a un addetto responsabile della sicurezza IT dell'organizzazione.

La tabella seguente illustra i diritti di accesso assegnati a ciascun ruolo utente predefinito.

Diritti di accesso dei ruoli utente predefiniti

Ruolo	Descrizione

Amministratore Administration Server	Consente tutte le operazioni nelle seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Elaborazione degli eventi**
	  • **Gerarchia di Administration Server**
	  • **Administration Server virtuali**
	• **Gestione sistema**:
	  • **Connettività**
	  • **Inventario hardware**
	  • **Inventario software**
	
	Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.

Operatore Administration Server	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Administration Server virtuali**
	• **Gestione sistema**:
	  • **Connettività**
	  • **Inventario hardware**
	  • **Inventario software**

Auditor	Consente tutte le operazioni nelle aree funzionali, in **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Oggetti eliminati** • **Gestione dei rapporti forzata** È possibile assegnare questo ruolo a una persona che esegue il controllo dell'organizzazione.

Ruolo	Descrizione

Amministratore installazione	Consente tutte le operazioni nelle seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Distribuzione del software Kaspersky**
	  • **Gestione delle chiavi di licenza**
	• **Gestione sistema**:
	  • **Distribuzione del sistema operativo**
	  • **Vulnerability e patch management**
	  • **Installazione remota**
	  • **Inventario software**
	Concede i diritti **Lettura** ed **Esecuzione** nell'area funzionale **Caratteristiche generali: Administration Server virtuali**.

Operatore installazione	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Distribuzione del software Kaspersky** (concede anche il diritto **Gestisci patch di Kaspersky** in quest'area)
	  • **Administration Server virtuali**
	• **Gestione sistema**:
	  • **Distribuzione del sistema operativo**
	  • **Vulnerability e patch management**
	  • **Installazione remota**
	  • **Inventario software**

Amministratore Kaspersky Endpoint Security	Consente tutte le operazioni nelle seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • Area Kaspersky Endpoint Security, incluse tutte le funzionalità Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.
Operatore Kaspersky Endpoint Security	Concede i diritti **Lettura** ed **Esecuzione** in tutte le seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • Area Kaspersky Endpoint Security, incluse tutte le funzionalità
Amministratore principale	Consente tutte le operazioni nelle aree funzionali, *ad eccezione* delle seguenti aree, **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Gestione dei rapporti forzata** Concede i diritti di **Lettura** e **Scrittura** nell'area funzionale **Caratteristiche generali: Gestione delle chiavi di criptaggio**.

Ruolo	Descrizione

Operatore principale	Concede i diritti **Lettura** ed **Esecuzione** (ove applicabile) in tutte le seguenti aree funzionali:
	• **Caratteristiche generali**:
	  • **Funzionalità di base**
	  • **Oggetti eliminati**
	  • **Operazioni in Administration Server**
	  • **Distribuzione applicazione Kaspersky**
	  • **Administration Server virtuali**
	• **Mobile Device Management: Generale**
	• **Gestione sistema**, incluse tutte le funzionalità
	• Area Kaspersky Endpoint Security, incluse tutte le funzionalità

Amministratore Mobile Device Management	Consente tutte le operazioni nelle seguenti aree funzionali: • **Caratteristiche generali: Funzionalità di base** • **Mobile Device Management: Generale**
Operatore Mobile Device Management	Concede i diritti **Lettura** ed **Esecuzione** nell'area funzionale **Caratteristiche generali**: **Funzionalità di base**. Concede i diritti **Lettura** e **Invia solo comandi informativi ai dispositivi mobili** nell'area funzionale **Mobile Device Management**: **Generale**.
Security Officer	Consente tutte le operazioni nelle seguenti aree funzionali, in **Caratteristiche generali**: • **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** • **Gestione dei rapporti forzata** Concede i diritti **Lettura**, **Scrittura**, **Esecuzione**, **Salva i file dei dispositivi nella workstation dell'amministratore** ed **Esegui operazioni per le selezioni di dispositivi** nell'area funzionale **Gestione sistema: Connettività**. È possibile assegnare questo ruolo a un addetto responsabile della sicurezza IT dell'organizzazione.
Utente del Portale Self Service	Consente tutte le operazioni nell'area funzionale **Mobile Device Management: Portale Self Service**. Questa funzionalità non è supportata in Kaspersky Security Center 11 e versioni successive.
Supervisore	Concede il diritto **Lettura** nelle aree funzionali **Caratteristiche generali**: **Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi** e **Caratteristiche generali**: **Gestione dei rapporti forzata**. È possibile assegnare questo ruolo a un security officer e ad altri manager responsabili della sicurezza IT dell'organizzazione.
Amministratore di Vulnerability e patch management	Consente tutte le operazioni nelle aree funzionali **Caratteristiche generali**: **Funzionalità di base** e **Gestione sistema** (incluse tutte le funzionalità).
Operatore di Vulnerability e patch management	Concede i diritti **Lettura** ed **Esecuzione** (ove applicabile) nelle aree funzionali **Caratteristiche generali**: **Funzionalità di base** e **Gestione sistema** (incluse tutte le funzionalità).

Assegnazione dei diritti di accesso a oggetti specifici

Oltre ad assegnare diritti di accesso a livello di server, è possibile configurare l'accesso a oggetti specifici, ad esempio a un'attività specifica. L'applicazione consente di specificare i diritti di accesso per i seguenti tipi di oggetti:

- Gruppi di amministrazione
- Attività
- Rapporti

- Selezioni dispositivi
- Selezioni eventi

Per assegnare i diritti di accesso a un oggetto specifico:

1. In base al tipo di oggetto, nel menu principale passare alla sezione corrispondente:
   - **Risorse (dispositivi) → Gerarchia dei gruppi**
   - **Risorse (dispositivi) → Attività**
   - **Monitoraggio e generazione dei rapporti → Rapporti**
   - **Risorse (dispositivi) → Selezioni dispositivi**
   - **Monitoraggio e generazione dei rapporti → Selezioni eventi**
2. Aprire le proprietà dell'oggetto per il quale si desidera configurare i diritti di accesso.

   Per aprire la finestra delle proprietà di un gruppo di amministrazione o di un'attività, fare clic sul nome dell'oggetto. È possibile aprire le proprietà di altri oggetti utilizzando il pulsante sulla barra degli strumenti.
3. Nella finestra delle proprietà, aprire la sezione **Diritti di accesso**.

   Verrà visualizzato l'elenco di utenti. Gli utenti e i gruppi di protezione elencati dispongono dei diritti di accesso all'oggetto. Per impostazione predefinita, se si utilizza una gerarchia di gruppi di amministrazione o server, l'elenco e i diritti di accesso vengono ereditati dal gruppo di amministrazione principale o dal server primario.
4. Per poter modificare l'elenco, abilitare l'opzione **Usa autorizzazioni personalizzate**.
5. Configurare i diritti di accesso:
   - Utilizzare i pulsanti **Aggiungi** ed **Elimina** per modificare l'elenco.
   - Specificare i diritti di accesso per un utente o un gruppo di protezione. Eseguire una delle seguenti operazioni:
     - Se si desidera specificare i diritti di accesso manualmente, selezionare l'utente o il gruppo di protezione, fare clic sul pulsante **Diritti di accesso**, quindi specificare i diritti di accesso.
     - Se si desidera assegnare un ruolo utente all'utente o al gruppo di protezione, selezionare l'utente o il gruppo di protezione, fare clic sul pulsante **Ruoli** e selezionare il ruolo da assegnare.
6. Fare clic sul pulsante **Salva**.

I diritti di accesso all'oggetto sono configurati.

Assegnazione dei diritti di accesso a utenti e gruppi di protezione

È possibile concedere a utenti e gruppi di protezione i diritti di accesso per utilizzare diverse funzionalità di Administration Server, ad esempio, Kaspersky Endpoint Security for Linux.

Per assegnare i diritti di accesso a un utente o un gruppo di protezione:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Diritti di accesso**, selezionare la casella di controllo accanto al nome dell'utente o del gruppo di protezione a cui assegnare i diritti, quindi fare clic sul pulsante **Diritti di accesso**.

   Non è possibile selezionare più utenti o gruppi di sicurezza contemporaneamente. Se si selezionano più elementi, il pulsante **Diritti di accesso** verrà disabilitato.

3. Configurare il set di diritti per l'utente o il gruppo:

   a. Espandere il nodo con le funzionalità di Administration Server o di un'altra applicazione Kaspersky.

   b. Selezionare la casella di controllo **Consenti** o **Nega** accanto alla funzionalità o al diritto di accesso desiderato.

      Esempio 1: selezionare la casella di controllo **Consenti** accanto al nodo **Integrazione applicazione** per concedere tutti i diritti di accesso disponibili alla funzionalità di integrazione dell'applicazione (**Lettura**, **Scrittura** ed **Esecuzione**) per un utente o un gruppo.

      Esempio 2: espandere il nodo **Gestione chiavi di criptaggio**, quindi selezionare la casella di controllo **Consenti** accanto all'autorizzazione **Scrittura** per concedere il diritto di accesso in **scrittura** alla funzionalità di gestione delle chiavi di criptaggio per un utente o un gruppo.

4. Dopo aver configurato il set di diritti di accesso, fare clic su **OK**.

Verrà configurato il set di diritti per l'utente o il gruppo di utenti.

Le autorizzazioni dell'Administration Server (o del gruppo di amministrazione) sono suddivise nelle seguenti aree:

- Caratteristiche generali:
  - Gestione dei gruppi di amministrazione
  - Accesso agli oggetti indipendentemente dagli elenchi di controllo degli accessi
  - Funzionalità di base
  - Oggetti eliminati
  - Gestione delle chiavi di criptaggio
  - Elaborazione degli eventi
  - Operazioni in Administration Server (solo nella finestra delle proprietà di Administration Server)
  - Tag dispositivo
  - Distribuzione applicazione Kaspersky
  - Gestione delle chiavi di licenza
  - Integrazione dell'applicazione
  - Gestione dei rapporti forzata
  - Gerarchia di Administration Server
  - Autorizzazioni utente
  - Administration Server virtuali
- Mobile Device Management:
  - Generale
  - Portale Self Service
- Gestione sistema:
  - Connettività
  - Esegui script da remoto
  - Inventario hardware
  - Controllo accesso alla rete (NAC)
  - Distribuzione del sistema operativo
  - Vulnerability e patch management
  - Installazione remota

- Inventario software

Se non si seleziona **Consenti** o **Nega** per un diritto di accesso, il diritto di accesso viene considerato *non definita*: è negata finché non viene negata o consentita in modo esplicito per l'utente.

I diritti di un utente sono la somma di quanto segue:

- I diritti propri dell'utente
- I diritti di tutti i ruoli assegnati all'utente
- I diritti di tutto il gruppo di protezione a cui appartiene l'utente
- I diritti di tutti i ruoli assegnati ai gruppi di protezione a cui appartiene l'utente

Se almeno uno di questi set di diritti ha l'autorizzazione **Nega**, l'autorizzazione viene negata all'utente, anche se altri set la consentono o la lasciano non definita.

È inoltre possibile aggiungere utenti e gruppi di protezione all'ambito di un ruolo utente per usare funzionalità diverse di Administration Server. Le impostazioni associate a un ruolo utente si applicheranno solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Aggiunta di un account di un utente interno

Se si desidera aggiungere un account utente, verificare che nell'account sia presenti il diritto Modifica ACL oggetti nell'area Funzionalità generali: Autorizzazioni utente.

Per aggiungere un nuovo account utente interno di Kaspersky Security Center:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la sceda **Utenti**.
2. Fare clic su **Aggiungi**.

3. Nella finestra **Aggiungi utente** visualizzata specificare le impostazioni del nuovo account utente:

   - **Nome**
   - **Password**

     La password deve rispettare le seguenti regole:

     - La password deve avere una lunghezza compresa tra 8 e 256 caratteri.
     - La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
       - Lettere maiuscole (A-Z)
       - Lettere minuscole (a-z)
       - Numeri (0-9)
       - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La password non deve contenere spazi, caratteri Unicode o la combinazione di "." e "@", quando "." si trova prima di "@".

     Per visualizzare la password immessa, fare clic su .

     È possibile abilitare l'opzione **L'utente deve modificare la password al primo accesso** per forzare la modifica della password al momento dell'autenticazione del primo utente.

4. Salvare le modifiche per completare la creazione del nuovo account utente.

Un nuovo account di utenti viene aggiunto all'elenco di utenti.

Creazione di un gruppo di protezione

Per creare un gruppo di protezione:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Gruppi**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Crea gruppo di protezione** visualizzata, specificare le seguenti impostazioni per il nuovo gruppo di protezione:

   - **Nome gruppo**
   - **Descrizione**

4. Fare clic su **Salva** per salvare le modifiche.

Un nuovo gruppo di protezione viene aggiunto all'elenco dei gruppi.

Modifica di un account di un utente interno

Se si desidera modificare un account utente, verificare che nell'account sia presenti il diritto Modifica ACL oggetti nell'area Funzionalità generali: Autorizzazioni utente.

Per modificare un account di un utente interno in Kaspersky Security Center:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account utente che si desidera modificare.

3. Nella finestra delle impostazioni utente visualizzata, nella scheda **Generale**, modificare le impostazioni dell'account utente:

   - Stato dell'utente

     Se necessario, spostare l'interruttore su **Disabilitato** per impedire all'utente di connettersi all'applicazione. È ad esempio possibile disabilitare un account dopo che un dipendente lascia l'azienda.

   - **Nome**
   - **Nome completo**
   - **Descrizione**
   - **Indirizzo e-mail**
   - **Telefono principale**
   - Password

     Se necessario, è possibile impostare una nuova password per la connessione dell'utente a Kaspersky Security Center come segue:

     a. Fare clic sul pulsante **Cambia password**, quindi impostare una nuova password per l'account utente.

     La password deve rispettare le seguenti regole:

     - La password deve avere una lunghezza compresa tra 8 e 256 caratteri.
     - La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
       - Lettere maiuscole (A-Z)
       - Lettere minuscole (a-z)
       - Numeri (0-9)
       - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
     - La password non deve contenere spazi, caratteri Unicode o la combinazione di "." e "@", quando "." si trova prima di "@".

     Per visualizzare la password immessa, fare clic su .

     b. Se necessario, abilitare l'opzione **L'utente deve modificare la password al primo accesso** per forzare la modifica della password al momento dell'autenticazione dell'utente successivo.

     c. Se l'account utente è protetto dalle modifiche non autorizzate, è necessario confermare di disporre delle autorizzazioni per modificare l'account. Nella finestra **Protezione account**, specificare le credenziali dell'account con il diritto Modifica ACL oggetti nell'area Funzionalità generali: Autorizzazioni utente.

4. Nella scheda **Sicurezza in fase di autenticazione** è possibile specificare le impostazioni di protezione per questo account.

5. Nella scheda **Gruppi** è possibile aggiungere l'utente ai gruppi di protezione.
6. Nella scheda **Dispositivi** è possibile assegnare dispositivi all'utente.
7. Nella scheda **Ruoli** è possibile assegnare ruoli all'utente.
8. Salvare le modifiche per completare la modifica dell'account utente.

L'account utente aggiornato verrà visualizzato nell'elenco di utenti.

Modifica di un gruppo di protezione

Per modificare un gruppo di protezione:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Gruppi**.
2. Fare clic sul nome del gruppo di protezione che si desidera modificare.
3. Nella finestra delle impostazioni del gruppo visualizzata modificare le impostazioni del gruppo di protezione:
   - Nella scheda **Generale**, è possibile modificare le impostazioni **Nome** e **Descrizione**. Queste impostazioni sono disponibili solo per i gruppi di protezione interni.
   - Nella scheda **Utenti**, è possibile aggiungere utenti al gruppo di protezione. Questa impostazione è disponibile solo per utenti interni e gruppi di protezione interni.
   - Nella scheda **Ruoli**, è possibile assegnare un ruolo al gruppo di protezione.
4. Fare clic su **Salva** per salvare le modifiche.

Le modifiche vengono applicate al gruppo di protezione.

Assegnazione di un ruolo a un utente o un gruppo di protezione

Per assegnare un ruolo a un utente o un gruppo di protezione:

1. Nel menu principale, passare su **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti** o **Gruppi**.
2. Selezionare il nome dell'utente o del gruppo di protezione a cui assegnare un ruolo.

   È possibile selezionare più nomi.
3. Nella riga del menu fare clic sul pulsante **Assegna ruolo**.

   Verrà avviata l'Assegnazione guidata ruolo.
4. Seguire le istruzioni della procedura guidata: selezionare il ruolo che si desidera assegnare agli utenti o gruppi di protezione selezionati, quindi selezionare l'ambito del ruolo.

   Un ambito di un ruolo utente è una combinazione di utenti e gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Il ruolo con un set di diritti per l'utilizzo di Administration Server viene assegnato all'utente (o agli utenti o al gruppo di protezione). Nell'elenco degli utenti o dei gruppi di sicurezza, viene visualizzata una casella di controllo nella colonna **Ha ruoli assegnati**.

Agli utenti creati in un server virtuale non può essere assegnato un ruolo in Administration Server.

Aggiunta di account utente a un gruppo di protezione interno

È possibile aggiungere solo account di utenti interni a un gruppo di protezione interno.

Per aggiungere account utente a un gruppo di protezione interno:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Selezionare le caselle di controllo accanto agli account utente che si desidera aggiungere a un gruppo di protezione.
3. Fare clic sul pulsante **Assegna gruppo**.
4. Nella finestra **Assegna gruppo** visualizzata selezionare il gruppo di protezione a cui si desidera aggiungere gli account utente.
5. Fare clic sul pulsante **Salva**.

Gli account utente verranno aggiunti al gruppo di protezione. È inoltre possibile aggiungere utenti interni a un gruppo di protezione utilizzando le impostazioni del gruppo.

Assegnazione di un utente come proprietario dispositivo

Per informazioni sull'assegnazione di un utente come proprietario di un dispositivo mobile, vedere la Guida di Kaspersky Security for Mobile.

Per assegnare un utente come proprietario dispositivo:

1. Se si desidera assegnare un proprietario di un dispositivo connesso a un Administration Server virtuale, passare prima all'Administration Server virtuale:
   a. Nel menu principale, fare clic sull'icona a forma di freccia di espansione (▶) a destra del nome corrente dell'Administration Server.
   b. Selezionare l'Administration Server desiderato.
2. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.

   Verrà visualizzato un elenco di utenti. Se si è attualmente connessi a un Administration Server virtuale, l'elenco include gli utenti dell'Administration Server virtuale corrente e dell'Administration Server primario.
3. Fare clic sul nome dell'account utente che si desidera assegnare come proprietario dispositivo.

4. Nella finestra delle impostazioni utente visualizzata, selezionare la scheda **Dispositivi**.
5. Fare clic su **Aggiungi**.
6. Dall'elenco dei dispositivi selezionare il dispositivo che si desidera assegnare all'utente.
7. Fare clic su **OK**.

Il dispositivo selezionato verrà aggiunto all'elenco dei dispositivi assegnati all'utente.

È possibile eseguire la stessa operazione in **Risorse (dispositivi)** → **Dispositivi gestiti**, facendo clic sul nome del dispositivo che si desidera assegnare e quindi facendo clic sul collegamento **Gestisci proprietario dispositivo**.

Configurazione della verifica in due passaggi per tutti gli utenti

Questo scenario descrive come abilitare la verifica in due passaggi per tutti gli utenti e come escludere gli account utente dalla verifica in due passaggi. Se non è stata abilitata la verifica in due passaggi per il proprio account prima di abilitarla per tutti gli altri utenti, l'applicazione apre innanzitutto la finestra per abilitare la verifica in due passaggi per il proprio account. Questo scenario descrive anche come abilitare la verifica in due passaggi per il proprio account.

> Se è stata abilitata la verifica in due passaggi per il proprio account, è possibile procedere al passaggio di abilitazione della verifica in due passaggi per tutti gli utenti.

Prerequisiti

Prima di iniziare:

- Assicurarsi che il proprio account utente disponga del diritto Modifica elenchi di controllo degli accessi agli oggetti dell'area funzionale **Caratteristiche generali: Autorizzazioni utente** per la modifica delle impostazioni di protezione per gli account di altri utenti.
- Assicurarsi che gli altri utenti di Administration Server installino un'app di autenticazione nei propri dispositivi.

Passaggi

L'abilitazione della verifica in due passaggi per tutti gli utenti procede per fasi:

1. **Installazione di un'app di autenticazione in un dispositivo**

   È possibile installare qualsiasi applicazione che supporti l'algoritmo TOTP (Time-based One-time Password), ad esempio:

   - Google Authenticator
   - Microsoft Authenticator
   - Bitrix24 OTP
   - Yandex ID

- Avanpost Authenticator
- Aladdin 2FA

Per verificare se Kaspersky Security Center supporta l'app di autenticazione che si desidera utilizzare, abilitare la verifica in due passaggi per tutti gli utenti o per un determinato utente.

Uno dei passaggi suggerisce di specificare il codice di sicurezza generato dall'app di autenticazione. In caso di esito positivo, Kaspersky Security Center supporta l'applicazione di autenticazione selezionata.

> Si sconsiglia vivamente di installare l'app di autenticazione nello stesso dispositivo da cui viene stabilita la connessione ad Administration Server.

2. **Sincronizzazione dell'ora dell'app di autenticazione con l'ora del dispositivo in cui è installato Administration Server**

   Verificare che l'ora nel dispositivo con l'app di autenticazione e l'ora nel dispositivo con Administration Server siano sincronizzate con UTC, utilizzando fonti orarie esterne. In caso contrario, potrebbero verificarsi errori durante l'autenticazione e l'attivazione della verifica in due passaggi.

3. **Abilitazione della verifica in due passaggi per il proprio account e ricezione della chiave segreta per il proprio account**

   Istruzioni dettagliate:

   - Per Administration Console basata su MMC: Abilitazione della verifica in due passaggi per il proprio account
   - Per Kaspersky Security Center Web Console: Abilitazione della verifica in due passaggi per il proprio account

   Dopo aver abilitato la verifica in due passaggi per il proprio account, è possibile abilitare la verifica in due passaggi per tutti gli utenti.

4. **Abilitazione della verifica in due passaggi per tutti gli utenti**

   Gli utenti con la verifica in due passaggi abilitata devono utilizzarla per accedere ad Administration Server.

   Istruzioni dettagliate:

   - Per Administration Console basata su MMC: Abilitazione della verifica in due passaggi per tutti gli utenti
   - Per Kaspersky Security Center Web Console: Abilitazione della verifica in due passaggi per tutti gli utenti

5. **Modifica del nome dell'emittente del codice di sicurezza**

   Se si dispone di più Administration Server con nomi simili, potrebbe essere necessario modificare i nomi dell'emittente del codice di sicurezza per un migliore riconoscimento dei diversi Administration Server.

   Istruzioni dettagliate:

   - Per Administration Console basata su MMC: Modifica del nome dell'emittente del codice di sicurezza
   - Per Kaspersky Security Center Web Console: Modifica del nome dell'emittente del codice di sicurezza

6. **Esclusione degli account utente per cui non è necessario abilitare la verifica in due passaggi**

   Se necessario, è possibile escludere gli utenti dalla verifica in due passaggi. Gli utenti con account esclusi non devono utilizzare la verifica in due passaggi per accedere ad Administration Server.

   Istruzioni dettagliate:

   - Per Administration Console basata su MMC: Esclusione degli account dalla verifica in due passaggi

- Per Kaspersky Security Center Web Console: Esclusione degli account dalla verifica in due passaggi

7. **Configurazione della verifica in due passaggi per il proprio account**

   Se gli utenti non sono esclusi dalla verifica in due passaggi e la verifica in due passaggi non è ancora configurata per i propri account, è necessario configurarla nella finestra che si apre quando accedono a Kaspersky Security Center. In caso contrario, non saranno in grado di accedere ad Administration Server in base ai propri diritti.

   Istruzioni dettagliate:

   - Per Administration Console basata su MMC: Configurazione della verifica in due passaggi per il proprio account
   - Per Kaspersky Security Center Web Console: Configurazione della verifica in due passaggi per il proprio account

Risultati

Al termine di questo scenario:

- La verifica in due passaggi è stata abilitata per l'account.
- La verifica in due passaggi è abilitata per tutti gli account utente di Administration Server, ad eccezione degli account utente che sono stati esclusi.

Informazioni sulla verifica in due passaggi

Quando la verifica in due passaggi è abilitata per un account, è necessario un codice di sicurezza monouso, oltre al nome utente e alla password, per accedere ad Administration Console o Kaspersky Security Center Web Console. Con l'autenticazione del dominio abilitata, l'utente deve solo immettere il codice di sicurezza monouso.

Per utilizzare la verifica in due passaggi, installa un'app di autenticazione che generi codici di protezione monouso nel dispositivo mobile o nel computer. È possibile utilizzare qualsiasi applicazione che supporti l'algoritmo TOTP (Time-based One-time Password), ad esempio:

- Google Authenticator
- Microsoft Authenticator
- Bitrix24 OTP
- Yandex ID
- Avanpost Authenticator
- Aladdin 2FA

Per verificare se Kaspersky Security Center supporta l'app di autenticazione che si desidera utilizzare, abilitare la verifica in due passaggi per tutti gli utenti o per un determinato utente.

Uno dei passaggi suggerisce di specificare il codice di sicurezza generato dall'app di autenticazione. In caso di esito positivo, Kaspersky Security Center supporta l'applicazione di autenticazione selezionata.

Si consiglia vivamente di salvare la chiave segreta o il codice QR e conservarla in un luogo sicuro. Questo codice consentirà di ripristinare l'accesso a Kaspersky Security Center Web Console nel caso in cui si perda l'accesso al dispositivo mobile.

Per proteggere l'utilizzo di Kaspersky Security Center, è possibile abilitare la verifica in due passaggi per il proprio account e abilitare la verifica in due passaggi per tutti gli utenti.

È possibile escludere gli account dalla verifica in due passaggi. Questa operazione può essere necessaria per gli account di servizio che non possono ricevere un codice di sicurezza per l'autenticazione.

Regole e limitazioni

Per poter attivare la verifica in due passaggi per tutti gli utenti e disattivare la verifica in due passaggi per utenti particolari:

- Verificare che l'account disponga del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.
- Abilitare la verifica in due passaggi per il proprio account.

Per poter disattivare la verifica in due passaggi per tutti gli utenti:

- Verificare che l'account disponga del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.
- Accedere a Kaspersky Security Center Web Console utilizzando la verifica in due passaggi.

Se la verifica in due passaggi è abilitata per un account utente in Kaspersky Security Center Administration Server versione 13 o successive, l'utente non sarà in grado di accedere a Kaspersky Security Center Web Console versione 12, 12.1 o 12.2.

Riemissione della chiave segreta

Qualsiasi utente può riemettere la chiave segreta utilizzata per la verifica in due passaggi. Quando un utente accede ad Administration Server con la chiave segreta riemessa, la nuova chiave segreta viene salvata per l'account utente. Se l'utente immette la nuova chiave segreta in modo errato, la nuova chiave segreta non viene salvata e la chiave segreta corrente rimane valida.

Un codice di sicurezza ha un identificatore denominato *nome dell'emittente*. Il nome dell'emittente del codice di sicurezza viene utilizzato come identificatore di Administration Server nell'app di autenticazione. Il nome dell'emittente del codice di sicurezza ha un valore predefinito uguale al nome di Administration Server. È possibile modificare il nome dell'emittente del codice di sicurezza. Se si modifica il nome dell'emittente del codice di sicurezza, è necessario emettere una nuova chiave segreta e passarla all'app di autenticazione.

Abilitazione della verifica in due passaggi per il proprio account (Web Console)

È possibile abilitare la verifica in due passaggi solo per il proprio account.

Prima di abilitare la verifica in due passaggi per il proprio account, assicurarsi che nel dispositivo mobile sia installata un'app di autenticazione. Assicurarsi che l'ora impostata nell'app di autenticazione sia sincronizzata con l'ora impostata nel dispositivo in cui è installato Administration Server.

Per abilitare la verifica in due passaggi per un account utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Utenti**.
2. Fare clic sul nome dell'account.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Sicurezza in fase di autenticazione**.
4. Nella scheda **Sicurezza in fase di autenticazione**:
   a. Selezionare l'opzione **Richiedi nome utente, password e codice di sicurezza (verifica in due passaggi)**. Fare clic sul pulsante **Salva**.
   b. Nella finestra della verifica in due passaggi visualizzata, fare clic su **Come configurare la verifica in due passaggi**.
      Immettere la chiave segreta nell'app di autenticazione o fare clic su **Visualizza codice QR** ed eseguire la scansione del codice QR tramite l'app di autenticazione sul dispositivo mobile per ricevere il codice di sicurezza monouso.
   c. Nella finestra della verifica in due passaggi specificare il codice di sicurezza generato dall'app di autenticazione, quindi fare clic sul pulsante **Controlla e applica**.
5. Fare clic sul pulsante **Salva**.

La verifica in due passaggi è stata abilitata per l'account.

Abilitazione della verifica in due passaggi per il proprio account (basata su MMC)

Prima di abilitare la verifica in due passaggi per il proprio account, assicurarsi che nel dispositivo mobile sia installata un'app di autenticazione. Assicurarsi che l'ora impostata nell'app di autenticazione sia sincronizzata con l'ora di Administration Server.

Per abilitare la verifica in due passaggi per il proprio account:

1. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server**, quindi selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server accedere al riquadro **Sezioni** e selezionare **Avanzate**, quindi **Verifica in due passaggi**.

3. Nella sezione **Verifica in due passaggi** fare clic sul pulsante **Configura**.

   > Se la verifica in due passaggi è già abilitata per l'account, fare clic sul pulsante **Configura** per reimpostare la chiave segreta in modo da poter riconfigurare la verifica in due passaggi.

   Nella finestra delle proprietà della verifica in due passaggi visualizzata verrà mostrata la chiave segreta.

4. Immettere la chiave segreta nell'app di autenticazione per ricevere il codice di sicurezza monouso. È possibile specificare manualmente la chiave segreta nell'app di autenticazione o eseguire la scansione del codice QR con l'app di autenticazione tramite il dispositivo mobile.

5. Specificare il codice di sicurezza generato dall'app di autenticazione, quindi fare clic sul pulsante **OK** per uscire dalla finestra delle proprietà della verifica in due passaggi.

6. Fare clic sul pulsante **Applica**.

7. Fare clic sul pulsante **OK**.

La verifica in due passaggi è stata abilitata per il proprio account.

Abilitazione della verifica in due passaggi richiesta per tutti gli utenti (Web Console)

È possibile abilitare la verifica in due passaggi per tutti gli utenti di Administration Server se il proprio account dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente** e se è stata eseguita l'autenticazione utilizzando la verifica in due passaggi.

Per abilitare la verifica in due passaggi per tutti gli utenti:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Sicurezza in fase di autenticazione** della finestra delle proprietà spostare l'interruttore dell'opzione di **verifica in due passaggi per tutti gli utenti** sulla posizione "abilitato".

3. Se non è stata abilitata la verifica in due passaggi per il proprio account, l'applicazione apre la finestra per abilitare la verifica in due passaggi per il proprio account.

   a. Nella finestra della verifica in due passaggi, fare clic su **Come configurare la verifica in due passaggi**.

   b. Immettere la chiave segreta manualmente nell'applicazione di autenticazione o fare clic su **Visualizza codice QR** ed eseguire la scansione del codice QR tramite l'applicazione di autenticazione sul dispositivo mobile per ricevere il codice di sicurezza monouso.

   c. Nella finestra della verifica in due passaggi specificare il codice di sicurezza generato dall'applicazione di autenticazione, quindi fare clic sul pulsante **Controlla e applica**.

La verifica in due passaggi è abilitata per tutti gli utenti. D'ora in poi gli utenti di Administration Server, inclusi gli utenti aggiunti dopo aver abilitato la verifica in due passaggi per tutti gli utenti, dovranno configurare la verifica in due passaggi per i propri account, ad eccezione degli utenti esclusi dalla verifica in due passaggi.

Abilitazione della verifica in due passaggi per tutti gli utenti (basata su MMC)

È possibile abilitare la verifica in due passaggi per tutti gli utenti di Administration Server se il proprio account dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente** e se è stata eseguita l'autenticazione utilizzando la verifica in due passaggi.

Per abilitare la verifica in due passaggi per tutti gli utenti:

1. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server**, quindi selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni** selezionare **Avanzate**, quindi **Verifica in due passaggi**.
3. Fare clic sul pulsante **Imposta come obbligatoria** per abilitare la verifica in due passaggi per tutti gli utenti.
4. Se non è stata abilitata la verifica in due passaggi per il proprio account, l'applicazione apre la finestra per abilitare la verifica in due passaggi per il proprio account.
    a. Immettere la chiave segreta nell'app di autenticazione per ricevere il codice di sicurezza monouso. È possibile specificare manualmente la chiave segreta nell'app di autenticazione o eseguire la scansione del codice QR dall'app di autenticazione sul dispositivo mobile per ricevere il codice di sicurezza monouso.
    b. Specificare il codice di sicurezza generato dall'app di autenticazione, quindi fare clic sul pulsante **OK** per uscire dalla finestra delle proprietà della verifica in due passaggi.
5. Nella sezione **Verifica in due passaggi** fare clic sul pulsante **Applica**, quindi fare clic sul pulsante **OK**.

La verifica in due passaggi è abilitata per tutti gli utenti. D'ora in poi tutti gli utenti di Administration Server, inclusi gli utenti aggiunti dopo aver abilitato questa opzione, dovranno configurare la verifica in due passaggi per i propri account, ad eccezione degli utenti i cui account sono esclusi dalla verifica in due passaggi.

Disabilitazione della verifica in due passaggi per un account utente (Web Console)

È possibile disabilitare la verifica in due passaggi per il proprio account, nonché per l'account di un altro utente.

È possibile disabilitare la verifica in due passaggi di un altro account utente se il proprio account dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente** e se è stata eseguita l'autenticazione utilizzando la verifica in due passaggi.

Per disabilitare la verifica in due passaggi per un account utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Utenti**.
2. Fare clic sul nome dell'account utente interno per cui si desidera disabilitare la verifica in due passaggi. Può trattarsi del proprio account o dell'account di un altro utente.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Protezione account**.

4. Nella scheda **Protezione account** selezionare l'opzione **Richiedi solo nome utente e password** se si desidera disabilitare la verifica in due passaggi per un account utente.

5. Fare clic sul pulsante **Salva**.

La verifica in due passaggi è disabilitata per l'account utente.

Se si desidera ripristinare l'accesso per un utente che non può accedere a Kaspersky Security Center Web Console utilizzando la verifica in due passaggi, disabilitare la verifica in due passaggi per questo account utente, quindi selezionare l'opzione **Richiedi solo nome utente e password** come descritto sopra. Successivamente, accedere a Kaspersky Security Center Web Console con l'account utente per il quale è stata disabilitata la verifica in due passaggi, quindi abilitare nuovamente la verifica.

Disabilitazione della verifica in due passaggi per un account utente (basata su MMC)

Per disabilitare la verifica in due passaggi per il proprio account:

1. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server**, quindi selezionare **Proprietà**.

2. Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni** selezionare **Avanzate**, quindi **Verifica in due passaggi**.

3. Nella sezione **Verifica in due passaggi** fare clic sul pulsante **Disabilita**.

4. Fare clic sul pulsante **Applica**.

5. Fare clic sul pulsante **OK**.

La verifica in due passaggi è stata disabilitata per il proprio account.

È possibile disabilitare la verifica in due passaggi degli account di altri utenti. In questo modo viene garantita la protezione ad esempio nel caso in cui un utente perda o rompa un dispositivo mobile.

È possibile disabilitare la verifica in due passaggi di un altro account utente se si dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente** e se è stata eseguita l'autenticazione utilizzando la verifica in due passaggi. Seguendo la procedura di seguito è possibile disabilitare la verifica in due passaggi anche per il proprio account.

Per disabilitare la verifica in due passaggi per qualsiasi account utente:

1. Nella struttura della console aprire la cartella **Account utente**.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.

2. Nell'area di lavoro fare doppio clic sull'account utente per cui si desidera disabilitare la verifica in due passaggi.

   Per tutti gli account utente per cui è abilitata la verifica in due passaggi, la colonna **Autenticazione a due fattori richiesta** è impostata su **Sì**.

3. Nella finestra **Proprietà:<nome utente>** visualizzata selezionare la sezione **Verifica in due passaggi**.

4. Nella sezione **Verifica in due passaggi** selezionare le seguenti opzioni:

   - Se si desidera disabilitare la verifica in due passaggi per un account utente, fare clic sul pulsante **Disabilita**.
   - Se si desidera escludere questo account utente dalla verifica in due passaggi, selezionare l'opzione **L'utente può eseguire l'autenticazione utilizzando solo nome utente e password**.

5. Fare clic sul pulsante **Applica**.
6. Fare clic sul pulsante **OK**.

La verifica in due passaggi per un account utente è stata disabilitata.

Se si desidera ripristinare l'accesso per un utente che non può accedere ad Administration Console utilizzando la verifica in due passaggi, disabilitare la verifica in due passaggi per questo account utente e selezionare l'opzione **L'utente può eseguire l'autenticazione utilizzando solo nome utente e password** in **Verifica in due passaggi** come descritto sopra. Successivamente, accedere ad Administration Console con l'account utente per il quale è stata disabilitata la verifica in due passaggi, quindi abilitare nuovamente la verifica.

Disabilitazione della verifica in due passaggi richiesta per tutti gli utenti (Web Console)

È possibile disabilitare la verifica in due passaggi richiesta per tutti gli utenti se la verifica in due passaggi è abilitata per il proprio account e se quest'ultimo dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**. Se la verifica in due passaggi non è abilitata per il proprio account, è necessario abilitare la verifica in due passaggi per il proprio account prima di disabilitarla per tutti gli utenti.

Per disabilitare la verifica in due passaggi per tutti gli utenti:

1. Nel menu principale, fare clic sull'icona delle impostazioni () accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Sicurezza in fase di autenticazione** della finestra delle proprietà spostare l'interruttore dell'opzione di **verifica in due passaggi per tutti gli utenti** sulla posizione "disabilitato".

La verifica in due passaggi è disabilitata per tutti gli utenti. La disabilitazione della verifica in due passaggi per tutti gli utenti non si applica agli account specifici per i quali la verifica in due passaggi è stata precedentemente abilitata separatamente.

Disabilitazione della verifica in due passaggi richiesta per tutti gli utenti (basata su MMC)

È possibile disabilitare la verifica in due passaggi richiesta per tutti gli utenti di Administration Server se si dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente** e se è stata eseguita l'autenticazione utilizzando la verifica in due passaggi.

Per disabilitare la verifica in due passaggi per tutti gli utenti:

1. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server**, quindi selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni** selezionare **Avanzate**, quindi **Verifica in due passaggi**.
3. Fare clic sul pulsante **Imposta come facoltativa** per disabilitare la verifica in due passaggi per tutti gli utenti.
4. Fare clic sul pulsante **Applica** nella sezione **Verifica in due passaggi**.
5. Fare clic sul pulsante **OK** nella sezione **Verifica in due passaggi**.

La verifica in due passaggi è disabilitata per tutti gli utenti. La disabilitazione della verifica in due passaggi per tutti gli utenti non si applica agli account specifici per i quali la verifica in due passaggi è stata precedentemente abilitata separatamente.

Esclusione di account dalla verifica in due passaggi (Web Console)

È possibile escludere gli account utente dalla verifica in due passaggi se si dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

Se un account utente viene escluso dall'elenco della verifica in due passaggi per tutti gli utenti, tale utente non deve utilizzare la verifica in due passaggi.

> L'esclusione degli account dalla verifica in due passaggi può essere necessaria per gli account di servizio che non possono passare il codice di sicurezza durante l'autenticazione.

Se si desidera escludere alcuni account utente dalla verifica in due passaggi:

1. Se si desidera escludere account Active Directory, è necessario eseguire il polling del controller di dominio di Microsoft Active Directory per aggiornare l'elenco degli utenti di Administration Server.
2. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
3. Nella scheda **Sicurezza in fase di autenticazione** della finestra delle proprietà, nella tabella delle esclusioni dalla verifica in due passaggi fare clic sul pulsante **Aggiungi**.
4. Nella finestra visualizzata:
   a. Selezionare gli account utente che si desidera escludere.
   b. Fare clic sul pulsante **OK**.

Gli account utente selezionati vengono esclusi dalla verifica in due passaggi.

Esclusione di account dalla verifica in due passaggi (basata su MMC)

È possibile escludere un account dalla verifica in due passaggi se il proprio account dispone del diritto Modifica elenchi di controllo degli accessi agli oggetti nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

Se un account utente viene escluso dalla verifica in due passaggi, l'utente può accedere ad Administration Console o Kaspersky Security Center Web Console senza utilizzare la verifica in due passaggi.

L'esclusione degli account dalla verifica in due passaggi può essere necessaria per gli account di servizio che non possono passare il codice di sicurezza durante l'autenticazione.

Per escludere un account utente dalla verifica in due passaggi:

1. Se si desidera escludere un account Active Directory, eseguire il polling di Active Directory per aggiornare l'elenco degli utenti di Administration Server.
2. Nella struttura della console aprire la cartella **Account utente**.

   La cartella **Account utente** è una sottocartella della cartella **Avanzate** per impostazione predefinita.
3. Nell'area di lavoro fare doppio clic sull'account utente che si desidera escludere dalla verifica in due passaggi
4. Nella finestra **Proprietà:<nome utente>** visualizzata selezionare la sezione **Verifica in due passaggi**.
5. Nella sezione visualizzata selezionare l'opzione **L'utente può eseguire l'autenticazione utilizzando solo nome utente e password**.
6. Nella sezione **Verifica in due passaggi** fare clic sul pulsante **Applica**, quindi fare clic sul pulsante **OK**.

Questo account utente è escluso dalla verifica in due passaggi. È possibile controllare gli account esclusi nell'elenco degli account utente.

Modifica del nome dell'emittente del codice di sicurezza (Web Console)

È possibile disporre di più identificatori (chiamati emittenti) per diversi Administration Server. È possibile modificare il nome dell'emittente di un codice di sicurezza ad esempio nel caso in cui Administration Server utilizzi già un nome simile dell'emittente del codice di sicurezza per un altro Administration Server. Per impostazione predefinita, il nome dell'emittente di un codice di sicurezza è uguale al nome di Administration Server.

Dopo aver modificato il nome dell'emittente del codice di sicurezza, è necessario riemettere una nuova chiave segreta e passarla all'app di autenticazione.

Per specificare un nuovo nome dell'emittente del codice di sicurezza:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Protezione account**.

3. Nella scheda **Protezione account** fare clic sul collegamento **Modifica**.

   Verrà visualizzata la sezione **Modifica emittente codice di sicurezza**.

4. Specificare un nuovo nome dell'emittente del codice di sicurezza.

5. Fare clic sul pulsante **OK**.

Viene specificato un nuovo nome dell'emittente del codice di sicurezza per Administration Server.

Modifica del nome dell'emittente del codice di sicurezza (basata su MMC)

È possibile disporre di più identificatori (chiamati emittenti) per diversi Administration Server. È possibile modificare il nome dell'emittente di un codice di sicurezza ad esempio nel caso in cui Administration Server utilizzi già un nome simile dell'emittente del codice di sicurezza per un altro Administration Server. Per impostazione predefinita, il nome dell'emittente di un codice di sicurezza è uguale al nome di Administration Server.

Dopo aver modificato il nome dell'emittente del codice di sicurezza, è necessario riemettere una nuova chiave segreta e passarla all'app di autenticazione.

Per specificare un nuovo nome dell'emittente del codice di sicurezza:

1. Nella struttura della console di Kaspersky Security Center aprire il menu di scelta rapida della cartella **Administration Server**, quindi selezionare **Proprietà**.

2. Nella finestra delle proprietà di Administration Server, nel riquadro **Sezioni** selezionare **Avanzate**, quindi **Verifica in due passaggi**.

3. Specificare un nuovo nome dell'emittente del codice di sicurezza nel campo **Emittente codice di sicurezza**.

4. Fare clic sul pulsante **Applica** nella sezione **Verifica in due passaggi**.

5. Fare clic sul pulsante **OK** nella sezione **Verifica in due passaggi**.

Viene specificato un nuovo nome dell'emittente del codice di sicurezza per Administration Server.

Configurazione della verifica in due passaggi per il proprio account (Web Console)

La prima volta che si accede a Kaspersky Security Center dopo l'abilitazione della verifica in due passaggi, si apre la finestra per la configurazione della verifica in due passaggi per l'account.

Prima di configurare la verifica in due passaggi per il proprio account, assicurarsi che nel dispositivo mobile sia installata un'app di autenticazione.

Verificare che l'ora nel dispositivo con l'app di autenticazione e l'ora nel dispositivo con Administration Server siano sincronizzate con UTC, utilizzando fonti orarie esterne.

Per configurare la verifica in due passaggi per il proprio account:

1. Generare un codice di sicurezza monouso utilizzando l'app di autenticazione sul dispositivo mobile. A tale scopo, eseguire una delle azioni seguenti:

   - Immettere manualmente la chiave segreta nell'app di autenticazione.
   - Fare clic su **Visualizza codice QR** ed eseguire la scansione del codice QR utilizzando l'app di autenticazione.

   Verrà visualizzato un codice di sicurezza sul dispositivo mobile.

2. Nella finestra di configurazione della verifica in due passaggi specificare il codice di sicurezza generato dall'app di autenticazione, quindi fare clic sul pulsante **Controlla e applica**.

La verifica in due passaggi viene configurata per il proprio account. È possibile accedere ad Administration Server in base ai propri diritti.

Configurazione della verifica in due passaggi per il proprio account (basata su MMC)

La prima volta che si accede a Kaspersky Security Center dopo l'abilitazione della verifica in due passaggi, si apre la finestra per la configurazione della verifica in due passaggi per l'account.

Prima di configurare la verifica in due passaggi per il proprio account, assicurarsi che nel dispositivo mobile sia installata un'app di autenticazione. Verificare che l'ora nel dispositivo con l'app di autenticazione e l'ora nel dispositivo con Administration Server siano sincronizzate con UTC, utilizzando fonti orarie esterne.

Per configurare la verifica in due passaggi per il proprio account:

1. Generare un codice di sicurezza monouso utilizzando l'app di autenticazione sul dispositivo mobile. A tale scopo, eseguire una delle azioni seguenti:

   - Immettere manualmente la chiave segreta nell'app di autenticazione.
   - Scansionare il codice QR utilizzando l'app di autenticazione.

   Verrà visualizzato un codice di sicurezza sul dispositivo mobile.

2. Nella finestra **Impostare la verifica in due passaggi**, specificare il codice di sicurezza generato dall'app di autenticazione, quindi fare clic sul pulsante **OK**.

La verifica in due passaggi viene configurata per il proprio account. È possibile accedere ad Administration Server in base ai propri diritti.

Generazione di una nuova chiave segreta

È possibile generare una nuova chiave segreta per la verifica in due passaggi per il proprio account solo se è stata eseguita l'autorizzazione utilizzando la verifica in due passaggi.

Per generare una nuova chiave segreta per un account utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Utenti**.
2. Fare clic sul nome dell'account utente per cui si desidera generare una nuova chiave segreta per la verifica in due passaggi.
3. Nella finestra delle impostazioni utente visualizzata selezionare la scheda **Protezione account**.
4. Nella scheda **Protezione account** fare clic sul collegamento **Genera una nuova chiave segreta**.
5. Nella finestra della verifica in due passaggi visualizzata specificare una nuova chiave di sicurezza generata dall'app di autenticazione.
6. Fare clic sul pulsante **Controlla e applica**.

Viene generata una nuova chiave segreta per l'utente.

Se il dispositivo mobile viene smarrito, è possibile installare un'app di autenticazione in un altro dispositivo mobile e generare una nuova chiave segreta per ripristinare l'accesso a Kaspersky Security Center Web Console.

Impedisci ai nuovi utenti di impostare la verifica in due passaggi per se stessi

Per migliorare ulteriormente la protezione dell'accesso a Kaspersky Security Center Web Console, è possibile impedire ai nuovi utenti di impostare autonomamente la verifica in due passaggi.

Quando questa opzione è abilitata, un utente con la verifica in due passaggi disabilitata, ad esempio un nuovo amministratore di dominio, non può configurare autonomamente la verifica in due passaggi. Pertanto, tale utente non può essere autenticato in Administration Server e non può accedere a Kaspersky Security Center Web Console senza l'approvazione di un altro amministratore di Kaspersky Security Center che ha già abilitato la verifica in due passaggi.

Questa opzione è disponibile se la verifica in due passaggi è abilitata per tutti gli utenti.

Per impedire ai nuovi utenti di impostare autonomamente la verifica in due passaggi:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Sicurezza in fase di autenticazione** della finestra delle proprietà, spostare l'interruttore **Vieta ai nuovi utenti di impostare la verifica in due passaggi per se stessi** nella posizione di abilitazione.

Questa opzione non influisce sugli account utente aggiunti alle esclusioni della verifica in due passaggi.

Per concedere a Kaspersky Security Center Web Console l'accesso a un utente con la verifica in due passaggi disabilitata, disattivare temporaneamente l'opzione **Vieta ai nuovi utenti di impostare la verifica in due passaggi per se stessi**, chiedere all'utente di abilitare la verifica in due passaggi, quindi riattivare l'opzione.

Assegnazione di un utente come proprietario dispositivo Linux dopo l'installazione di Network Agent

Per consentire all'utente di registrarsi come proprietario del dispositivo Linux:

1. In Kaspersky Security Center Web Console, accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

   Viene aperto l'elenco dei pacchetti di installazione.

2. Fare clic sul pacchetto di installazione di Network Agent.

   Verrà visualizzata la finestra delle proprietà del pacchetto di installazione.

3. Nella finestra delle proprietà del pacchetto di installazione, fare clic su **Impostazioni** → **Avanzate**.

4. Nella sezione **Registrazione dell'utente come proprietario del dispositivo (solo Linux)**, attivare l'opzione **Consenti l'esecuzione dell'utilità di registrazione utente dopo l'installazione di Network Agent** e fare clic su **Salva**.

L'utilità per la registrazione dell'utente come proprietario dispositivo può essere eseguita tramite la riga di comando nel dispositivo client.

Per registrare un utente come proprietario del dispositivo Linux nel dispositivo client:

1. Eseguire il seguente comando nella riga di comando nel dispositivo client:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner
   ```

2. Immettere nome utente e password, se richiesti.

   Se login e password sono inclusi nel file di risposta o nel pacchetto di installazione di Network Agent, eseguire il seguente comando nella riga di comando nel dispositivo client:
   ```
   $ /opt/kaspersky/klnagent64/bin/nagregister -set_owner -unattended
   ```

Se l'utente è incluso in un gruppo di protezione interno, l'accesso deve contenere il nome utente.

Se l'utente è incluso in un gruppo di protezione di Active Directory, l'accesso deve contenere il nome utente e il nome di dominio.

Se per l'utente è attivata la verifica in due passaggi, è necessario immettere la password TOTP (Time-based One-time Password) generata dall'app.

L'utente verrà registrato come proprietario dispositivo.

Eliminazione di un utente o un gruppo di protezione

È possibile eliminare solo utenti interni o gruppi di protezione interni.

Per eliminare un utente o un gruppo di protezione:

1. Nel menu principale, passare su **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti** o **Gruppi**.
2. Selezionare la casella di controllo accanto all'utente o al gruppo di protezione che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Nella finestra visualizzata fare clic su **OK**.

L'utente o il gruppo di protezione verrà eliminato.

Modifica della password per un account utente

Potrebbe essere necessario modificare la password del proprio account o di un altro account utente se la password corrente sta per scadere o se si desidera modificarla con una più sicura.

La password deve rispettare le seguenti regole:

- La password deve avere una lunghezza compresa tra 8 e 256 caratteri.
- La password deve contenere caratteri da almeno tre dei gruppi elencati di seguito:
  - Lettere maiuscole (A-Z)
  - Lettere minuscole (a-z)
  - Numeri (0-9)
  - Caratteri speciali (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- La password non deve contenere spazi, caratteri Unicode o la combinazione di "." e "@", quando "." si trova prima di "@".

Modifica della password del proprio account

Per modificare la password per il proprio account:

1. Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Cambia password**.
2. Immettere la password corrente, quindi specificare la nuova password per la connessione a Kaspersky Security Center.

   Per visualizzare la password immessa, fare clic su .
3. Se l'account è protetto dalle modifiche non autorizzate, è necessario confermare di disporre delle autorizzazioni per modificare l'account. Nella finestra **Protezione account** specificare le credenziali del proprio account o dell'account con il diritto Modifica ACL oggetti nell'area Funzionalità Generali: Autorizzazioni utente.
4. Se la verifica in due passaggi è abilitata per l'account utilizzato nel passaggio precedente, immettere il codice di sicurezza generato dall'app di autenticazione nel dispositivo mobile.

Modifica della password per un account utente interno

Per modificare la password per un account utente interno:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account utente che si desidera modificare.
3. Nella finestra delle impostazioni utente visualizzata, nella scheda **Generale**, fare clic sul pulsante **Cambia password**.
4. Impostare una nuova password per la connessione dell'utente a Kaspersky Security Center.

   Per visualizzare la password immessa, fare clic su .
5. Se necessario, abilitare l'opzione **L'utente deve modificare la password al primo accesso** per forzare la modifica della password al momento dell'autenticazione dell'utente successivo.
6. Se l'account utente è protetto dalle modifiche non autorizzate, è necessario confermare di disporre delle autorizzazioni per modificare l'account. Nella finestra **Protezione account**, specificare le credenziali dell'account con il diritto Modifica ACL oggetti nell'area Funzionalità generali: Autorizzazioni utente.

Configurazione delle opzioni per la modifica di una password utilizzando i contrassegni del server

È possibile utilizzare l'utilità klscflag per configurare la modifica della password utilizzando i seguenti comandi:

- Configurazione del periodo di rotazione delle password (contrassegno `LP_SplPwdChangePeriodDays`)

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangePeriodDays -t d -v <periodo_rotazione>`

  Dove `<rotation_period>` è un periodo di tempo in giorni dopo il quale scade la password utente. Valori possibili: 0-730. Se il valore del parametro è 0, la rotazione della password è disabilitata.

- Configurazione dell'ora dell'avviso preliminare sulla necessità di modificare la password (contrassegno `LP_SplPwdChangeNotificationHours`)

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdChangeNotificationHours -t d -v <periodo_avviso>`

  Dove `<periodo_avviso>` è un periodo di tempo espresso in ore prima della scadenza della password utente. Durante questo periodo, viene visualizzata la notifica della necessità di modificare la password. Valori possibili: 0-17520. Se il valore del parametro è 0, il tempo di avviso corrisponde al 25% del periodo di rotazione della password.

- Specifica del valore predefinito dell'opzione **L'utente deve modificare la password al primo accesso** (il contrassegno `LP_SplPwdForceChange`)

  `klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_SplPwdForceChange -t d -v <valore>`

  Dove i possibili valori del contrassegno `<valore>`:

  `1`: l'opzione **L'utente deve modificare la password al primo accesso** è abilitata.

  `0`: l'opzione **L'utente deve modificare la password al primo accesso** è disabilitata.

Per visualizzare il valore corrente del contrassegno, eseguire il seguente comando:

```
klscflag.exe -fget -pv .core/.independent -s KLLIM -n <flag> -t d
```

Dove <contrassegno> è il contrassegno `LP_SplPwdChangePeriodDays`, `LP_SplPwdChangeNotificationHours` o `LP_SplPwdForceChange`.

Creazione di un ruolo utente

Per creare un ruolo utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Nome nuovo ruolo** visualizzata immettere il nome del nuovo ruolo.
4. Fare clic su **OK** per applicare le modifiche.
5. Nella finestra delle proprietà del ruolo visualizzata modificare le impostazioni del ruolo:
   - Nella scheda **Generale** modificare il nome del ruolo.
     Non è possibile modificare il nome di un ruolo predefinito.
   - Nella scheda **Impostazioni** modificare l'ambito del ruolo, i criteri e i profili associati al ruolo.
   - Nella scheda **Diritti di accesso** modificare i diritti per l'accesso alle applicazioni Kaspersky.
6. Fare clic su **Salva** per salvare le modifiche.

Il nuovo ruolo verrà visualizzato nell'elenco dei ruoli utente.

Modifica di un ruolo utente

Per modificare un ruolo utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic sul nome del ruolo che si desidera modificare.
3. Nella finestra delle proprietà del ruolo visualizzata modificare le impostazioni del ruolo:
   - Nella scheda **Generale** modificare il nome del ruolo.
     Non è possibile modificare il nome di un ruolo predefinito.
   - Nella scheda **Impostazioni** modificare l'ambito del ruolo, i criteri e i profili associati al ruolo.
   - Nella scheda **Diritti di accesso** modificare i diritti per l'accesso alle applicazioni Kaspersky.
4. Fare clic su **Salva** per salvare le modifiche.

Il ruolo aggiornato verrà visualizzato nell'elenco dei ruoli utente.

Modifica dell'ambito di un ruolo utente

Un *ambito di un ruolo utente* è una combinazione di utenti e gruppi di amministrazione. Le impostazioni associate a un ruolo utente si applicano solo ai dispositivi che appartengono agli utenti con questo ruolo e solo se tali dispositivi appartengono a gruppi associati a questo ruolo, inclusi i gruppi figlio.

Per aggiungere utenti, gruppi di protezione e gruppi di amministrazione all'ambito di un ruolo utente, è possibile utilizzare una dei seguenti metodi:

Metodo 1:

1. Nel menu principale, passare su **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti** o **Gruppi**.
2. Selezionare le caselle di controllo accanto agli utenti o ai gruppi di protezione che si desidera aggiungere all'ambito del ruolo utente.
3. Fare clic sul pulsante **Assegna ruolo**.

   Verrà avviata l'Assegnazione guidata ruolo. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
4. Nel passaggio **Selezionare un ruolo** selezionare il ruolo utente che si desidera assegnare.
5. Nel passaggio **Definire l'ambito** selezionare il gruppo di amministrazione da aggiungere all'ambito del ruolo utente.
6. Fare clic sul pulsante **Assegna ruolo** per chiudere la finestra.

Gli utenti o i gruppi di protezione selezionati e il gruppo di amministrazione selezionato verranno aggiunti all'ambito del ruolo utente.

Metodo 2:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic sul nome del ruolo per cui si desidera definire l'ambito.
3. Nella finestra delle proprietà del ruolo visualizzata, selezionare la scheda **Impostazioni**.
4. Nella sezione **Ambito ruolo** fare clic su **Aggiungi**.

   Verrà avviata l'Assegnazione guidata ruolo. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
5. Nel passaggio **Definire l'ambito** selezionare il gruppo di amministrazione da aggiungere all'ambito del ruolo utente.
6. Nel passaggio **Selezionare gli utenti** della procedura guidata selezionare gli utenti e i gruppi di protezione che si desidera aggiungere all'ambito del ruolo utente.
7. Fare clic sul pulsante **Assegna ruolo** per chiudere la finestra.
8. Fare clic sul pulsante **Chiudi** (⨯) per chiudere la finestra delle proprietà del ruolo.

Gli utenti o i gruppi di protezione selezionati e il gruppo di amministrazione selezionato verranno aggiunti all'ambito del ruolo utente.

Metodo 3:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Diritti di accesso**, selezionare la casella di controllo accanto al nome dell'utente o del gruppo di sicurezza che si desidera aggiungere all'ambito dei ruoli utente, quindi fare clic sul pulsante **Ruoli**.

   Non è possibile selezionare più utenti o gruppi di sicurezza contemporaneamente. Se si selezionano più elementi, il pulsante **Ruoli** verrà disabilitato.

3. Nella finestra **Ruoli** selezionare il ruolo utente che si desidera assegnare, quindi applicare e salvare le modifiche.

   Gli utenti o i gruppi di protezione selezionati verranno aggiunti all'ambito del ruolo utente.

Eliminazione di un ruolo utente

Per eliminare un ruolo utente:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Selezionare la casella di controllo accanto al nome del ruolo che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Nella finestra visualizzata fare clic su **OK**.

Il ruolo utente verrà eliminato.

Associazione dei profili criterio ai ruoli

È possibile associare i ruoli utente ai profili criterio. In questo caso, la regola di attivazione per questo profilo criterio si basa sul ruolo: il profilo criterio diventa attivo per un utente che ha il ruolo specificato.

Il criterio vieta ad esempio un software di navigazione GPS in tutti i dispositivi in un gruppo di amministrazione. Il software di navigazione GPS è necessario in un solo dispositivo nel gruppo di amministrazione Utenti: quello di proprietà di un corriere. In questo caso, è possibile assegnare un ruolo "Corriere" al proprietario, quindi creare un profilo criterio che consente l'esecuzione del software di navigazione GPS solo nei dispositivi i cui proprietari hanno il ruolo "Corriere". Tutte le altre impostazioni del criterio vengono mantenute. Solo l'utente con il ruolo "Corriere" sarà autorizzato a eseguire il software di navigazione GPS. Se in seguito viene assegnato il ruolo "Corriere" a un altro dipendente, anche il nuovo dipendente potrà eseguire il software di navigazione nel dispositivo dell'organizzazione. L'esecuzione del software di navigazione GPS sarà ancora non consentita negli altri dispositivi dello stesso gruppo di amministrazione.

Per associare un ruolo a un profilo criterio:

1. Nel menu principale accedere a **Utenti e ruoli** → **Ruoli**.
2. Fare clic sul nome del ruolo che si desidera associare a un profilo criterio.

   Verrà visualizzata la finestra delle proprietà del ruolo, con la scheda **Generale** selezionata.

3. Selezionare la scheda **Impostazioni** e scorrere fino alla sezione **Criteri e profili**.

4. Fare clic su **Modifica**.

5. Per associare il ruolo a:

   - **Un profilo criterio esistente**: fare clic sull'icona della freccia di espansione (>) accanto al nome del criterio desiderato, quindi selezionare la casella di controllo accanto al profilo a cui associare il ruolo.

   - **Un nuovo profilo criterio**:

     a. Selezionare la casella di controllo accanto al criterio per cui si desidera creare un profilo.

     b. Fare clic su **Nuovo profilo criterio**.

     c. Specificare un nome per il nuovo profilo e configurare le impostazioni del profilo.

     d. Fare clic sul pulsante **Salva**.

     e. Selezionare la casella di controllo accanto al nuovo profilo.

6. Fare clic su **Assegna al ruolo**.

Il profilo verrà associato al ruolo e visualizzato nelle proprietà del ruolo. Il profilo si applica automaticamente a qualsiasi dispositivo il cui proprietario è assegnato al ruolo.

Propagazione dei ruoli utente agli Administration Server secondari

Per impostazione predefinita, gli elenchi dei ruoli utente degli Administration Server primari e secondari sono indipendenti. È possibile configurare l'applicazione in modo da propagare automaticamente i ruoli utente creati nell'Administration Server primario a tutti gli Administration Server secondari. I ruoli utente possono inoltre essere propagati da un Administration Server secondario ai relativi Administration Server secondari.

Per propagare i ruoli utente dall'Administration Server primario agli Administration Server secondari:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server, con la scheda **Generale** selezionata.

2. Passare alla sezione **Gerarchia di Administration Server**.

3. Abilitare l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari**, quindi fare clic sul pulsante **Salva**.

L'applicazione copierà i ruoli utente dell'Administration Server primario negli Administration Server secondari.

Quando l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari** è abilitata e vengono propagati i ruoli utente, questi non possono essere modificati o eliminati negli Administration Server secondari. Quando si crea un nuovo ruolo o si modifica un ruolo esistente nell'Administration Server primario, le modifiche vengono copiate automaticamente negli Administration Server secondari. Quando si elimina un ruolo utente nell'Administration Server primario, questo ruolo rimane negli Administration Server secondari, ma può essere modificato o eliminato.

I ruoli propagati all'Administration Server secondario dal server primario sono visualizzati con i segni di spunta verdi (✓). Non è possibile modificare tali ruoli nell'Administration Server secondario.

Se si crea un ruolo nell'Administration Server primario ed è presente un ruolo con lo stesso nome nell'Administration Server secondario, il nuovo ruolo viene copiato nell'Administration Server secondario con l'aggiunta di un indice al nome, ad esempio ~~1, ~~2 (l'indice può essere casuale).

Se si disabilita l'opzione **Trasferisci elenco dei ruoli agli Administration Server secondari**, tutti i ruoli utente restano negli Administration Server secondari, ma diventano indipendenti da quelli nell'Administration Server primario. Dopo essere diventati indipendenti, i ruoli utente negli Administration Server secondari possono essere modificati o eliminati.

Modifica della password dell'account

È possibile modificare la password dell'account locale, ad esempio quando l'utente dimentica la password dell'account locale o per eseguire una modifica pianificata della password.

La modifica della password verrà applicata anche se l'utente non ha eseguito l'accesso all'account. È inoltre possibile modificare la password per l'account root locale.

> Questa attività può essere eseguita solo nei dispositivi Linux.

Per modificare la password dell'account locale in dispositivi specifici:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.
   Verrà avviata la Creazione guidata nuova attività.
3. Nel campo **Tipo di attività** selezionare **Modifica password account (solo Linux)**.

4. Selezionare una delle seguenti opzioni:

- **Assegna attività a un gruppo di amministrazione**

  L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

  Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

- **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**

  È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

  Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

- **Assegna attività a una selezione dispositivi**

  L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

  Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

L'attività *Modifica password account (solo Linux)* viene creata per i dispositivi specificati. Se è stata selezionata l'opzione **Assegna attività a un gruppo di amministrazione**, si tratta di un'attività di gruppo.

5. Nel passaggio **Ambito dell'attività**, specificare un gruppo di amministrazione, dispositivi con indirizzi IP specifici o una selezione di dispositivi.

   Le impostazioni disponibili dipendono dall'opzione selezionata nel passaggio precedente.

6. Al passaggio **Inserire il nome e la nuova password dell'account**, specificare le seguenti impostazioni:

   - Nel campo **Nome account** specificare il nome dell'account per il quale si desidera modificare la password.
   - Nel campo **Nuova password** specificare la password che verrà impostata per l'account specificato nel campo precedente.

     Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.
   - Se necessario, selezionare la casella di controllo **Imposta come password monouso (l'utente deve modificare la password dopo il primo accesso)**.

     - Imposta come password monouso (l'utente deve modificare la password dopo il primo accesso)

       Se questa casella di controllo è selezionata, all'utente verrà richiesto di impostare una nuova password dopo il primo accesso.

       Se questa casella di controllo è deselezionata, all'utente non verrà richiesto di impostare una nuova password dopo il primo accesso.

       Per impostazione predefinita, questa casella di controllo è deselezionata.

7. Nel passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

   Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata la finestra delle impostazioni dell'attività. In questa finestra, è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio delle attività, se necessario.

8. Nell'elenco delle attività, selezionare l'attività creata, quindi fare clic su **Avvia**.

   In alternativa, attendere l'avvio dell'attività in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di modifica della password dell'account, la password viene modificata per l'account locale specificato nei dispositivi specificati.

Per garantire il corretto funzionamento delle attività di modifica della password dell'account, SELinux deve essere disabilitato nel dispositivo dell'utente.

Revoca dei diritti di amministratore locale

È possibile revocare i diritti di amministratore locale dagli account. Ciò fornisce un ulteriore livello di controllo degli account utente. Ad esempio, è possibile revocare i diritti di amministratore locale al termine di un'assegnazione una tantum.

Quando questa attività viene eseguita, l'account locale specificato viene controllato per vedere se appartiene a gruppi di amministratori locali. Questi gruppi sono definiti nelle impostazioni del criterio di Network Agent. È possibile personalizzare l'elenco dei gruppi di amministratori locali nelle impostazioni dei criteri di Network Agent. È inoltre possibile controllare l'elenco degli account utente privilegiati utilizzando il **Rapporto sugli utenti dei dispositivi (solo Linux)**.

Questa attività può essere eseguita solo nei dispositivi Linux.

Per revocare i diritti di amministratore locale su dispositivi specifici:

1. Nel menu principale, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Nel campo **Tipo di attività** selezionare **Revoca diritti di amministratore locale (solo Linux)**.
4. Selezionare una delle seguenti opzioni:

   - **Assegna attività a un gruppo di amministrazione**

     L'attività viene assegnata ai dispositivi inclusi in un gruppo di amministrazione. È possibile specificare uno dei gruppi esistenti o crearne uno nuovo.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività di invio di un messaggio agli utenti se il messaggio è specifico per i dispositivi inclusi in un determinato gruppo di amministrazione.

     Se un'attività è assegnata a un gruppo di amministrazione, la scheda **Sicurezza** non viene visualizzata nella finestra delle proprietà dell'attività perché le attività di gruppo sono soggette alle impostazioni di protezione dei gruppi ai quali si applicano.

   - **Specifica gli indirizzi dei dispositivi manualmente o importa gli indirizzi da un elenco**

     È possibile specificare nomi NetBIOS, nomi DNS, indirizzi IP e subnet IP dei dispositivi a cui si desidera assegnare l'attività.

     Questa opzione può essere utilizzata per eseguire un'attività per una subnet specifica. È ad esempio possibile installare una determinata applicazione nei dispositivi degli addetti alla contabilità o eseguire la scansione dei dispositivi in una subnet potenzialmente infetta.

   - **Assegna attività a una selezione dispositivi**

     L'attività viene assegnata ai dispositivi inclusi in una selezione dispositivi. È possibile specificare una delle selezioni esistenti.

     Questa opzione può ad esempio essere utilizzata per eseguire un'attività nei dispositivi con una versione specifica del sistema operativo.

   L'attività *Revoca diritti di amministratore locale (solo Linux)* viene creata per i dispositivi specificati. Se è stata selezionata l'opzione **Assegna attività a un gruppo di amministrazione**, si tratta di un'attività di gruppo.
5. Nel passaggio **Ambito dell'attività**, specificare un gruppo di amministrazione, dispositivi con indirizzi IP specifici o una selezione di dispositivi.

   Le impostazioni disponibili dipendono dall'opzione selezionata nel passaggio precedente.

6. A questo punto della procedura guidata, specificare le seguenti impostazioni:

   - Nel gruppo impostazioni **Modalità operativa** specificare la modalità operativa:

     - **Revoca i diritti di amministratore locale dagli account elencati**

       Se questa opzione è selezionata, i diritti di amministratore locale verranno revocati dagli account locali specificati.

       Per impostazione predefinita, questa opzione è selezionata.

     - **Escludi gli account elencati dalla revoca dei diritti di amministratore locale**

       Se questa opzione è selezionata, i diritti di amministratore locale verranno revocati a tutti gli account locali, ad eccezione di quelli specificati.

       Per impostazione predefinita, questa opzione non è selezionata.

   - Specificare gli account locali:

     - Fare clic su **Aggiungi**.

     - Nella finestra visualizzata, procedere come segue:

       - Nel campo **Nome account**, specificare il nome dell'account locale.

       - Nel gruppo impostazioni **Azione account** (disponibile solo se l'opzione **Revoca i diritti di amministratore locale dagli account elencati** è selezionata), selezionare l'azione.

       - **Mantieni account**

         Se questa opzione è selezionata, l'account locale non viene eliminato dopo la revoca dei diritti di amministratore locale.

         Per impostazione predefinita, questa opzione è selezionata.

       - **Elimina account**

         Se questa opzione è selezionata, l'account locale verrà eliminato indipendentemente dal fatto che disponga dei diritti di amministratore locale.

         Per impostazione predefinita, questa opzione non è selezionata.

7. Nel passaggio **Completare la creazione dell'attività**, fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

   Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata la finestra delle impostazioni dell'attività. In questa finestra, è possibile controllare i parametri dell'attività, modificarli o configurare una pianificazione di avvio delle attività, se necessario.

8. Nell'elenco delle attività, selezionare l'attività creata, quindi fare clic su **Avvia**.

   In alternativa, attendere l'avvio dell'attività in base alla pianificazione specificata nelle impostazioni dell'attività.

Al termine dell'attività di revoca dei diritti di amministratore locale, i diritti di amministratore locale vengono revocati dagli account locali specificati nei dispositivi specificati.

Gestione delle revisioni degli oggetti

Questa sezione contiene informazioni sulla gestione delle revisioni degli oggetti. Kaspersky Security Center consente di tenere traccia delle modifiche apportate agli oggetti. Ogni volta che si salvano le modifiche apportate a un oggetto, viene creata una *revisione*. Ogni revisione ha un numero.

Gli oggetti delle applicazioni che supportano la gestione delle revisioni includono:

- Proprietà di Administration Server
- Criteri
- Attività
- Gruppi di amministrazione
- Account utente
- Pacchetti di installazione

È possibile eseguire le seguenti azioni sulle revisioni degli oggetti:

- Visualizzare una revisione selezionata (disponibile solo per i criteri)
- Eseguire il rollback delle modifiche apportate a un oggetto a una revisione selezionata
- Salva le revisioni come file JSON (disponibile solo per i criteri)

Nella finestra delle proprietà di un oggetto che supporta la gestione delle revisioni, la sezione **Cronologia revisioni** visualizza un elenco delle revisioni degli oggetti con i seguenti dettagli:

- **Revisione**—Numero di revisione dell'oggetto.
- **Data/ora**—Data e ora di modifica dell'oggetto.
- **Utente**—Nome dell'utente che ha modificato l'oggetto.
- **Indirizzo IP dispositivo utente**—indirizzo IP del dispositivo da cui è stato modificato l'oggetto.
- **Indirizzo IP Web Console**—indirizzo IP di Kaspersky Security Center Web Console con cui è stato modificato l'oggetto.
- **Azione**—Azione eseguita sull'oggetto.
- **Descrizione**—Descrizione della revisione relativa alla modifica apportata alle impostazioni dell'oggetto.

  Per impostazione predefinita, la descrizione della revisione dell'oggetto è vuota. Per aggiungere una descrizione a una revisione, selezionare la revisione desiderata, quindi fare clic sul pulsante **Modifica descrizione**. Nella finestra aperta, immettere il testo relativo alla descrizione della revisione.

Rollback di un oggetto a una revisione precedente

È possibile eseguire il rollback delle modifiche apportate a un oggetto, se necessario. Potrebbe ad esempio essere necessario ripristinare lo stato delle impostazioni di un criterio in una data specifica.

Per eseguire il rollback delle modifiche apportate a un oggetto:

1. Nella finestra delle proprietà dell'oggetto aprire la scheda **Cronologia revisioni**.
2. Nell'elenco delle revisioni dell'oggetto selezionare la revisione per la quale si desidera eseguire il rollback delle modifiche.
3. Fare clic sul pulsante **Rollback**.
4. Fare clic su **OK** per confermare l'operazione.

   Verrà eseguito il rollback dell'oggetto alla revisione selezionata. L'elenco delle revisioni dell'oggetto visualizza un record dell'azione eseguita. La descrizione della revisione indica il numero della revisione a cui è stato riportato l'oggetto.

L'operazione di rollback è disponibile solo per gli oggetti delle attività e dei criteri.

Aggiunta di una descrizione della revisione

Kaspersky Security Center consente di tenere traccia delle modifiche apportate agli oggetti. Ogni volta che si salvano le modifiche apportate a un oggetto, viene creata una revisione. Ogni revisione ha un numero.

È possibile aggiungere una descrizione per la revisione, in modo da semplificare la ricerca delle revisioni nell'elenco.

Per aggiungere una descrizione per una revisione:

1. Nella finestra delle proprietà dell'oggetto aprire la scheda **Cronologia revisioni**.
2. Nell'elenco delle revisioni di un oggetto selezionare la revisione per cui è necessario aggiungere una descrizione.
3. Fare clic sul pulsante **Modifica descrizione**.

   Verrà visualizzata la finestra **Descrizione**.
4. Nella finestra **Descrizione** immettere il testo relativo alla descrizione della revisione.

   Per impostazione predefinita, la descrizione della revisione dell'oggetto è vuota.
5. Salvare la descrizione della revisione.

Viene aggiunta la descrizione per la revisione dell'oggetto.

Visualizzazione e salvataggio della revisione di un criterio

Kaspersky Security Center consente di visualizzare quali modifiche sono state apportate a un criterio in un determinato periodo, nonché di salvare le informazioni su tali modifiche in un file.

La visualizzazione e il salvataggio di una revisione del criterio sono disponibili se il plug-in Web di gestione corrispondente supporta questa funzionalità.

Per visualizzare una revisione dei criteri:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio per la revisione che si desidera visualizzare, quindi andare alla sezione **Cronologia revisioni**.
3. Nell'elenco delle revisioni dei criteri fare clic sul numero della revisione che si desidera visualizzare.

   Se la dimensione della revisione è superiore a 10 MB, non sarà possibile visualizzarla utilizzando Kaspersky Security Center Web Console. Verrà richiesto di salvare la revisione selezionata in un file JSON.

   Se la dimensione della revisione non supera i 10 MB, viene visualizzato un rapporto in formato HTML con le impostazioni della revisione del criterio selezionata. Poiché il rapporto viene visualizzato in una finestra popup, verificare che i popup siano consentiti nel browser.

Per salvare la revisione di un criterio in un file JSON:

Nell'elenco delle revisioni dei criteri selezionare la revisione che si desidera salvare, quindi fare clic su **Salva su file**.

La revisione viene salvata in un file JSON.

Eliminazione di oggetti

Questa sezione fornisce informazioni sull'eliminazione degli oggetti.

È possibile eliminare oggetti come:

- Criteri
- Attività
- Pacchetti di installazione
- Administration Server virtuali
- Utenti
- Gruppi di protezione
- Gruppi di amministrazione

Per eliminare un oggetto:

1. Aprire la sezione richiesta di Kaspersky Security Center Web Console, quindi selezionare l'oggetto.
2. Nella barra degli strumenti, fare clic sul pulsante **Elimina**.
3. Nella finestra visualizzata fare clic su **OK** per confermare la selezione.

L'oggetto selezionato verrà eliminato.

Quando si elimina un oggetto, le relative informazioni rimangono nel database. Il periodo di archiviazione per le informazioni sugli oggetti eliminati corrisponde al periodo di archiviazione per le revisioni degli oggetti (il periodo consigliato è di 90 giorni). È possibile modificare il periodo di archiviazione solo se si dispone dell'autorizzazione **Modifica** nell'area dei diritti **Oggetti eliminati**.

Informazioni sull'eliminazione dei dispositivi client

Quando si elimina un dispositivo gestito da un gruppo di amministrazione, l'applicazione sposta il dispositivo nel gruppo Dispositivi non assegnati. Dopo l'eliminazione del dispositivo, le applicazioni Kaspersky installate, Network Agent e qualsiasi applicazione di protezione, ad esempio Kaspersky Endpoint Security, rimangono nel dispositivo.

Kaspersky Security Center gestisce i dispositivi nel gruppo Dispositivi non assegnati in base alle seguenti regole:

- Se sono state configurate regole di spostamento dei dispositivi e un dispositivo soddisfa i criteri di una regola di spostamento, il dispositivo viene spostato automaticamente in un gruppo di amministrazione in base alla regola.

- Il dispositivo viene archiviato nel gruppo Dispositivi non assegnati e rimosso automaticamente dal gruppo in base alle regole di conservazione dei dispositivi.

  Le regole di conservazione dei dispositivi non influiscono sui dispositivi con una o più unità criptate con Criptaggio dell'intero disco. Tali dispositivi non vengono eliminati automaticamente; è possibile eliminarli solo manualmente. Se è necessario eliminare un dispositivo con un'unità criptata, decriptare prima l'unità, quindi eliminare il dispositivo.

  > Quando si elimina un dispositivo con un'unità criptata, vengono eliminati anche i dati necessari per decriptare l'unità. Se si seleziona la casella di controllo **Comprendo il rischio e desidero eliminare i dispositivi selezionati** nella finestra di conferma che si apre quando si eliminano tali dispositivi (dal gruppo **Dispositivi non assegnati** o **Dispositivi gestiti**), significa che si è a conoscenza della successiva eliminazione dei dati.

  Per decriptare l'unità, devono essere soddisfatte le seguenti condizioni:

  - Il dispositivo viene riconnesso ad Administration Server al fine di ripristinare i dati necessari per decriptare l'unità.
  - L'utente del dispositivo ricorda la password di decriptaggio.
  - L'applicazione di protezione utilizzata per criptare l'unità, ad esempio Kaspersky Endpoint Security for Windows, è ancora installata nel dispositivo.

  Se l'unità è stata criptata con la tecnologia Criptaggio disco Kaspersky, è inoltre possibile provare a recuperare i dati utilizzando l'utilità di ripristino FDERT.

> In VDI, se si dispone di un dispositivo con unità criptate, le informazioni nell'unità criptata vengono eliminate dopo l'eliminazione del dispositivo.

Quando si elimina manualmente un dispositivo dal gruppo Dispositivi non assegnati, l'applicazione rimuove il dispositivo dall'elenco. Dopo l'eliminazione del dispositivo, le eventuali applicazioni Kaspersky installate rimangono nel dispositivo. Quindi, se il dispositivo è ancora visibile in Administration Server ed è stato configurato il polling di rete periodico, Kaspersky Security Center rileva il dispositivo durante il polling di rete e lo aggiunge nuovamente al gruppo Dispositivi non assegnati. Pertanto, è ragionevole eliminare manualmente un dispositivo solo se il dispositivo è invisibile ad Administration Server.

Finestra Kaspersky Security Network (KSN)

In questa sezione viene descritto come utilizzare un'infrastruttura di servizi online denominata Kaspersky Security Network (KSN). Vengono fornite informazioni dettagliate su KSN e istruzioni su come abilitare KSN, configurare l'accesso a KSN e visualizzare le statistiche di utilizzo del server proxy KSN.

> Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Informazioni su KSN

Kaspersky Security Network (KSN) è un'infrastruttura di servizi online che consente di accedere alla Knowledge Base di Kaspersky, in cui sono disponibili informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora l'efficacia di alcuni componenti della protezione e riduce il rischio di falsi positivi. KSN consente di utilizzare i database di reputazione di Kaspersky per recuperare informazioni sulle applicazioni installate nei dispositivi gestiti.

Kaspersky Security Center supporta le seguenti soluzioni di infrastruttura:

- *KSN* è una soluzione che consente di scambiare informazioni con Kaspersky Security Network. Se si partecipa a KSN, si autorizza l'invio automatico a Kaspersky di informazioni sul funzionamento delle applicazioni Kaspersky installate nei dispositivi client gestiti tramite Kaspersky Security Center. Le informazioni vengono trasferite in base alle impostazioni di accesso a KSN correnti. Gli analisti di Kaspersky analizzano inoltre le informazioni ricevute e le includono nei database statistici e di reputazione di Kaspersky Security Network. Kaspersky Security Center utilizza questa soluzione per impostazione predefinita.

- *Kaspersky Private Security Network (KPSN)* è una soluzione che consente agli utenti di dispositivi con applicazioni Kaspersky installate di ottenere l'accesso ai database di reputazione di Kaspersky Security Network e ad altri dati statistici, senza inviare dati a KSN Globale dai propri dispositivi. KPSN è progettato per i clienti aziendali che non sono in grado di partecipare al programma Kaspersky Security Network per uno dei seguenti motivi:

  - I dispositivi dell'utente non sono connessi a Internet.

  - La trasmissione dei dati all'esterno del paese o all'esterno della rete LAN aziendale è vietata dalla legge o limitata dai criteri di protezione aziendali.

  È possibile configurare le impostazioni di accesso di Kaspersky Private Security Network nella sezione **Impostazioni proxy KSN** della finestra delle proprietà di Administration Server.

All'utente verrà richiesto di partecipare a KSN durante l'esecuzione dell'Avvio rapido guidato. È possibile iniziare o smettere di utilizzare KSN in qualsiasi momento durante l'utilizzo dell'applicazione.

È necessario utilizzare KSN in conformità con l'Informativa KSN letta e accettata durante l'attivazione di KSN. Se l'Informativa KSN viene aggiornata, viene visualizzata quando si esegue l'upgrade di una versione di Administration Server. È possibile accettare o rifiutare l'Informativa KSN aggiornata. In caso di rifiuto, si continuerà a utilizzare KSN in conformità con la versione precedente dell'Informativa KSN già accettata.

Quando KSN è abilitato, Kaspersky Security Center verifica se i server KSN sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. Ciò è necessario per garantire il mantenimento del livello di sicurezza per i dispositivi gestiti.

I dispositivi client gestiti da Administration Server interagiscono con KSN attraverso il server proxy KSN. Il server proxy KSN fornisce le seguenti funzionalità:

- I dispositivi client possono inviare richieste a KSN, ottenere informazioni da KSN e trasferire informazioni a KSN anche se non hanno accesso diretto a Internet.

- Il server proxy KSN memorizza nella cache i dati elaborati, riducendo in tal modo il carico sul canale in uscita e il tempo di attesa per ottenere le informazioni richieste da un dispositivo client.

È possibile configurare il server proxy KSN nella sezione **Impostazioni proxy KSN** della finestra delle proprietà di Administration Server.

Impostazione dell'accesso a KSN

È possibile configurare l'accesso a Kaspersky Security Network (KSN) in Administration Server e in un punto di distribuzione.

Per impostare l'accesso di Administration Server a KSN:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.

3. Spostare l'interruttore sulla posizione **Abilita proxy KSN in Administration Server Abilitato**.

   Se questa opzione è abilitata, il server proxy KSN invia i dati a KSN per aumentare l'efficienza dei componenti di Kaspersky Security Center e migliorare le prestazioni delle applicazioni Kaspersky. I dati vengono inviati dai dispositivi client a KSN in conformità con il criterio di Kaspersky Endpoint Security attivo in tali dispositivi client. Se l'interruttore è disabilitato, non verranno inviati dati a KSN da Administration Server e dai dispositivi client tramite Kaspersky Security Center. I dispositivi client possono comunque inviare dati a KSN direttamente (ignorando Kaspersky Security Center), in base alle relative impostazioni. Il criterio di Kaspersky Endpoint Security attivo nei dispositivi client determina quali dati saranno inviati a KSN direttamente (ignorando Kaspersky Security Center) da tali dispositivi.

4. Impostare l'interruttore sulla posizione **Usa Kaspersky Security Network Abilitato**.

   Se questa opzione è abilitata, i dispositivi client invieranno i risultati dell'installazione delle patch a Kaspersky. Quando si abilita questa opzione, leggere e accettare le condizioni dell'informativa KSN.

   Se si utilizza KPSN, spostare l'interruttore sulla posizione **Usa Kaspersky Private Security Network Abilitato** e fare clic sul pulsante **Seleziona il file con le impostazioni del proxy KSN** per scaricare le impostazioni di KPSN (file con estensioni pkcs7 e pem). Una volta scaricate le impostazioni, l'interfaccia mostra il nome e i contatti del provider, nonché la data di creazione del file con le impostazioni di KPSN.

   > Quando si abilita KPSN, prestare attenzione ai punti di distribuzione configurati per l'invio di richieste KSN direttamente a KSN Cloud. I punti di distribuzione in cui è installato Network Agent versione 11 (o precedente) continueranno a inviare richieste KSN a KSN Cloud. Per riconfigurare i punti di distribuzione per l'invio di richieste KSN a KPSN, abilitare l'opzione **Inoltra richieste KSN ad Administration Server** per ciascun punto di distribuzione. È possibile abilitare questa opzione nelle proprietà del punto di distribuzione o nel criterio di Network Agent.

   Quando si sposta l'interruttore sulla posizione **Usa Kaspersky Private Security Network Abilitato**, viene visualizzato un messaggio con informazioni dettagliate su KPSN.

   Le seguenti applicazioni Kaspersky supportano KPSN:

   - Kaspersky Security Center
   - Kaspersky Endpoint Security for Windows
   - Kaspersky Endpoint Security for Linux
   - Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2
   - Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent

   Se si abilita KPSN in Kaspersky Security Center, tali applicazioni ricevono informazioni sul supporto di KPSN Privato. Nella finestra delle impostazioni dell'applicazione, nella sottosezione **Kaspersky Security Network** della sezione **Protezione Minacce Avanzata**, vengono visualizzate le informazioni sul provider KSN selezionato: KSN o KPSN.

   > Se si utilizzano versioni delle applicazioni precedenti a Kaspersky Security for Virtualization 3.0 Agentless Service Pack 2 oppure a Kaspersky Security for Virtualization 3.0 Service Pack 1 Light Agent durante l'esecuzione di KPSN, è consigliabile utilizzare Administration Server secondari per cui l'utilizzo di KPSN Privato non è stato abilitato.

   > Kaspersky Security Center non invia dati statistici a Kaspersky Security Network se KPSN è configurato nella sezione **Impostazioni proxy KSN** della finestra delle proprietà di Administration Server.

5. Se sono state configurate le impostazioni del server proxy nelle proprietà di Administration Server, ma l'architettura di rete richiede di utilizzare direttamente KPSN, abilitare l'opzione **Ignora impostazioni del server proxy durante la connessione a KPSN**. In caso contrario, le richieste dalle applicazioni gestite non possono raggiungere KPSN.

6. Configurare la connessione di Administration Server al servizio proxy KSN:

   - In **Impostazioni di connessione**, per **Porta TCP** specificare il numero della porta TCP che verrà utilizzata per la connessione al server proxy KSN. La porta predefinita per la connessione al server proxy KSN è la 13111.
   - Se si desidera che Administration Server si connetta al server proxy KSN attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** port e specificare il numero della porta in **Porta UDP**. Per impostazione predefinita, questa opzione è disabilitata e viene utilizzata la porta TCP. Se l'opzione è attivata, la porta UDP predefinita per la connessione al server KSN Proxy è 15111.
   - Se si desidera che Administration Server si connetta al server proxy KSN attraverso una porta HTTPS, abilitare l'opzione **Usa HTTPS** e specificare il numero della porta in **HTTPS tramite porta**. Per impostazione predefinita, questa opzione è disabilitata e viene utilizzata la porta TCP. Se l'opzione è attivata, la porta HTTPS predefinita per la connessione al server KSN Proxy è 17111.

7. Impostare l'interruttore sulla posizione **Connetti Administration Server secondari a KSN tramite l'Administration Server primario Abilitato**

   Se questa opzione è abilitata, gli Administration Server secondari utilizzano l'Administration Server primario come server proxy KSN. Se questa opzione è disabilitata, gli Administration Server secondari si connettono a KSN autonomamente. In questo caso, i dispositivi gestiti utilizzano gli Administration Server secondari come server proxy KSN.

   > Gli Administration Server secondari utilizzano l'Administration Server primario come server proxy se nel riquadro destro della sezione **Impostazioni proxy KSN** nelle proprietà degli Administration Server secondari l'interruttore è sulla posizione **Abilita proxy KSN in Administration Server Abilitato**.

8. Fare clic sul pulsante **Salva**.

Le impostazioni di accesso a KSN verranno salvate.

È inoltre possibile impostare l'accesso del punto di distribuzione a KSN, ad esempio se si desidera ridurre il carico sull'Administration Server. Il punto di distribuzione che opera come server proxy KSN invia richieste KSN direttamente dai dispositivi gestiti a Kaspersky, senza utilizzare l'Administration Server.

Per configurare l'accesso del punto di distribuzione a Kaspersky Security Network (KSN):

1. Accertarsi che il punto di distribuzione sia assegnato manualmente.
2. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

3. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.
4. Fare clic sul nome del punto di distribuzione per aprire la relativa finestra delle proprietà.
5. Nella finestra delle proprietà del punto di distribuzione, nella sezione **Proxy KSN** abilitare l'opzione **Abilita proxy KSN da parte del punto di distribuzione**, quindi abilitare l'opzione **Accedi a KSN Cloud/KPSN direttamente tramite Internet**.
6. Fare clic su **OK**.

Il punto di distribuzione opererà come un server proxy KSN.

Abilitazione e disabilitazione dell'utilizzo di KSN

Per abilitare l'utilizzo di KSN:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.

3. Spostare l'interruttore sulla posizione **Abilita proxy KSN in Administration Server Abilitato**.

Il server proxy KSN è abilitato e invia i dati a KSN per aumentare l'efficienza dei componenti di Kaspersky Security Center e migliorare le prestazioni delle applicazioni Kaspersky.

1. A seconda della soluzione di infrastruttura KSN in uso, abilitare gli interruttori corrispondenti.

   - Se si utilizza KSN Globale, spostare l'interruttore sulla posizione **Usa Kaspersky Security Network Abilitato**.

     L'invio dei dati a KSN è ora disponibile. Quando si abilita questa opzione, è necessario leggere e accettare le condizioni dell'Informativa KSN.

   - Se si utilizza KPSN, spostare l'interruttore sulla posizione **Usa Kaspersky Private Security Network Abilitato**, quindi fare clic sul pulsante **Seleziona il file con le impostazioni del proxy KSN** per scaricare le impostazioni di KPSN (file con estensioni pkcs7 e pem). Una volta scaricate le impostazioni, l'interfaccia mostra il nome e i contatti del provider, nonché la data di creazione del file con le impostazioni di KPSN.

     Quando si sposta l'interruttore sulla posizione **Usa Kaspersky Private Security Network Abilitato**, viene visualizzato un messaggio con informazioni dettagliate su KPSN.

2. Fare clic sul pulsante **Salva**.

Per disabilitare l'utilizzo di KSN:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.

3. Spostare l'interruttore sulla posizione **Abilita proxy KSN in Administration Server Disabilitato** per disabilitare il servizio proxy KSN.

4. Fare clic sul pulsante **Salva**.

Visualizzazione dell'Informativa KSN accettata

Quando si abilita Kaspersky Security Network (KSN), è necessario leggere e accettare l'Informativa KSN. È possibile visualizzare l'Informativa KSN accettata in qualsiasi momento.

Per visualizzare l'Informativa KSN accettata:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.

3. Fare clic sul collegamento **Visualizza l'Informativa di Kaspersky Security Network**.

Nella finestra visualizzata è possibile visualizzare il testo dell'Informativa KSN accettata.

Accettazione di un'Informativa KSN aggiornata

È necessario utilizzare KSN in conformità con l'Informativa KSN letta e accettata durante l'attivazione di KSN. Se l'Informativa KSN viene aggiornata, viene visualizzata quando si esegue l'upgrade di una versione di Administration Server. È possibile accettare o rifiutare l'Informativa KSN aggiornata. In caso di rifiuto, si continuerà a utilizzare KSN in conformità con la versione dell'Informativa KSN accettata precedentemente.

Dopo l'upgrade di una versione di Administration Server, l'Informativa KSN aggiornata viene visualizzata automaticamente. Se si rifiuta l'Informativa KSN aggiornata, è comunque possibile visualizzarla e accettarla in un secondo momento.

Per visualizzare e successivamente accettare o rifiutare un'Informativa KSN aggiornata:

1. Fare clic sul collegamento **Visualizza notifiche** nell'angolo superiore destro della finestra principale dell'applicazione.

   Verrà visualizzata la finestra **Notifiche**.

2. Fare clic sul collegamento **Visualizza l'Informativa KSN aggiornata**.

   Verrà visualizzata la finestra **Aggiornamento dell'Informativa di Kaspersky Security Network**.

3. Leggere l'Informativa KSN, quindi prendere una decisione facendo clic su uno dei seguenti pulsanti:

   - **Accetto l'Informativa KSN aggiornata**
   - **Usa KSN con l'Informativa precedente**

A seconda della scelta, KSN continuerà a funzionare in conformità con i termini dell'Informativa KSN corrente o aggiornata. È possibile visualizzare il testo dell'Informativa KSN accettata nelle proprietà di Administration Server in qualsiasi momento.

Verifica per stabilire se il punto di distribuzione funziona come server proxy KSN

In un dispositivo gestito a cui è assegnato il ruolo di punto di distribuzione è possibile abilitare il server proxy KSN. Un dispositivo gestito funziona come server proxy KSN quando il servizio ksnproxy è in esecuzione nel dispositivo. È possibile controllare, attivare o disattivare questo servizio nel dispositivo in locale.

È possibile assegnare un dispositivo basato su Windows o Linux come punto di distribuzione. Il metodo di controllo del punto di distribuzione dipende dal sistema operativo di questo punto di distribuzione.

Per verificare se il punto di distribuzione basato su Windows funziona come server proxy KSN:

1. Nel dispositivo del punto di distribuzione, in Windows, aprire **Servizi** (**Tutti i programmi** → **Strumenti di amministrazione** → **Servizi**).

2. Nell'elenco dei servizi verificare se il servizio ksnproxy è in esecuzione.

   Se il servizio ksnproxy è in esecuzione, Network Agent nel dispositivo partecipa a Kaspersky Security Network e funziona come server proxy KSN per i dispositivi gestiti inclusi nell'ambito del punto di distribuzione.

Se si desidera, è possibile disattivare il servizio ksnproxy. In questo caso Network Agent nel punto di distribuzione interrompe la partecipazione a Kaspersky Security Network. Sono necessari i diritti di amministratore locale.

Per verificare se il punto di distribuzione basato su Linux funziona come server proxy KSN:

1. Nel dispositivo del punto di distribuzione, visualizzare l'elenco dei processi in esecuzione.

2. Nell'elenco dei processi in esecuzione, controllare se il processo `/opt/kaspersky/ksc64/sbin/ksnproxy` è in esecuzione.

Se il processo `/opt/kaspersky/ksc64/sbin/ksnproxy` è in esecuzione, Network Agent nel dispositivo partecipa a Kaspersky Security Network e funziona come server proxy KSN per i dispositivi gestiti inclusi nell'ambito del punto di distribuzione.

Scenario: Upgrade di Kaspersky Security Center e delle applicazioni di protezione gestite

In questa sezione viene illustrato brevemente lo scenario principale per l'upgrade di Kaspersky Security Center e delle applicazioni di protezione gestite.

L'upgrade di Kaspersky Security Center e delle applicazioni di protezione gestite prevedono diversi passaggi:

1. **Verifica dei requisiti hardware e software**

   Verificare che l'hardware soddisfi i requisiti e installare gli aggiornamenti richiesti.

2. **Pianificazione delle risorse**

   Valutare quanto spazio su disco è occupato dal database. Verificare di disporre di spazio su disco sufficiente per archiviare la copia di backup delle impostazioni di Administration Server e del database.

3. **Come ottenere il file del programma di installazione per Kaspersky Security Center**

   Recuperare il file eseguibile per la versione corrente di Kaspersky Security Center e salvarlo nel dispositivo che opererà come Administration Server. Leggere le note sulla release della versione di Kaspersky Security Center che si desidera utilizzare.

4. **Creazione di una copia di backup della versione precedente**

   Utilizzare l'utilità di backup e ripristino dei dati per creare una copia di backup dei dati di Administration Server. È inoltre possibile creare un'attività di backup.

   Si consiglia di esportare l'elenco dei plug-in installati.

5. **Esecuzione del programma di installazione**

Avviare il file eseguibile per la versione più recente di Kaspersky Security Center. Quando si esegue il file, specificare che si dispone di una copia di backup e indicarne la posizione. I dati verranno ripristinati dal backup.

6. **Upgrade delle applicazioni gestite**

   È possibile eseguire l'upgrade dell'applicazione se è disponibile una versione più recente. Leggere l'elenco delle applicazioni Kaspersky supportate e verificare che la versione di Kaspersky Security Center in uso sia compatibile con questa applicazione. Eseguire quindi l'upgrade dell'applicazione come descritto nelle relative note sulla release.

Risultati

Al completamento dello scenario di upgrade, verificare che la nuova versione di Administration Server sia installata correttamente in Microsoft Management Console. Fare clic su **Guida** → **Informazioni su Kaspersky Security Center**. Verrà visualizzata la versione.

Per verificare che sia in uso la nuova versione di Administration Server in Kaspersky Security Center Web Console, nella parte superiore dello schermo, fare clic sull'icona delle impostazioni ( ) accanto al nome di Administration Server. Nella finestra delle proprietà di Administration Server visualizzata, nella scheda **Generale**, selezionare la sezione **Generale**. Verrà visualizzata la versione.

Se è necessario, ripristinare i dati di Administration Server, attenersi alla procedura descritta nell'argomento seguente: Backup e ripristino dei dati in modalità interattiva.

Se è stato eseguito l'upgrade di un'applicazione di protezione gestita, verificare che sia installata correttamente nei dispositivi gestiti. Per ulteriori informazioni, consultare la documentazione dell'applicazione.

Aggiornamento di database e applicazioni Kaspersky

Questa sezione descrive i passaggi da eseguire per aggiornare periodicamente i seguenti elementi:

- Database e moduli del software Kaspersky
- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center e le applicazioni di protezione

Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Scenario: Aggiornamento periodico di database e applicazioni Kaspersky

Questa sezione fornisce uno scenario per l'aggiornamento periodico dei database, dei moduli software e delle applicazioni Kaspersky. Dopo aver completato lo scenario Configurazione della protezione di rete, è necessario mantenere l'affidabilità del sistema di protezione per assicurarsi che gli Administration Server e i dispositivi gestiti siano protetti da varie minacce, inclusi virus, attacchi di rete e attacchi di phishing.

La protezione della rete viene mantenuta aggiornata tramite aggiornamenti periodici dei seguenti elementi:

- Database e moduli del software Kaspersky
- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center e le applicazioni di protezione

Completando questo scenario, è possibile avere la certezza di quanto segue:

- La rete è protetta dal software Kaspersky più recente, inclusi i componenti di Kaspersky Security Center e le applicazioni di protezione.
- I database anti-virus e gli altri database Kaspersky di importanza critica per la sicurezza della rete sono sempre aggiornati.

Prerequisiti

I dispositivi gestiti devono disporre di una connessione ad Administration Server. Se non dispongono di una connessione, valutare se eseguire l'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky manualmente o direttamente dai server degli aggiornamenti Kaspersky.

Administration Server deve disporre di una connessione a Internet.

Prima di iniziare, verificare di avere:

1. Distribuito le applicazioni di protezione Kaspersky nei dispositivi gestiti in base allo scenario di distribuzione delle applicazioni Kaspersky tramite Kaspersky Security Center Web Console.
2. Creato e configurato tutti i criteri, i profili criterio e le attività richiesti in base allo scenario di configurazione della protezione di rete.
3. Assegnato un numero appropriato di punti di distribuzione in base al numero di dispositivi gestiti e alla topologia della rete.

L'aggiornamento dei database e delle applicazioni Kaspersky prevede diversi passaggi:

1. **Scelta di uno schema di aggiornamento**

   Esistono diversi schemi che è possibile utilizzare per installare gli aggiornamenti dei componenti di Kaspersky Security Center e delle applicazioni di protezione. Scegliere lo schema o gli schemi più appropriati per i requisiti della rete.

2. **Creazione dell'attività per il download degli aggiornamenti nell'archivio di Administration Server**

   Questa attività viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. Se la procedura guidata non è stata eseguita, creare l'attività ora.

   Questa attività è necessaria per scaricare gli aggiornamenti dai server di aggiornamento Kaspersky nell'archivio di Administration Server, nonché per aggiornare i database e i moduli software Kaspersky per Kaspersky Security Center. Dopo aver scaricato gli aggiornamenti, questi possono essere propagati ai dispositivi gestiti.

   Se nella rete sono stati assegnati punti di distribuzione, gli aggiornamenti vengono scaricati automaticamente dall'archivio di Administration Server agli archivi dei punti di distribuzione. In questo caso, i dispositivi gestiti inclusi nell'ambito di un punto di distribuzione scaricano gli aggiornamenti dall'archivio del punto di distribuzione anziché dall'archivio di Administration Server.

   Istruzioni dettagliate:

- Administration Console: Creazione dell'attività per il download degli aggiornamenti nell'archivio dell'Administration Server
- Kaspersky Security Center Web Console: Creazione dell'attività per il download degli aggiornamenti nell'archivio dell'Administration Server

3. **Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione (facoltativo)**

   Per impostazione predefinita, gli aggiornamenti vengono scaricati nei punti di distribuzione dall'Administration Server. È possibile configurare Kaspersky Security Center per scaricare gli aggiornamenti nei punti di distribuzione direttamente dai server di aggiornamento Kaspersky. Il download negli archivi dei punti di distribuzione è preferibile se il traffico tra Administration Server e punti di distribuzione è superiore rispetto a quello del traffico tra i punti di distribuzione e i server di aggiornamento Kaspersky oppure se Administration Server non dispone di accesso a Internet.

   Quando nella rete sono stati assegnati punti di distribuzione ed è stata creata l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, i punti di distribuzione scaricano gli aggiornamenti dai server di aggiornamento Kaspersky e non dall'archivio dell'Administration Server.

   Istruzioni dettagliate:

   - Administration Console: Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione
   - Kaspersky Security Center Web Console: Creazione dell'attività per il download degli aggiornamenti negli archivi dei punti di distribuzione

4. **Configurazione dei punti di distribuzione**

   Quando nella rete sono stati assegnati punti di distribuzione, verificare che l'opzione **Distribuisci aggiornamenti** sia abilitata nelle proprietà di tutti i punti di distribuzione richiesti. Quando questa opzione è disabilitata per un punto di distribuzione, i dispositivi inclusi nell'ambito del punto di distribuzione scaricano gli aggiornamenti dall'archivio di Administration Server.

   Se si desidera che i dispositivi gestiti ricevano gli aggiornamenti solo dai punti di distribuzione, abilitare l'opzione **Distribuisci i file solo tramite punti di distribuzione** nel criterio di Network Agent.

5. **Ottimizzazione del processo di aggiornamento utilizzando il modello offline di download degli aggiornamenti o i file diff (facoltativo)**

   È possibile ottimizzare il processo di aggiornamento utilizzando il modello offline di download degli aggiornamenti (abilitato per impostazione predefinita) oppure i file diff. Per ogni segmento di rete, è necessario scegliere quale di queste due funzionalità abilitare, perché non possono funzionare contemporaneamente.

   Quando il modello offline di download degli aggiornamenti è abilitato, Network Agent scarica gli aggiornamenti richiesti nel dispositivo gestito una volta che gli aggiornamenti sono stati scaricati nell'archivio di Administration Server, prima che l'applicazione di protezione li richieda. Questo migliora l'affidabilità del processo di aggiornamento. Per utilizzare questa funzionalità, abilitare l'opzione **Scarica aggiornamenti e database anti-virus da Administration Server anticipatamente (scelta consigliata)** nel criterio di Network Agent.

   Se non si utilizza il modello offline di download degli aggiornamenti, è possibile ottimizzare il traffico tra Administration Server e i dispositivi gestiti tramite i file diff. Quando questa funzionalità è abilitata, Administration Server o un punto di distribuzione scarica file diff anziché interi file di database o moduli software Kaspersky. Un file diff descrive le differenze tra due versioni di un file di un database o un modulo software. Pertanto, un file diff occupa meno spazio di un intero file. Questo comporta una riduzione del traffico tra Administration Server o i punti di distribuzione e i dispositivi gestiti. Per utilizzare questa funzionalità, abilitare l'opzione **Scarica file diff** nelle proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* e/o dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

   Istruzioni dettagliate:

   - Utilizzo dei file diff per l'aggiornamento dei database e dei moduli del software Kaspersky

- Administration Console: Abilitazione e disabilitazione del modello offline per il download degli aggiornamenti
- Kaspersky Security Center Web Console: Abilitazione e disabilitazione del modello offline per il download degli aggiornamenti

6. **Verifica degli aggiornamenti scaricati (facoltativo)**

   Prima di installare gli aggiornamenti scaricati, è possibile verificare gli aggiornamenti tramite l'attività di *Verifica aggiornamenti*. Questa attività esegue in sequenza le attività di aggiornamento dei dispositivi e le attività di scansione malware configurate tramite le impostazioni per il gruppo specificato di dispositivi di test. Una volta ottenuti i risultati delle attività, Administration Server avvia o blocca la propagazione degli aggiornamenti ai dispositivi rimanenti.

   L'attività *Verifica aggiornamenti* può essere eseguita durante l'esecuzione dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Nelle proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* abilitare l'opzione **Verifica gli aggiornamenti prima della distribuzione** in Administration Console o l'opzione **Esegui la verifica degli aggiornamenti** in Kaspersky Security Center Web Console.

   Istruzioni dettagliate:

   - Administration Console: Verifica degli aggiornamenti scaricati
   - Kaspersky Security Center Web Console: Verifica degli aggiornamenti scaricati

7. **Approvazione e rifiuto degli aggiornamenti software**

   Per impostazione predefinita, gli aggiornamenti software scaricati hanno lo stato *Indefinito*. È possibile modificare lo stato in *Approvato* o *Rifiutato*. Gli aggiornamenti approvati vengono sempre installati. Se un aggiornamento richiede la visualizzazione e l'accettazione dei termini del Contratto di licenza con l'utente finale, è prima necessario accettare i termini. Successivamente, l'aggiornamento può essere propagato ai dispositivi gestiti. Gli aggiornamenti indefiniti possono essere installati solo in Network Agent e negli altri componenti di Kaspersky Security Center in conformità con le impostazioni del criterio di Network Agent. Gli aggiornamenti per cui è stato impostato lo stato *Rifiutato* non verranno installati nei dispositivi. Se in precedenza era stato installato un aggiornamento rifiutato per un'applicazione di protezione, Kaspersky Security Center tenterà di disinstallare l'aggiornamento da tutti i dispositivi.

   L'approvazione e il rifiuto degli aggiornamenti sono disponibili solo per Network Agent e le applicazioni Kaspersky gestite installate nei dispositivi client basati su Windows e basatu su Linux. L'aggiornamento continuo di Administration Server, Kaspersky Security Center Web Console e plug-in Web di gestione non è supportato.

   Istruzioni dettagliate:

   - Administration Console: Approvazione e rifiuto degli aggiornamenti software
   - Kaspersky Security Center Web Console: Approvazione e rifiuto degli aggiornamenti software

8. **Configurazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center**

   Gli aggiornamenti scaricati e le patch scaricate per Network Agent e altri componenti di Kaspersky Security Center vengono installati automaticamente. Se l'opzione **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito** è stata mantenuta abilitata nelle proprietà di Network Agent, tutti gli aggiornamenti verranno installati automaticamente dopo essere stati scaricati nell'archivio (o in diversi archivi). Se questa opzione è disabilitata, le patch di Kaspersky che sono state scaricate e contrassegnate con lo stato *Indefinito* saranno installate solo dopo che si modifica il relativo stato in *Approvato*.

   Istruzioni dettagliate:

   - Administration Console: Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center

- Kaspersky Security Center Web Console: Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center

9. **Installazione degli aggiornamenti per Administration Server**

   Gli aggiornamenti software per Administration Server non dipendono dagli stati degli aggiornamenti. Non vengono installati automaticamente e devono prima essere approvati dall'amministratore nella scheda **Monitoraggio** di Administration Console (**Administration Server** `<nome server>` → **Monitoraggio**) o nella sezione **Notifiche** di Kaspersky Security Center Web Console (**Monitoraggio e generazione dei rapporti** → **Notifiche**). Successivamente, l'amministratore deve eseguire esplicitamente l'installazione degli aggiornamenti.

10. **Configurazione dell'installazione automatica degli aggiornamenti per le applicazioni di protezione**

    Creare le *Attività* di aggiornamento per le applicazioni gestite per garantire aggiornamenti tempestivi alle applicazioni, ai moduli software e ai database Kaspersky, inclusi i database anti-virus. Per garantire aggiornamenti tempestivi, è consigliabile selezionare l'opzione **Quando vengono scaricati nuovi aggiornamenti nell'archivio** durante la configurazione della pianificazione dell'attività.

    Se la rete include dispositivi solo IPv6 e si desidera aggiornare regolarmente le applicazioni di protezione installate in tali dispositivi, assicurarsi che Administration Server (versione non precedente alla 13.2) e Network Agent (versione non precedente alla 13.2) siano installati nei dispositivi gestiti.

    Per impostazione predefinita, gli aggiornamenti per Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Security for Linux vengono installati solo dopo aver modificato lo stato degli aggiornamenti in *Approvato*. È possibile modificare le impostazioni di aggiornamento nell'*attività* di aggiornamento.

    Se un aggiornamento richiede la visualizzazione e l'accettazione dei termini del Contratto di licenza con l'utente finale, è prima necessario accettare i termini. Successivamente, l'aggiornamento può essere propagato ai dispositivi gestiti.

    Istruzioni dettagliate:

    - Administration Console: Installazione automatica degli aggiornamenti di Kaspersky Endpoint Security nei dispositivi
    - Kaspersky Security Center Web Console: Installazione automatica degli aggiornamenti di Kaspersky Endpoint Security nei dispositivi

Risultati

Al termine dello scenario, Kaspersky Security Center è configurato per aggiornare i database Kaspersky e le applicazioni Kaspersky installate dopo che gli aggiornamenti vengono scaricati nell'archivio di Administration Server o negli archivi dei punti di distribuzione. È quindi possibile procedere al monitoraggio dello stato della rete.

Informazioni sull'aggiornamento dei database, dei moduli software e delle applicazioni Kaspersky

Per assicurarsi che la protezione dei propri Administration Server e dispositivi gestiti sia aggiornata, è necessario garantire aggiornamenti tempestivi dei seguenti componenti:

- Database e moduli del software Kaspersky

Prima di scaricare i database e i moduli software di Kaspersky, Kaspersky Security Center verifica se i server Kaspersky sono accessibili. Se non è possibile accedere ai server utilizzando il DNS di sistema, l'applicazione utilizza i server DNS pubblici. Ciò è necessario per garantire che i database anti-virus siano aggiornati e per mantenere il livello di sicurezza per i dispositivi gestiti.

- Applicazioni Kaspersky installate, inclusi i componenti di Kaspersky Security Center e le applicazioni di protezione

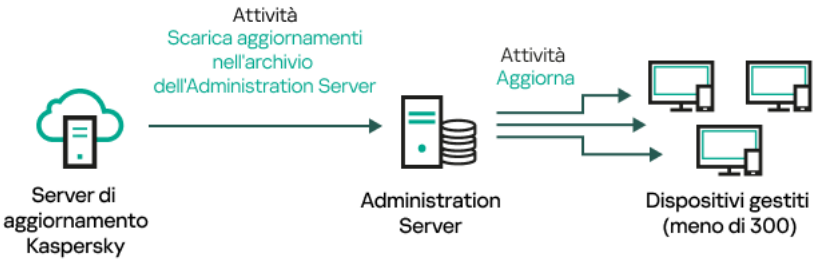
  Kaspersky Security Center consente di aggiornare automaticamente Network Agent e le applicazioni Kaspersky installate nei dispositivi client basati su Windows e basati su Linux. L'aggiornamento continuo di Administration Server, Kaspersky Security Center Web Console e plug-in Web di gestione non è supportato. Per aggiornare questi componenti è necessario scaricare le versioni più recenti delle applicazioni dal sito Web di Kaspersky, quindi installarle manualmente.

In base alla configurazione della propria rete è possibile utilizzare i seguenti schemi di download e distribuzione degli aggiornamenti richiesti ai dispositivi gestiti:

- Utilizzando un'unica attività: *Scarica aggiornamenti nell'archivio dell'Administration Server*
- Utilizzando due attività:
  - L'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*
  - L'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*
- Manualmente attraverso una cartella locale, una cartella condivisa o un server FTP
- Direttamente dai server di aggiornamento Kaspersky a Kaspersky Endpoint Security nei dispositivi gestiti
- Tramite una cartella locale o di rete se Administration Server non dispone della connessione a Internet

Utilizzo dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server

In questo schema Kaspersky Security Center scarica gli aggiornamenti tramite l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Nelle reti piccole che contengono meno di 300 dispositivi gestiti in un singolo segmento di rete o meno di 10 dispositivi gestiti in ciascun segmento di rete, gli aggiornamenti vengono distribuiti nei dispositivi gestiti direttamente dall'archivio di Administration Server (vedere la figura di seguito).

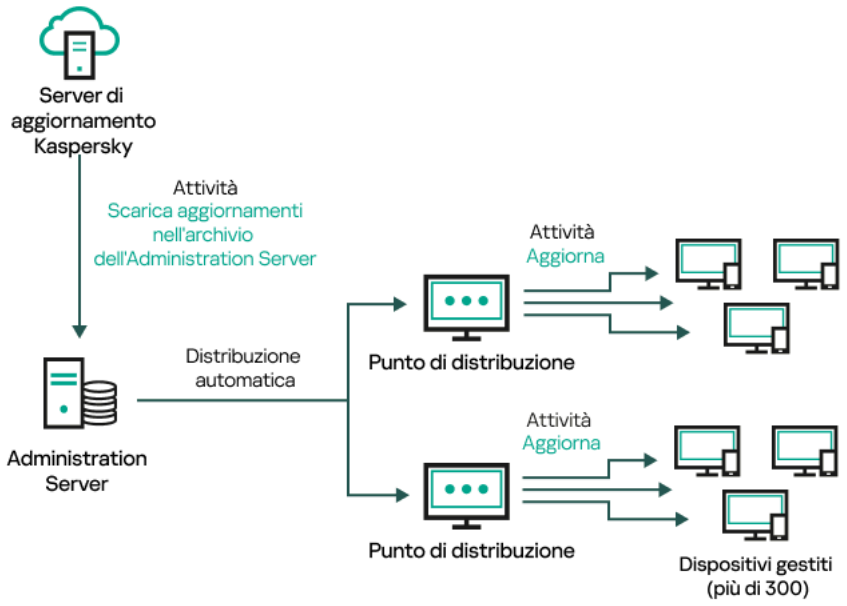


Aggiornamento tramite l'attività Scarica aggiornamenti nell'archivio dell'Administration Server senza punti di distribuzione

Per impostazione predefinita, Administration Server comunica con i server di aggiornamento Kaspersky e scarica gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server per fare in modo che utilizzi il protocollo HTTP anziché HTTPS.

Se la rete contiene più di 300 dispositivi gestiti in un singolo segmento di rete o se la rete è composta da più segmenti di rete con più di 9 dispositivi gestiti in ciascun segmento di rete, è consigliabile utilizzare i punti di distribuzione per propagare gli aggiornamenti ai dispositivi gestiti (vedere la figura di seguito). I punti di distribuzione riducono il carico per Administration Server e ottimizzano il traffico tra Administration Server e dispositivi gestiti. È possibile calcolare il numero e la configurazione dei punti di distribuzione richiesti per la rete.

In questo schema gli aggiornamenti vengono scaricati automaticamente dall'archivio di Administration Server agli archivi dei punti di distribuzione. I dispositivi gestiti inclusi nell'ambito di un punto di distribuzione scaricano gli aggiornamenti dall'archivio del punto di distribuzione anziché dall'archivio di Administration Server.



Aggiornamento tramite l'attività Scarica aggiornamenti nell'archivio dell'Administration Server con punti di distribuzione

Al completamento dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, i seguenti aggiornamenti vengono scaricati nell'archivio dell'Administration Server:

- Moduli del software e database Kaspersky per Kaspersky Security Center

  Questi aggiornamenti vengono installati automaticamente.

- Moduli del software e database Kaspersky per le applicazioni di protezione nei dispositivi gestiti

  Questi aggiornamenti vengono installati tramite l'attività di aggiornamento per Kaspersky Endpoint Security for Windows.

- Aggiornamenti per Administration Server

  Questi aggiornamenti non vengono installati automaticamente. L'amministratore deve approvare esplicitamente ed eseguire l'installazione degli aggiornamenti.

  Sono necessari i diritti di amministratore locale per l'installazione delle patch nell'Administration Server.

- Aggiornamenti per i componenti di Kaspersky Security Center

  Per impostazione predefinita, questi aggiornamenti vengono installati automaticamente. È possibile modificare le impostazioni nel criterio di Network Agent.

- Aggiornamenti per le applicazioni di protezione

  Per impostazione predefinita, Kaspersky Endpoint Security for Windows installa solo gli aggiornamenti approvati. È possibile approvare gli aggiornamenti tramite Administration Console o tramite Kaspersky Security Center Web Console. Gli aggiornamenti vengono installati attraverso l'attività di *aggiornamento* e possono essere configurati nelle proprietà di questa attività.

L'attività *Scarica aggiornamenti nell'archivio di Administration Server* non è disponibile negli Administration Server virtuali. L'archivio dell'Administration Server virtuale visualizza gli aggiornamenti scaricati nell'Administration Server primario.

È possibile configurare la verifica della possibilità di utilizzare gli aggiornamenti e degli eventuali errori in un set di dispositivi di test. Se la verifica ha esito positivo, gli aggiornamenti vengono distribuiti agli altri dispositivi gestiti.

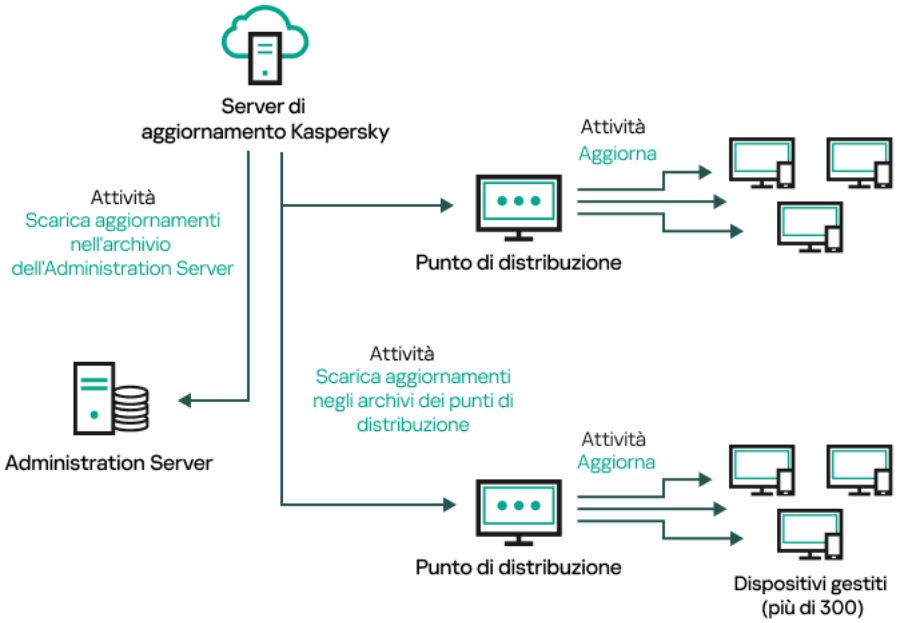
Ogni applicazione Kaspersky richiede gli aggiornamenti necessari da Administration Server. Administration Server aggrega tali richieste e scarica solo gli aggiornamenti che sono richiesti da un'applicazione. Questo garantisce che gli stessi aggiornamenti non vengano scaricati più volte e che gli aggiornamenti non necessari non vengano scaricati affatto. Durante l'esecuzione dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, Administration Server invia automaticamente le seguenti informazioni ai server di aggiornamento Kaspersky per garantire il download delle versioni appropriate dei moduli software e dei database Kaspersky:

- Versione e ID applicazione
- ID di installazione dell'applicazione
- ID chiave attiva
- ID di esecuzione dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*

Le informazioni trasmesse non contengono dati personali o altri dati riservati. AO Kaspersky Lab protegge le informazioni in base ai requisiti previsti dalla legge.

Tramite due attività: l'attività Scarica aggiornamenti nell'archivio dell'Administration Server e l'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

È possibile scaricare gli aggiornamenti negli archivi dei punti di distribuzione direttamente dai server di aggiornamento Kaspersky anziché dall'archivio di Administration Server, quindi distribuire gli aggiornamenti ai dispositivi gestiti (vedere la figura di seguito). Il download negli archivi dei punti di distribuzione è preferibile se il traffico tra Administration Server e punti di distribuzione è superiore rispetto a quello del traffico tra i punti di distribuzione e i server di aggiornamento Kaspersky oppure se Administration Server non dispone di accesso a Internet.



Aggiornamento tramite l'attività Scarica aggiornamenti nell'archivio dell'Administration Server e l'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

Per impostazione predefinita, Administration Server e i punti di distribuzione comunicano con i server di aggiornamento Kaspersky e scaricano gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server e/o i punti di distribuzione per fare in modo che utilizzino il protocollo HTTP anziché HTTPS.

Per implementare questo schema, creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* oltre all'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. In seguito, i punti di distribuzione scaricheranno gli aggiornamenti dai server di aggiornamento Kaspersky e non dall'archivio di Admnistration Server.

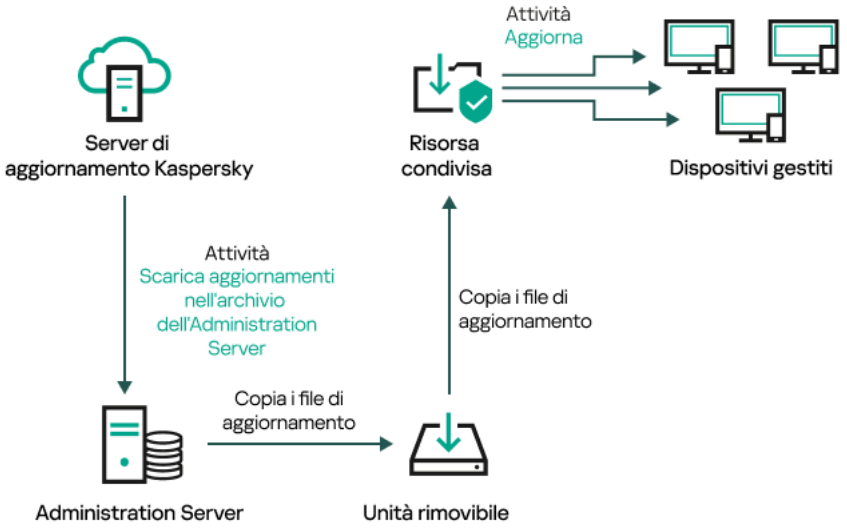
I dispositivi dei punti di distribuzione che eseguono macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky.

Se uno o più dispositivi che eseguono macOS rientrano nell'ambito dell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, l'attività viene completata con lo stato *Non riuscito*, anche se è stata completata correttamente in tutti i dispositivi Windows.

Anche l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* è richiesta per questo schema, poiché questa attività è utilizzata per scaricare i moduli software e i database Kaspersky per Kaspersky Security Center.

Manualmente attraverso una cartella locale, una cartella condivisa o un server FTP

Se i dispositivi client non hanno una connessione ad Administration Server, è possibile utilizzare una cartella locale o una risorsa condivisa come sorgente per l'aggiornamento di database, moduli software e applicazioni Kaspersky. In questo schema è necessario copiare gli aggiornamenti richiesti dall'archivio di Administration Server in un'unità rimovibile, quindi copiare gli aggiornamenti nella cartella locale o nella risorsa condivisa specificata come sorgente degli aggiornamenti nelle impostazioni di Kaspersky Endpoint Security (vedere la figura di seguito).



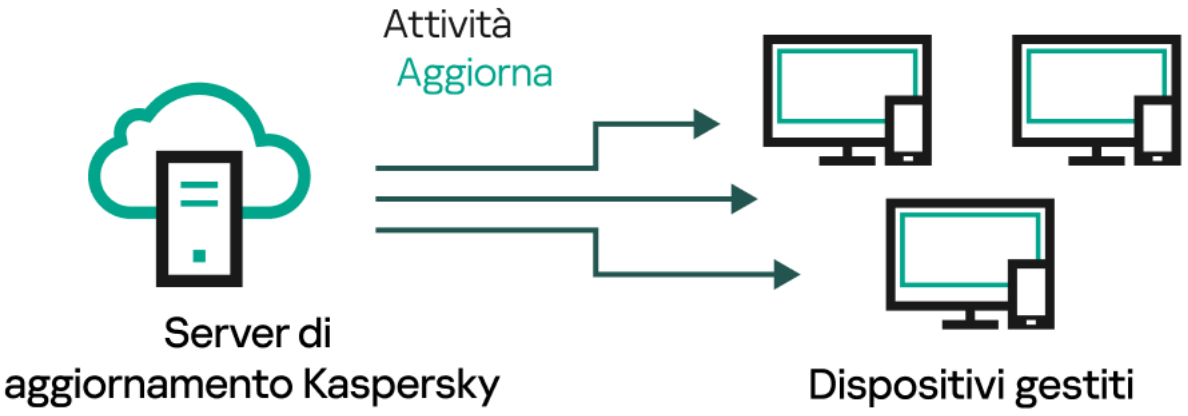
Aggiornamento tramite una cartella locale, una cartella condivisa o un server FTP

Per ulteriori informazioni sulle sorgenti degli aggiornamenti in Kaspersky Endpoint Security, consultare le seguenti Guide:

- Guida di Kaspersky Endpoint Security for Windows
- Guida di Kaspersky Endpoint Security for Linux

Direttamente dai server di aggiornamento Kaspersky a Kaspersky Endpoint Security nei dispositivi gestiti

Nei dispositivi gestiti, è possibile configurare Kaspersky Endpoint Security per ricevere gli aggiornamenti direttamente dai server di aggiornamento Kaspersky (vedere la figura di seguito).



Aggiornamento delle applicazioni di protezione direttamente dai server di aggiornamento Kaspersky

In questo schema, l'applicazione di protezione non utilizza gli archivi forniti da Kaspersky Security Center. Per ricevere gli aggiornamenti direttamente dai server di aggiornamento Kaspersky, specificare i server di aggiornamento Kaspersky come sorgente degli aggiornamenti nell'interfaccia dell'applicazione di protezione. Per ulteriori informazioni su queste impostazioni, consultare le seguenti Guide:

- Guida di Kaspersky Endpoint Security for Windows
- Guida di Kaspersky Endpoint Security for Linux

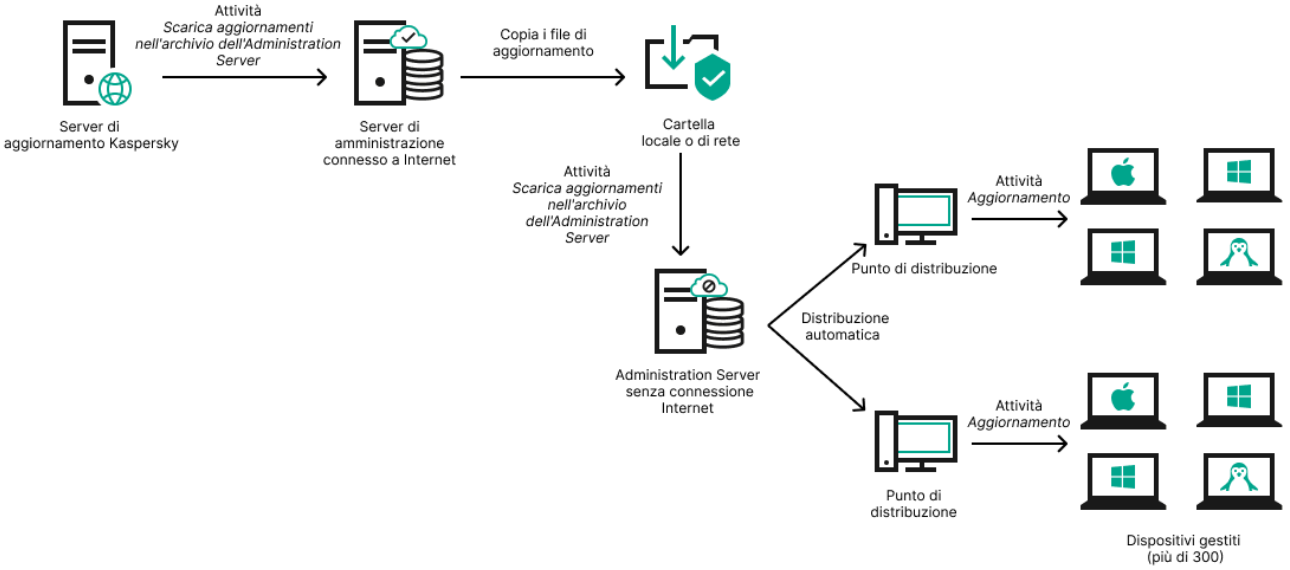
Tramite una cartella locale o di rete se Administration Server non dispone della connessione a Internet

Se Administration Server non dispone della connessione a Internet, è possibile configurare l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* per scaricare gli aggiornamenti da una cartella locale o di rete. In questo caso, di tanto in tanto è necessario copiare i file di aggiornamento necessari nella cartella specificata. È ad esempio possibile copiare i file di aggiornamento necessari da una delle seguenti origini:

- Administration Server con una connessione Internet (vedere la figura seguente)

  Poiché un Administration Server scarica solo gli aggiornamenti richiesti dalle applicazioni di protezione, i set di applicazioni di protezione gestiti dagli Administration Server (quello con una connessione Internet e quello senza connessione), devono corrispondere.

  Se l'Administration Server utilizzato per scaricare gli aggiornamenti dispone della versione 13.2 o precedente, aprire le proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, quindi abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**.



Aggiornamento tramite una cartella locale o di rete se Administration Server non dispone di una connessione Internet

- Kaspersky Update Utility

  Poiché questa utilità utilizza il vecchio schema per scaricare gli aggiornamenti, aprire le proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, quindi abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**.

Creazione dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server

L'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* viene creata automaticamente in Administration Server dall'Avvio rapido guidato di Kaspersky Security Center. È possibile creare una sola attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Di conseguenza, è possibile creare un'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* solo se tale attività è stata rimossa dall'elenco di attività di Administration Server.

Questa attività è necessaria per scaricare gli aggiornamenti dai server di aggiornamento Kaspersky nell'archivio di Administration Server. L'elenco degli aggiornamenti include:

- Aggiornamenti dei database e dei moduli software di Administration Server
- Aggiornamenti dei database e dei moduli software delle applicazioni di protezione Kaspersky
- Aggiornamenti dei componenti di Kaspersky Security Center
- Aggiornamenti delle applicazioni di protezione Kaspersky

Dopo aver scaricato gli aggiornamenti, questi possono essere propagati ai dispositivi gestiti.

Prima di distribuire gli aggiornamenti ai dispositivi gestiti, è possibile eseguire l'attività *Verifica aggiornamenti*. Ciò consente di assicurarsi che Administration Server installi correttamente gli aggiornamenti scaricati e che il livello di sicurezza non diminuisca a causa degli aggiornamenti. Per verificarli prima della distribuzione, configurare l'opzione **Esegui la verifica degli aggiornamenti** nelle impostazioni dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*.

*Per creare l'attività **Scarica aggiornamenti nell'archivio dell'Administration Server**:*

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Scarica aggiornamenti nell'archivio dell'Administration Server**.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
6. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
7. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

8. Nella finestra delle proprietà visualizzata, nella scheda **Impostazioni applicazione**, specificare le seguenti impostazioni:

- Sorgenti degli aggiornamenti

  È possibile utilizzare le seguenti risorse come sorgenti degli aggiornamenti per l'Administration Server:

  - Server degli aggiornamenti Kaspersky

    I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni. Per impostazione predefinita, Administration Server comunica con i server di aggiornamento Kaspersky e scarica gli aggiornamenti utilizzando il protocollo HTTPS. È possibile configurare Administration Server per fare in modo che utilizzi il protocollo HTTP anziché HTTPS.

    Opzione selezionata per impostazione predefinita.

  - Administration Server primario

    Questa risorsa si applica alle attività create per un Administration Server secondario o virtuale.

  - Cartella locale o di rete

    Un'unità locale o una cartella di rete che contiene gli aggiornamenti più recenti. Una cartella di rete può essere un server FTP o HTTP oppure una condivisione SMB. Se una cartella di rete richiede l'autenticazione, è supportato solo il protocollo SMB. Quando si seleziona una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server.

    > Una cartella di rete o un server FTP o HTTP utilizzato da una sorgente degli aggiornamenti deve contenere una struttura di cartelle (con gli aggiornamenti) che corrisponde alla struttura creata durante l'utilizzo dei server di aggiornamento Kaspersky.

  Nel caso in cui una cartella condivisa che contiene aggiornamenti sia protetta da password, abilitare l'opzione **Specifica l'account per accedere alla cartella condivisa della sorgente degli aggiornamenti (se disponibile)** e inserire le credenziali dell'account necessarie per l'accesso.

- Cartella per l'archiviazione degli aggiornamenti

  Il percorso della cartella specificata per l'archiviazione degli aggiornamenti salvati. È possibile copiare il percorso della cartella specificata negli appunti. Non è possibile modificare il percorso di una cartella specificata per un'attività di gruppo.

- Altre impostazioni:

  - Forza aggiornamento degli Administration Server secondari

    Se questa opzione è abilitata, Administration Server avvia le attività di aggiornamento negli Administration Server secondari non appena vengono scaricati nuovi aggiornamenti. Le attività di aggiornamento vengono avviate utilizzando la sorgente dell'aggiornamento configurata nelle proprietà dell'attività negli Administration Server secondari.

    Se questa opzione è disabilitata, le attività di aggiornamento negli Administration Server secondari vengono avviate in base alla relativa pianificazione.

    Per impostazione predefinita, questa opzione è disabilitata.

  - Copia gli aggiornamenti scaricati in cartelle aggiuntive

Dopo avere ricevuto gli aggiornamenti, l'Administration Server li copia nelle cartelle specificate. Utilizzare questa opzione se si desidera gestire manualmente la distribuzione degli aggiornamenti nella rete.

Questa opzione può ad esempio essere utilizzata nella seguente situazione: la rete dell'organizzazione è composta da diverse subnet indipendenti e i dispositivi in ciascuna subnet non hanno accesso ad altre subnet. I dispositivi in tutte le subnet hanno tuttavia accesso a una condivisione di rete comune. In questo caso, è possibile impostare Administration Server in una delle subnet per il download degli aggiornamenti dai server di aggiornamento Kaspersky, abilitare questa opzione e quindi specificare la condivisione di rete. Nelle attività di download degli aggiornamenti nell'archivio per gli altri Administration Server specificare la stessa condivisione di rete come sorgente degli aggiornamenti.

Se si seleziona di copiare gli aggiornamenti scaricati in una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server. Il percorso della cartella dipende dal sistema operativo del dispositivo. Poiché la cartella locale si trova in Administration Server basato su Linux, è necessario specificare il percorso POSIX, ad esempio /path/to/dir.

Quando si seleziona una cartella di rete che si trova in Administration Server basato su Linux, è necessario garantire preventivamente l'accesso alla cartella di rete dal dispositivo in cui è installato Administration Server montando la cartella. L'accesso alla cartella viene eseguito utilizzando il protocollo SMB.

Per impostazione predefinita, questa opzione è disabilitata.

- **Non forzare l'aggiornamento dei dispositivi e degli Administration Server secondari prima del completamento della copia**

  Le attività di download degli aggiornamenti nei dispositivi client e negli Administration Server secondari vengono avviate solo una volta che gli aggiornamenti sono stati copiati dalla cartella degli aggiornamenti principale nelle cartelle degli aggiornamenti aggiuntive.

  Questa opzione deve essere abilitata se i dispositivi client e gli Administration Server secondari scaricano gli aggiornamenti da cartelle di rete aggiuntive.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Contenuto degli aggiornamenti**:

  - **Scarica file diff**

    Questa opzione consente di abilitare la funzionalità di download dei file diff.

    Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica gli aggiornamenti utilizzando lo schema precedente**

A partire dalla versione 14, Kaspersky Security Center scarica gli aggiornamenti dei database e dei moduli software utilizzando il nuovo schema. Affinché l'applicazione possa scaricare gli aggiornamenti utilizzando il nuovo schema, la sorgente degli aggiornamenti deve contenere i file di aggiornamento con i metadati compatibili con il nuovo schema. Se la sorgente degli aggiornamenti contiene i file di aggiornamento con i metadati compatibili solo con lo schema precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**. In caso contrario, l'attività di download degli aggiornamenti avrà esito negativo.

È ad esempio necessario abilitare questa opzione quando una cartella locale o di rete è specificata come sorgente degli aggiornamenti e i file di aggiornamento in questa cartella sono stati scaricati da una delle seguenti applicazioni:

- Kaspersky Update Utility

  Questa utilità scarica gli aggiornamenti utilizzando lo schema precedente.

- Kaspersky Security Center 13.2 o versione precedente

  Ad esempio, Administration Server 1 non dispone di una connessione Internet. In questo caso, è possibile scaricare gli aggiornamenti utilizzando un Administration Server 2 dotato di una connessione Internet, quindi posizionare gli aggiornamenti in una cartella locale o di rete per utilizzarlo come sorgente degli aggiornamenti per Administration Server 1. Se Administration Server 2 dispone della versione 13.2 ò precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente** nell'attività per Administration Server 1.

Per impostazione predefinita, questa opzione è disabilitata.

- **Esegui la verifica degli aggiornamenti**

  Administration Server esegue il download degli aggiornamenti dalla sorgente, li salva in un archivio temporaneo ed esegue l'attività definita nel campo **Attività di verifica degli aggiornamenti**. Se l'attività viene completata correttamente, gli aggiornamenti verranno copiati dall'archivio temporaneo in una cartella condivisa di Administration Server e saranno distribuiti in tutti gli altri dispositivi per cui Administration Server opera come sorgente degli aggiornamenti (verranno avviate le attività con il tipo di pianificazione **Quando vengono scaricati nuovi aggiornamenti nell'archivio**). L'attività di download degli aggiornamenti nell'archivio viene conclusa solo una volta completata l'attività *Verifica aggiornamenti*.

  Per impostazione predefinita, questa opzione è disabilitata.

9. Nella finestra delle proprietà dell'attività, nella scheda **Pianificazione**, creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- Avvia attività:

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - Manualmente

    L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

    Per impostazione predefinita, questa opzione è selezionata.

  - Ogni N minuti

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - Ogni N ore

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - Ogni N giorni

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - In base ai giorni della settimana

    L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

  - Mensile

    L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

    Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

    Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

  - Ogni mese nei giorni specificati delle settimane selezionate

L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

> Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

È possibile selezionare più giorni della settimana.

- **Durante un'epidemia di virus**

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- **Al completamento di un'altra attività**

  L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

  È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

  Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

  - Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
  - Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

    Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
  - Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- **Esegui attività non effettuate**

Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale automaticamente per l'avvio delle attività con un intervallo di**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

- **Arresta se l'attività viene eseguita per più di**

  Al termine del periodo di tempo specificato, l'attività viene arrestata automaticamente, che sia stata completata o meno.

  Abilitare questa opzione se si desidera interrompere (o arrestare) le attività che richiedono troppo tempo per l'esecuzione.

  Per impostazione predefinita, questa opzione è disabilitata. Il tempo predefinito per l'esecuzione dell'attività è 120 minuti.

10. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Quando Administration Server esegue l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, gli aggiornamenti dei database e dei moduli software vengono scaricati dalla sorgente degli aggiornamenti e archiviati nella cartella condivisa di Administration Server. Se questa attività viene creata per un gruppo di amministrazione, verrà applicata solo ai Network Agent inclusi nel gruppo di amministrazione specificato.

Gli aggiornamenti vengono distribuiti nei dispositivi client e negli Administration Server secondari dalla cartella condivisa di Administration Server.

Verifica degli aggiornamenti scaricati

Prima di installare gli aggiornamenti nei dispositivi gestiti, è possibile verificare la possibilità di utilizzare gli aggiornamenti e gli eventuali errori tramite l'attività *Verifica aggiornamenti*. L'attività di *verifica degli aggiornamenti* viene eseguita automaticamente nell'ambito dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*. Administration Server scarica gli aggiornamenti dalla sorgente, li salva nell'archivio temporaneo ed esegue l'attività *Verifica aggiornamenti*. Se l'attività viene completata correttamente, gli aggiornamenti sono copiati dall'archivio temporaneo nella cartella condivisa di Administration Server. Vengono distribuiti a tutti i dispositivi client per cui l'Administration Server opera come sorgente degli aggiornamenti.

Se i risultati dell'attività *Verifica aggiornamenti* mostrano che gli aggiornamenti presenti nell'archivio temporaneo non sono corretti o se l'attività *Verifica aggiornamenti* viene completata con un errore, gli aggiornamenti non vengono copiati nella cartella condivisa. L'Administration Server mantiene il set di aggiornamenti precedente. Inoltre, le attività con il tipo di pianificazione **Quando vengono scaricati nuovi aggiornamenti nell'archivio** non vengono avviate. Tali operazioni vengono eseguite al successivo avvio dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, se la scansione dei nuovi aggiornamenti viene completata correttamente.

Un set di aggiornamenti è considerato non valido se viene soddisfatta una delle seguenti condizioni in almeno un dispositivo di test:

- Si è verificato un errore dell'attività di aggiornamento.
- Lo stato della protezione in tempo reale dell'applicazione di protezione è cambiato dopo l'applicazione degli aggiornamenti.
- È stato rilevato un oggetto infetto durante l'esecuzione dell'attività di scansione su richiesta.
- Si è verificato un errore di runtime di un'applicazione Kaspersky.

Se nei dispositivi di test non si verifica alcuna delle condizioni elencate, il set di aggiornamenti viene considerato valido e l'attività *Verifica aggiornamenti* viene considerata completata correttamente.

Prima di iniziare a creare l'attività *Verifica aggiornamenti*, eseguire i prerequisiti:

1. Creare un gruppo di amministrazione con diversi dispositivi di test. Sarà necessario questo gruppo per verificare gli aggiornamenti.

   È consigliabile utilizzare dispositivi con il livello di protezione più affidabile e con la configurazione delle applicazioni più diffusa nella rete. Questo approccio aumenta la qualità e la probabilità di rilevamento dei virus durante le scansioni e riduce al minimo il rischio di falsi positivi. Se vengono rilevati virus nei dispositivi di test, l'attività *Verifica aggiornamenti* viene considerata non riuscita.

2. Creare le attività di aggiornamento e scansione malware per un'applicazione supportata da Kaspersky Security Center, ad esempio Kaspersky Endpoint Security for Windows o Kaspersky Security for Windows Server. Quando si creano le attività di aggiornamento e scansione malware, specificare il gruppo di amministrazione con i dispositivi di test.

   L'attività *Verifica aggiornamenti* esegue in sequenza le attività di aggiornamento e scansione malware nei dispositivi di test per verificare che tutti gli aggiornamenti siano validi. Inoltre, durante la creazione dell'attività *Verifica aggiornamenti*, è necessario specificare le attività di aggiornamento e scansione malware.

3. Creare l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*.

Per fare in modo che Kaspersky Security Center verifichi gli aggiornamenti scaricati prima di distribuirli ai dispositivi client:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sull'attività **Scarica aggiornamenti nell'archivio dell'Administration Server**.
3. Nella finestra delle proprietà dell'attività visualizzata, passare alla scheda **Impostazioni applicazione**, quindi abilitare l'opzione **Esegui la verifica degli aggiornamenti**.
4. Se l'attività di *verifica dell'aggiornamento* esiste, fare clic sul pulsante **Seleziona attività**. Nella finestra visualizzata selezionare l'attività *Verifica aggiornamenti* nel gruppo di amministrazione con dispositivi di test.

5. Se non è stata creata l'attività *Verifica aggiornamenti* in precedenza, procedere come segue:

   a. Fare clic sul pulsante **Nuova attività**.

   b. Nella Creazione guidata nuova attività visualizzata, specificare il nome dell'attività se si desidera modificare il nome preimpostato.

   c. Selezionare il gruppo di amministrazione con i dispositivi di test creato in precedenza.

   d. In primo luogo, selezionare l'attività di aggiornamento di un'applicazione desiderata supportata da Kaspersky Security Center, quindi selezionare l'attività di scansione malware.

   Successivamente, vengono visualizzate le seguenti opzioni. È consigliabile lasciarle abilitate:

   - **Riavvia il dispositivo dopo l'aggiornamento del database**

     Dopo l'aggiornamento dei database anti-virus in un dispositivo, è consigliabile riavviare il dispositivo.

     Per impostazione predefinita, l'opzione è abilitata.

   - **Verifica lo stato della protezione in tempo reale dopo l'aggiornamento del database e il riavvio del dispositivo**

     Se questa opzione è abilitata, l'attività *Verifica aggiornamenti* verifica se gli aggiornamenti scaricati nell'archivio dell'Administration Server sono validi e se il livello di protezione è diminuito dopo l'aggiornamento dei database anti-virus e il riavvio del dispositivo.

     Per impostazione predefinita, questa opzione è abilitata.

   e. Specificare un account da cui verrà eseguita l'attività *Verifica aggiornamenti*. È possibile utilizzare il proprio account e lasciare abilitata l'opzione **Account predefinito**. In alternativa, è possibile specificare che l'attività deve essere eseguita con un altro account che disponga dei diritti di accesso necessari. A tale scopo, selezionare l'opzione **Specifica account**, quindi immettere le credenziali di tale account.

6. Fare clic su **Salva** per chiudere la finestra delle proprietà dell'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*.

La verifica automatica degli aggiornamenti è abilitata. Adesso è possibile eseguire l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server*, che inizierà dalla verifica degli aggiornamenti.

Creazione dell'attività Scarica aggiornamenti negli archivi dei punti di distribuzione

L'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* è disponibile solo per i dispositivi dei punti di distribuzione che eseguono Windows. I dispositivi dei punti di distribuzione in cui viene eseguito Linux o macOS non possono scaricare gli aggiornamenti dai server di aggiornamento Kaspersky. Se almeno un dispositivo in cui viene eseguito Linux o macOS rientra nell'ambito dell'attività, per l'attività verrà visualizzato lo stato *Non riuscito*. Anche se l'attività viene completata correttamente in tutti i dispositivi Windows, verrà restituito un errore nei dispositivi rimanenti.

È possibile creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per un gruppo di amministrazione. L'attività verrà eseguita per i punti di distribuzione inclusi nel gruppo di amministrazione specificato.

È ad esempio possibile utilizzare questa attività se il costo del traffico tra l'Administration Server e i punti di distribuzione è superiore rispetto a quello del traffico tra i punti di distribuzione e i server di aggiornamento Kaspersky oppure se l'Administration Server non dispone di accesso a Internet.

Questa attività è necessaria per scaricare gli aggiornamenti dai server di aggiornamento Kaspersky negli archivi dei punti di distribuzione. L'elenco degli aggiornamenti include:

- Aggiornamenti dei database e dei moduli software delle applicazioni di protezione Kaspersky
- Aggiornamenti dei componenti di Kaspersky Security Center
- Aggiornamenti delle applicazioni di protezione Kaspersky

Dopo aver scaricato gli aggiornamenti, questi possono essere propagati ai dispositivi gestiti.

Se i punti di distribuzione si connettono a Internet utilizzando un server proxy, è necessario specificare le impostazioni corrispondenti nel criterio di Network Agent.

*Per creare l'attività **Scarica aggiornamenti negli archivi dei punti di distribuzione** per un gruppo di amministrazione selezionato:*

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center, nel campo **Tipo di attività** selezionare **Scarica aggiornamenti negli archivi dei punti di distribuzione**.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare un pulsante di opzione per specificare il gruppo di amministrazione, la selezione dispositivi o i dispositivi a cui si applica l'attività.
6. Nel passaggio **Completare la creazione dell'attività** dell'attività, se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
7. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
8. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

9. Nella scheda **Impostazioni applicazione** della finestra delle proprietà dell'attività specificare le seguenti impostazioni:

- **Sorgenti degli aggiornamenti**

  È possibile utilizzare le seguenti risorse come sorgenti degli aggiornamenti per il punto di distribuzione:

  - Server degli aggiornamenti Kaspersky

    I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.

    Questa opzione è selezionata per impostazione predefinita.

  - Cartella locale o di rete

    Un'unità locale o una cartella di rete che contiene gli aggiornamenti più recenti. Una cartella di rete può essere un server FTP o HTTP oppure una condivisione SMB. Se una cartella di rete richiede l'autenticazione, è supportato solo il protocollo SMB. Quando si seleziona una cartella locale, è necessario specificare una cartella nel dispositivo in cui è installato Administration Server.

    Una cartella di rete o un server FTP o HTTP utilizzato da una sorgente degli aggiornamenti deve contenere una struttura di cartelle (con gli aggiornamenti) che corrisponde alla struttura creata durante l'utilizzo dei server di aggiornamento Kaspersky.

- **Cartella per l'archiviazione degli aggiornamenti**

  Il percorso della cartella specificata per l'archiviazione degli aggiornamenti salvati. È possibile copiare il percorso della cartella specificata negli appunti. Non è possibile modificare il percorso di una cartella specificata per un'attività di gruppo.

- **Scarica file diff**

  Questa opzione consente di abilitare la funzionalità di download dei file diff.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica gli aggiornamenti utilizzando lo schema precedente**

A partire dalla versione 14, Kaspersky Security Center scarica gli aggiornamenti dei database e dei moduli software utilizzando il nuovo schema. Affinché l'applicazione possa scaricare gli aggiornamenti utilizzando il nuovo schema, la sorgente degli aggiornamenti deve contenere i file di aggiornamento con i metadati compatibili con il nuovo schema. Se la sorgente degli aggiornamenti contiene i file di aggiornamento con i metadati compatibili solo con lo schema precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente**. In caso contrario, l'attività di download degli aggiornamenti avrà esito negativo.

È ad esempio necessario abilitare questa opzione quando una cartella locale o di rete è specificata come sorgente degli aggiornamenti e i file di aggiornamento in questa cartella sono stati scaricati da una delle seguenti applicazioni:

- Kaspersky Update Utility

  Questa utilità scarica gli aggiornamenti utilizzando lo schema precedente.

- Kaspersky Security Center 13.2 o versione precedente

  Un punto di distribuzione è ad esempio configurato per acquisire gli aggiornamenti da una cartella locale o di rete. In questo caso, è possibile scaricare gli aggiornamenti utilizzando un Administration Server dotato di una connessione Internet, quindi posizionare gli aggiornamenti nella cartella locale nel punto di distribuzione. Se la versione di Administration Server è la 13.2 o precedente, abilitare l'opzione **Scarica gli aggiornamenti utilizzando lo schema precedente** nell'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*.

Per impostazione predefinita, questa opzione è disabilitata.

10. Creare una pianificazione per l'avvio dell'attività. Se necessario, specificare le seguenti impostazioni:

- **Avvia attività**

  Selezionare la pianificazione per l'esecuzione dell'attività e configurare la pianificazione selezionata.

  - **Manualmente**

    L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

    Per impostazione predefinita, questa opzione è selezionata.

  - **Ogni N minuti**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

  - **Ogni N ore**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

  - **Ogni N giorni**

    L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

    Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - **In base ai giorni della settimana**

    L'attività viene eseguita periodicamente, nei giorni specificati della settimana, all'ora specificata.

    Per impostazione predefinita, l'attività viene eseguita ogni venerdì alle 18:00:00.

  - **Mensile**

    L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

    Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

    Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

  - **Ogni mese nei giorni specificati delle settimane selezionate**

L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

È possibile selezionare più giorni della settimana.

- Durante un'epidemia di virus

  L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

  - Anti-virus per workstation e file server
  - Anti-virus per la difesa perimetrale
  - Anti-virus per i sistemi di posta

  Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

  Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- Al completamento di un'altra attività

  L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

  È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

  Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

  - Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
  - Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

    Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
  - Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

- Esegui attività non effettuate

Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

Per impostazione predefinita, questa opzione è disabilitata.

- **Usa automaticamente il ritardo casuale per l'avvio delle attività**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

- **Usa ritardo casuale automaticamente per l'avvio delle attività con un intervallo di**

  Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

  Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

11. Fare clic sul pulsante **Salva**.

    L'attività verrà creata e configurata.

    Oltre alle impostazioni specificate durante la creazione dell'attività, è possibile modificare altre proprietà di un'attività creata.

Quando si esegue l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*, gli aggiornamenti dei database e dei moduli software vengono scaricati dalla sorgente degli aggiornamenti e archiviati nella cartella condivisa. Gli aggiornamenti scaricati verranno utilizzati solo dai punti di distribuzione inclusi nel gruppo di amministrazione specificato e che non hanno alcuna attività di download degli aggiornamenti esplicitamente configurata.

Abilitazione e disabilitazione dell'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center

Gli aggiornamenti e le patch per Administration Server possono essere installati solo manualmente, dopo aver ottenuto l'approvazione esplicita dall'amministratore.

L'installazione automatica degli aggiornamenti e delle patch per i componenti di Kaspersky Security Center è abilitata per impostazione predefinita durante l'installazione di Network Agent nel dispositivo. È possibile disabilitarla durante l'installazione di Network Agent o disabilitarla in un secondo momento utilizzando un criterio.

Per disabilitare l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center durante l'installazione locale di Network Agent in un dispositivo:

1. Avviare l'installazione locale di Network Agent nel dispositivo.
2. Durante il passaggio **Impostazioni avanzate** deselezionare la casella di controllo **Installa automaticamente gli aggiornamenti applicabili e le patch per i componenti con stato Indefinito**.
3. Seguire le istruzioni della procedura guidata.

   Nel dispositivo verrà installato Network Agent con l'installazione automatica di aggiornamenti e patch disabilitata per i componenti di Kaspersky Security Center. È possibile abilitare l'installazione automatica di aggiornamenti e patch in un secondo momento utilizzando un criterio.

Per disabilitare l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center durante l'installazione di Network Agent nel dispositivo tramite un pacchetto di installazione:

1. Nel menu principale accedere a **Operazioni → Archivi → Pacchetti di installazione**.
2. Fare clic sul pacchetto **Kaspersky Security Center Network Agent <numero di versione>**.
3. Nella finestra delle proprietà aprire la scheda **Impostazioni**.
4. Disattivare l'interruttore **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito**.

   Network Agent con l'installazione automatica di aggiornamenti e patch disabilitata per i componenti di Kaspersky Security Center verrà installato da questo pacchetto. È possibile abilitare l'installazione automatica di aggiornamenti e patch in un secondo momento utilizzando un criterio.

Se questa casella di controllo è stata selezionata o deselezionata durante l'installazione di Network Agent nel dispositivo, successivamente è possibile abilitare (o disabilitare) l'aggiornamento automatico utilizzando il criterio di Network Agent.

Per abilitare o disabilitare l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center utilizzando il criterio di Network Agent:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul criterio di Network Agent.
3. Nella finestra delle proprietà del criterio aprire la scheda **Impostazioni applicazione**.
4. Nella sezione **Gestire patch e aggiornamenti** attivare o disattivare l'interruttore **Installa automaticamente le patch e gli aggiornamenti applicabili per i componenti con lo stato Indefinito** per abilitare o disabilitare, rispettivamente, l'applicazione automatica di aggiornamenti e patch.
5. Impostare il lucchetto (🔒) per questo interruttore.

Il criterio verrà applicato ai dispositivi selezionati e l'installazione automatica di aggiornamenti e patch per i componenti di Kaspersky Security Center verrà abilitata (o disabilitata) in tali dispositivi.

Installazione automatica degli aggiornamenti per Kaspersky Endpoint Security for Windows

È possibile configurare gli aggiornamenti automatici dei database e dei moduli software di Kaspersky Endpoint Security for Windows nei dispositivi client.

Per configurare il download e l'installazione automatica degli aggiornamenti di Kaspersky Endpoint Security for Windows nei dispositivi:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Endpoint Security for Windows, selezionare **Aggiornamento** come sottotipo di attività.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Scegliere l'ambito dell'attività.
6. Specificare il gruppo di amministrazione, la selezione dispositivi o i dispositivi a cui si applica l'attività.
7. Nel passaggio **Completare la creazione dell'attività** dell'attività, se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
8. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
9. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

10. Nella scheda **Impostazioni applicazione** della finestra delle proprietà dell'attività definire le impostazioni dell'attività di aggiornamento in modalità locale o mobile:

    - **Modalità locale**: Viene stabilita la connessione tra il dispositivo e Administration Server.
    - **Modalità mobile**: Non viene stabilita alcuna connessione tra Kaspersky Security Center e il dispositivo (ad esempio quando il dispositivo non è connesso a Internet).

11. Abilitare le sorgenti degli aggiornamenti che si desidera utilizzare per aggiornare i database e i moduli dell'applicazione per Kaspersky Endpoint Security for Windows. Se necessario, modificare le posizioni delle sorgenti nell'elenco utilizzando i pulsanti **Sposta su** e **Sposta giù**. Se sono abilitate diverse sorgenti degli aggiornamenti, Kaspersky Endpoint Security for Windows tenta di connettersi a tali sorgenti una dopo l'altra, a partire a quella all'inizio dell'elenco, ed esegue l'attività di aggiornamento recuperando il pacchetto di aggiornamento dalla prima sorgente disponibile.

12. Abilitare l'opzione **Installa gli aggiornamenti approvati del modulo delle applicazioni** per scaricare e installare gli aggiornamenti dei moduli software oltre ai database dell'applicazione.

    Se l'opzione è abilitata, Kaspersky Endpoint Security for Windows invia una notifica all'utente per informarlo degli aggiornamenti dei moduli software disponibili e include gli aggiornamenti dei moduli software nel pacchetto di aggiornamento durante l'esecuzione dell'attività di aggiornamento. Kaspersky Endpoint Security for Windows installa solo gli aggiornamenti per cui è stato impostato lo stato *Approvato*. Verranno installati in locale tramite l'interfaccia dell'applicazione o tramite Kaspersky Security Center.

    È inoltre possibile abilitare l'opzione **Installa automaticamente gli aggiornamenti critici del modulo delle applicazioni**. Se sono disponibili aggiornamenti per i moduli software, Kaspersky Endpoint Security for Windows li installa automaticamente con lo stato *Critico*. Gli aggiornamenti rimanenti saranno installati dopo essere stati approvati dall'amministratore.

    Se l'aggiornamento dei moduli software richiede la visualizzazione e l'accettazione delle condizioni del Contratto di licenza e dell'Informativa sulla privacy, l'applicazione installa gli aggiornamenti dopo che le condizioni del Contratto di licenza e dell'Informativa sulla privacy sono state accettate dall'utente.

13. Selezionare la casella di controllo **Copia aggiornamenti nella cartella** per fare in modo che gli aggiornamenti scaricati vengano salvati in una cartella, quindi specificare il percorso della cartella.

14. Pianificare l'attività. Per garantire aggiornamenti tempestivi, è consigliabile selezionare l'opzione **Quando vengono scaricati nuovi aggiornamenti nell'archivio**.

15. Fare clic su **Salva**.

Quando è in esecuzione l'attività **Aggiornamento**, l'applicazione invia richieste ai server di aggiornamento Kaspersky.

Alcuni aggiornamenti richiedono l'installazione delle versioni più recenti dei plug-in di gestione.

Approvazione e rifiuto degli aggiornamenti software

Le impostazioni di un'attività di installazione degli aggiornamenti possono richiedere l'approvazione degli aggiornamenti da installare. È possibile approvare gli aggiornamenti da installare e rifiutare quelli che non devono essere installati.

Ad esempio, potrebbe essere utile controllare prima l'installazione degli aggiornamenti in un ambiente di test e verificare che non interferiscano con l'utilizzo dei dispositivi e solo successivamente consentire l'installazione degli aggiornamenti nei dispositivi client.

L'approvazione e il rifiuto degli aggiornamenti sono disponibili solo per Network Agent e le applicazioni gestite installate nei dispositivi client basati su Windows. L'aggiornamento continuo di Administration Server, Kaspersky Security Center Web Console e plug-in Web di gestione non è supportato. Per aggiornare questi componenti è necessario scaricare le versioni più recenti delle applicazioni dal sito Web di Kaspersky, quindi installarle manualmente.

Per approvare o rifiutare uno o più aggiornamenti:

1. Nel menu principale, passare a **Operazioni → Applicazioni Kaspersky → Aggiornamenti immediati**.

   Verrà visualizzato un elenco degli aggiornamenti disponibili.

   Gli aggiornamenti delle applicazioni gestite potrebbero richiedere l'installazione di una versione minima specifica di Kaspersky Security Center. Se questa versione è successiva alla versione corrente, gli aggiornamenti vengono visualizzati ma non possono essere approvati. Inoltre, nessun pacchetto di installazione può essere creato da tali aggiornamenti finché non si esegue l'upgrade di Kaspersky Security Center. Viene richiesto di eseguire l'upgrade dell'istanza di Kaspersky Security Center alla versione minima richiesta.

2. Selezionare gli aggiornamenti che si desidera accettare o rifiutare.

3. Fare clic su **Approva** per approvare gli aggiornamenti selezionati o su **Rifiuta** per rifiutare gli aggiornamenti selezionati.

   Il valore predefinito è *Indefinito*.

Gli aggiornamenti a cui è assegnato lo stato *Approvato* verranno inseriti in una coda per l'installazione.

Gli aggiornamenti a cui è assegnato lo stato *Rifiutato* verranno disinstallati (se possibile) da tutti i dispositivi in cui erano installati in precedenza. Inoltre, non verranno installati in altri dispositivi in futuro.

Alcuni aggiornamenti per le applicazioni Kaspersky non possono essere disinstallati. Se si imposta lo stato *Rifiutato* per tali aggiornamenti, Kaspersky Security Center non li disinstallerà dai dispositivi in cui erano installati in precedenza. Tuttavia, tali aggiornamenti non verranno installati in altri dispositivi in futuro.

Se si imposta lo stato *Rifiutato* per gli aggiornamenti software di terze parti, tali aggiornamenti non verranno installati nei dispositivi in cui l'installazione era stata pianificata ma non ancora eseguita. Gli aggiornamenti rimarranno nei dispositivi in cui erano già installati. Se è necessario eliminare gli aggiornamenti, è possibile eliminarli manualmente in locale.

Aggiornamento di Administration Server

È possibile installare gli aggiornamenti di Administration Server utilizzando Aggiornamento guidato di Administration Server.

Per installare un aggiornamento di Administration Server:

1. Nel menu principale, passare a **Operazioni → Applicazioni Kaspersky → Aggiornamenti immediati**.
2. Eseguire l'Aggiornamento guidato di Administration Server in uno dei seguenti modi:
   - Fare clic sul nome di un aggiornamento di Administration Server nell'elenco degli aggiornamenti e, nella finestra visualizzata, fare clic sul collegamento **Esegui Aggiornamento guidato di Administration Server**.
   - Fare clic sul collegamento **Esegui Aggiornamento guidato di Administration Server** nel campo della notifica nella parte superiore della finestra.
3. Nella finestra Aggiornamento guidato di Administration Server selezionare una delle seguenti opzioni per specificare quando installare un aggiornamento:
   - **Installa ora**. Selezionare questa opzione se si desidera installare subito l'aggiornamento.
   - **Rimanda installazione**. Selezionare questa opzione se si desidera installare l'aggiornamento in un secondo momento. In questo caso, verrà visualizzata una notifica in merito all'aggiornamento.
   - **Ignora aggiornamento**. Selezionare questa opzione se non si desidera installare un aggiornamento e non si desidera ricevere notifiche in merito all'aggiornamento.
4. Selezionare l'opzione **Crea una copia di backup di Administration Server prima dell'installazione dell'aggiornamento** se si desidera creare un backup di Administration Server prima di installare l'aggiornamento.
5. Fare clic sul pulsante **OK** per terminare la procedura guidata.

Se il processo di backup viene interrotto, viene interrotto anche il processo di installazione dell'aggiornamento.

Abilitazione e disabilitazione del modello offline per il download degli aggiornamenti

È consigliabile evitare di disabilitare il modello offline per il download degli aggiornamenti. Se viene disabilitato possono verificarsi errori durante l'invio degli aggiornamenti ai dispositivi. In alcuni casi è possibile che uno specialista del Servizio di assistenza tecnica di Kaspersky consigli di disabilitare l'opzione **Scarica aggiornamenti e database anti-virus da Administration Server anticipatamente**. Sarà quindi necessario accertarsi che l'attività per la ricezione degli aggiornamenti per le applicazioni Kaspersky sia stata configurata.

Per abilitare o disabilitare il modello offline per il download degli aggiornamenti per un gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi) → Criteri e profili**.
2. Fare clic su **Gruppi**.
3. Nella struttura dei gruppi di amministrazione selezionare il gruppo di amministrazione per cui è necessario abilitare il modello offline per il download degli aggiornamenti.

4. Fare clic sul criterio di Network Agent.

   Verrà visualizzata la finestra delle proprietà del criterio di Network Agent.

   Per impostazione predefinita, le impostazioni dei criteri secondari sono ereditate dai criteri principali e non possono essere modificate. Se il criterio che si desidera modificare è ereditato, è prima necessario creare un nuovo criterio per Network Agent nel gruppo di amministrazione desiderato. Nel nuovo criterio creato è possibile modificare le impostazioni che non sono bloccate nel criterio principale.

5. Nella scheda **Impostazioni applicazione** selezionare la sezione **Gestire patch e aggiornamenti**.

6. Abilitare o disabilitare l'opzione **Scarica aggiornamenti e database anti-virus da Administration Server anticipatamente (scelta consigliata)** per abilitare o disabilitare il modello offline per il download degli aggiornamenti.

   Per impostazione predefinita, il modello offline per il download degli aggiornamenti è abilitato.

Il modello offline per il download degli aggiornamenti verrà abilitato o disabilitato.

Aggiornamento dei database e dei moduli software Kaspersky nei dispositivi offline

L'aggiornamento dei database e dei moduli software Kaspersky nei dispositivi gestiti è un'attività importante per mantenere la protezione dei dispositivi da virus e altre minacce. Gli amministratori in genere configurano aggiornamenti periodici tramite l'archivio di Administration Server o gli archivi dei punti di distribuzione.

Quando è necessario aggiornare i database e i moduli software in un dispositivo (o un gruppo di dispositivi) che non è connesso all'Administration Server (primario o secondario), a un punto di distribuzione o a Internet, è necessario utilizzare sorgenti degli aggiornamenti alternative, come un server FTP o una cartella locale. In questo caso, è necessario distribuire i file degli aggiornamenti richiesti utilizzando un dispositivo di archiviazione di massa, come un'unità flash o un disco rigido esterno.

È possibile copiare gli aggiornamenti richiesti da:

- Administration Server.

  Per essere certi che l'archivio dell'Administration Server contenga gli aggiornamenti richiesti per l'applicazione di protezione installata in un dispositivo offline, in almeno uno dei dispositivi online gestiti deve essere installata la stessa applicazione di protezione. Questa applicazione deve essere configurata per ricevere gli aggiornamenti dall'archivio di Administration Server tramite l'attività Scarica aggiornamenti nell'archivio dell'Administration Server.

- Qualsiasi dispositivo in cui sia installata e configurata la stessa applicazione di protezione per la ricezione degli aggiornamenti dall'archivio dell'Administration Server, dall'archivio di un punto di distribuzione o direttamente dai server di aggiornamento Kaspersky.

Di seguito è riportato un esempio di configurazione degli aggiornamenti dei database e dei moduli software copiandoli dall'archivio di Administration Server.

Per aggiornare i database e i moduli software Kaspersky nei dispositivi offline:

1. Connettere l'unità rimovibile al dispositivo in cui è installato Administration Server.
2. Copiare i file degli aggiornamenti nell'unità rimovibile.

   Per impostazione predefinita, gli aggiornamenti si trovano in: \\<nome server>\KLSHARE\Updates.

   In alternativa, è possibile configurare Kaspersky Security Center per copiare periodicamente gli aggiornamenti nella cartella selezionata. A tale scopo, utilizzare l'opzione **Copia gli aggiornamenti scaricati in cartelle aggiuntive** nelle proprietà dell'attività Scarica aggiornamenti nell'archivio dell'Administration Server. Se si specifica una cartella posizionata in un'unità flash o un disco rigido esterno come cartella di destinazione per questa opzione, tale dispositivo di archiviazione di massa conterrà sempre la versione più recente degli aggiornamenti.
3. Nei dispositivi offline configurare l'applicazione di protezione (ad esempio, Kaspersky Endpoint Security for Windows) per la ricezione degli aggiornamenti da una cartella locale o una risorsa condivisa, come un server FTP o una cartella condivisa.
4. Copiare i file degli aggiornamenti dall'unità rimovibile nella cartella locale o nella risorsa condivisa che si desidera utilizzare come sorgente degli aggiornamenti.
5. Nel dispositivo offline che richiede l'installazione degli aggiornamenti avviare l'attività di aggiornamento di Kaspersky Endpoint Security for Windows.

Al termine dell'attività di aggiornamento, i database e i moduli software Kaspersky sono aggiornati nel dispositivo.

Backup e ripristino dei plug-in Web

Kaspersky Security Center Web Console consente di eseguire il backup dello stato corrente di un plug-in Web per poter ripristinare lo stato salvato in un secondo momento. È ad esempio possibile eseguire il backup di un plug-in Web prima di eseguirne l'aggiornamento a una versione più recente. Dopo l'aggiornamento, se la versione più recente non soddisfa i requisiti o le aspettative dell'utente, è possibile ripristinare la versione precedente del plug-in Web dal backup.

Per eseguire il backup dei plug-in Web:

1. Nel menu principale accedere a **Impostazioni** → **Plug-in Web**.
2. Nella sezione **Plug-in Web** selezionare i plug-in Web di cui si desidera eseguire il backup, quindi fare clic sul pulsante **Crea copia di backup**.

Viene eseguito il backup dei plug-in Web selezionati. È possibile visualizzare i backup creati nella sezione **Backup**.

Per ripristinare un plug-in Web da un backup:

1. Nel menu principale, passare a **Impostazioni** → **Backup**.
2. Nella sezione **Backup** selezionare il backup del plug-in Web che si desidera ripristinare, quindi fare clic sul pulsante **Ripristina da backup**.

Il plug-in Web viene ripristinato dal backup selezionato.

Regolazione di punti di distribuzione e gateway di connessione

Una struttura di gruppi di amministrazione in Kaspersky Security Center esegue le seguenti funzioni:

- Imposta l'ambito dei criteri

  È disponibile un metodo alternativo per l'applicazione delle impostazioni appropriate nei dispositivi, utilizzando i *profili criterio*. In questo caso, l'ambito dei criteri viene definito con tag, posizioni dei dispositivi nelle unità organizzative di Active Directory o appartenenza a gruppi di protezione di Active Directory.

- Imposta l'ambito delle attività di gruppo

  Esiste un approccio alla definizione dell'ambito delle attività di gruppo che non è basato su una gerarchia di gruppi di amministrazione: l'utilizzo di attività per selezioni dispositivi e di attività per dispositivi specifici.

- Imposta i diritti di accesso a dispositivi, Administration Server virtuali e Administration Server secondari

- Assegna i punti di distribuzione

Al momento della creazione della struttura dei gruppi di amministrazione, è necessario tenere conto della topologia della rete dell'organizzazione per l'assegnazione ottimale dei punti di distribuzione. La distribuzione ottimale dei punti di distribuzione consente di ridurre il traffico nella rete dell'organizzazione.

A seconda dello schema dell'organizzazione e della topologia di rete, le seguenti configurazioni standard possono essere applicate alla struttura dei gruppi di amministrazione:

- Singola sede

- Più sedi remote di piccole dimensioni

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Configurazione standard dei punti di distribuzione: singola sede

In una configurazione standard con una singola sede, tutti i dispositivi si trovano nella rete dell'organizzazione e sono visibili reciprocamente. La rete dell'organizzazione può comprendere diversi componenti (reti o segmenti di rete) connessi tramite canali con larghezza di banda ridotta.

Sono disponibili i seguenti metodi per creare la struttura dei gruppi di amministrazione:

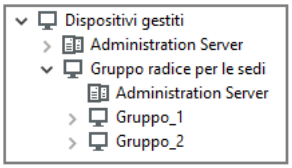
- Creazione della struttura dei gruppi di amministrazione tenendo conto della topologia di rete. La struttura dei gruppi di amministrazione potrebbe non riflettere la topologia di rete alla perfezione. Una corrispondenza tra i diversi componenti della rete e alcuni gruppi di amministrazione può essere sufficiente. È possibile utilizzare l'assegnazione automatica dei punti di distribuzione o assegnarli manualmente.

- Creazione della struttura dei gruppi di amministrazione senza tenere conto della topologia di rete. In questo caso è necessario disabilitare l'assegnazione automatica dei punti di distribuzione e quindi assegnare a uno o più dispositivi il ruolo di punti di distribuzione per un gruppo di amministrazione radice in ciascun componente della rete, ad esempio per il gruppo **Dispositivi gestiti**. Tutti i punti di distribuzione saranno allo stesso livello e avranno lo stesso ambito che comprende tutti i dispositivi della rete dell'organizzazione. In questo caso, tutti i Network Agent si connetteranno al punto di distribuzione con il percorso più vicino. Il percorso di un punto di distribuzione è monitorabile con l'utilità tracert.

Configurazione standard dei punti di distribuzione: più sedi remote di piccole dimensioni

Questa configurazione standard prevede la presenza di diverse sedi remote, che possono comunicare con la sede centrale via Internet. Ogni sede remota è situata dietro il NAT, ovvero la connessione da una sede remota all'altra non è possibile perché le sedi sono isolate tra loro.

La configurazione deve essere riflessa nella struttura dei gruppi di amministrazione: è necessario creare un gruppo di amministrazione distinto per ogni sede remota (i gruppi **Sede 1** e **Sede 2** nella figura seguente).



Le sedi remote sono incluse nella struttura dei gruppi di amministrazione

È necessario assegnare uno o più punti di distribuzione a ogni gruppo di amministrazione che corrisponde a una sede. I punti di distribuzione devono essere dispositivi nella sede remota con una quantità sufficiente di spazio libero su disco. I dispositivi distribuiti nel gruppo **Sede 1**, ad esempio, accederanno ai punti di distribuzione assegnati al gruppo di amministrazione **Sede 1**.

Se alcuni utenti si spostano fisicamente tra le sedi con i loro computer portatili, è necessario selezionare due o più dispositivi (oltre ai punti di distribuzione esistenti) in ogni sede remota e assegnare loro il ruolo di punti di distribuzione per un gruppo di amministrazione di primo livello (**Gruppo radice per le sedi** nella figura precedente).

Esempio: un computer portatile è distribuito nel gruppo di amministrazione **Sede 1** e quindi viene spostato fisicamente nella sede che corrisponde al gruppo di amministrazione **Sede 2**. Dopo lo spostamento del portatile, Network Agent tenta di accedere ai punti di distribuzione assegnati al gruppo **Sede 1**, ma tali punti di distribuzione non sono disponibili. Network Agent inizia quindi a tentare di accedere ai punti di distribuzione che sono stati assegnati al **Gruppo radice per le sedi**. Poiché le sedi remote sono isolate tra loro, i tentativi di accedere ai punti di distribuzione assegnati al gruppo di amministrazione **Gruppo radice per le sedi** avranno esito positivo solo quando Network Agent tenta di accedere ai punti di distribuzione nel gruppo **Sede 2**. In altre parole, il computer portatile rimarrà nel gruppo di amministrazione che corrisponde alla sede iniziale, ma utilizzerà il punto di distribuzione della sede in cui si trova fisicamente al momento.

Informazioni sull'assegnazione dei punti di distribuzione

È possibile assegnare un dispositivo gestito come punto di distribuzione manualmente o automaticamente.

Se si assegna manualmente un dispositivo gestito come punto di distribuzione, è possibile selezionare qualsiasi dispositivo nella rete.

Se si assegnano automaticamente i punti di distribuzione, Kaspersky Security Center può selezionare solo il dispositivo gestito che soddisfa le seguenti condizioni:

- Il dispositivo dispone di almeno 50 GB di spazio disponibile sul disco.
- Il dispositivo gestito è connesso direttamente a Kaspersky Security Center (non tramite il gateway).

- Il dispositivo gestito non è un laptop.

> Se la rete non dispone di dispositivi che soddisfano le condizioni specificate, Kaspersky Security Center non assegnerà automaticamente alcun dispositivo come punto di distribuzione.

Assegnazione automatica di punti di distribuzione

È consigliabile assegnare automaticamente i punti di distribuzione. In questo caso, Kaspersky Security Center selezionerà autonomamente a quali dispositivi assegnare i punti di distribuzione.

Per assegnare automaticamente i punti di distribuzione:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Selezionare l'opzione **Assegna i punti di distribuzione automaticamente**.

   > Se è abilitata l'assegnazione automatica dei dispositivi come punti di distribuzione, non è possibile configurare i punti di distribuzione manualmente, né modificare l'elenco dei punti di distribuzione.

4. Fare clic sul pulsante **Salva**.

Administration Server assegna e configura i punti di distribuzione automaticamente.

Assegnazione manuale di punti di distribuzione

Kaspersky Security Center consente di assegnare manualmente ai dispositivi il ruolo di punti di distribuzione.

È consigliabile assegnare automaticamente i punti di distribuzione. In questo caso, Kaspersky Security Center selezionerà autonomamente a quali dispositivi assegnare i punti di distribuzione. Tuttavia, se per qualche motivo non è possibile assegnare automaticamente i punti di distribuzione (se ad esempio si desidera utilizzare i server assegnati in modo esclusivo), è possibile assegnare i punti di distribuzione manualmente dopo averne calcolato il numero ed eseguito la configurazione.

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Per assegnare manualmente a un dispositivo il ruolo di punto di distribuzione:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Selezionare l'opzione **Assegna i punti di distribuzione manualmente**.

4. Fare clic sul pulsante **Assegna**.

5. Selezionare il dispositivo che si desidera rendere un punto di distribuzione.

   Quando si seleziona un dispositivo, tenere presenti le funzionalità operative dei punti di distribuzione e i requisiti definiti per il dispositivo che opera come punto di distribuzione.

6. Selezionare il gruppo di amministrazione da includere nell'ambito del punto di distribuzione selezionato.

7. Fare clic sul pulsante **OK**.

   Il punto di distribuzione aggiunto sarà visualizzato nell'elenco dei punti di distribuzione, nella sezione **Punti di distribuzione**.

8. Fare clic sul nuovo punto di distribuzione aggiunto nell'elenco per aprire la relativa finestra delle proprietà.

9. Configurare il punto di distribuzione nella finestra delle proprietà:

- La sezione **Generale** contiene le impostazioni per l'interazione tra il punto di distribuzione e i dispositivi client:

  - **Porta SSL**

    Numero della porta SSL per la connessione criptata tra i dispositivi client e il punto di distribuzione tramite SSL.

    Per impostazione predefinita, viene utilizzata la porta 13000.

  - **Usa multicast**

    Se questa opzione è abilitata, verrà utilizzata la modalità IP multicast per la distribuzione automatica dei pacchetti di installazione ai dispositivi client del gruppo.

    Il multicast IP riduce il tempo necessario per installare un'applicazione da un pacchetto di installazione in un gruppo di dispositivi client, ma aumenta il tempo di installazione quando si installa un'applicazione in un singolo dispositivo client.

  - **Indirizzo IP multicast**

    Indirizzo IP che verrà utilizzato per la modalità multicast. È possibile definire un indirizzo IP nell'intervallo da 224.0.0.0 a 239.255.255.255

    Per impostazione predefinita Kaspersky Security Center assegna automaticamente un indirizzo IP multicast univoco all'interno dell'intervallo specificato.

  - **Numero di porta IP multicast**

    Numero di porta per la modalità IP multicast.

    Il numero di porta predefinito è 15001. Se il dispositivo in cui è installato Administration Server è specificato come punto di distribuzione, per impostazione predefinita viene utilizzata la porta 13001 per la connessione SSL.

  - **Indirizzo del punto di distribuzione per i dispositivi remoti**

    L'indirizzo IPv4 attraverso il quale i dispositivi remoti si connettono al punto di distribuzione.

  - **Distribuisci aggiornamenti**

Gli aggiornamenti vengono distribuiti ai dispositivi gestiti dalle seguenti sorgenti:

- Questo punto di distribuzione se l'opzione è abilitata.
- Altri punti di distribuzione, Administration Server o server degli aggiornamenti Kaspersky se l'opzione è disabilitata.

Se si utilizzano i punti di distribuzione per distribuire gli aggiornamenti, è possibile risparmiare traffico riducendo il numero di download. È inoltre possibile alleggerire il carico su Administration Server e ridistribuirlo tra i punti di distribuzione. È possibile calcolare il numero di punti di distribuzione per la propria rete in modo da ottimizzare il traffico e il carico.

Se si disabilita questa opzione, il numero di download degli aggiornamenti e il carico su Administration Server potrebbero aumentare. Per impostazione predefinita, questa opzione è abilitata.

- **Distribuisci pacchetti di installazione**

I pacchetti di installazione vengono distribuiti ai dispositivi gestiti dalle seguenti sorgenti:

- Questo punto di distribuzione se l'opzione è abilitata.
- Altri punti di distribuzione, Administration Server o server degli aggiornamenti Kaspersky se l'opzione è disabilitata.

Se si utilizzano i punti di distribuzione per distribuire i pacchetti di installazione, è possibile risparmiare traffico riducendo il numero di download. È inoltre possibile alleggerire il carico su Administration Server e ridistribuirlo tra i punti di distribuzione. È possibile calcolare il numero di punti di distribuzione per la propria rete in modo da ottimizzare il traffico e il carico.

Se si disabilita questa opzione, il numero di download dei pacchetti di installazione e il carico su Administration Server potrebbero aumentare. Per impostazione predefinita, questa opzione è abilitata.

- **Esegui server push**

In Kaspersky Security Center un punto di distribuzione può fungere da server push per i dispositivi gestiti tramite il protocollo mobile e per i dispositivi gestiti da Network Agent. È ad esempio necessario abilitare un server push se si desidera forzare la sincronizzazione dei dispositivi KasperskyOS con Administration Server. Un server push ha lo stesso ambito dei dispositivi gestiti del punto di distribuzione in cui è abilitato il server push. Se sono stati assegnati più punti di distribuzione per lo stesso gruppo di amministrazione, è possibile abilitare il server push in ciascuno dei punti di distribuzione. In questo caso, Administration Server bilancia il carico tra i punti di distribuzione.

- **Porta server push**

Il numero di porta per il server push. È possibile specificare il numero di qualsiasi porta non occupata.

- Nella sezione **Ambito** specificare l'ambito in cui il punto di distribuzione distribuirà gli aggiornamenti (gruppi di amministrazione e/o percorso di rete).

Solo i dispositivi con un sistema operativo Windows possono determinare il percorso di rete. Non è possibile determinare il percorso di rete per i dispositivi che eseguono altri sistemi operativi.

- Se il punto di distribuzione funziona su un computer diverso da Administration Server, nella sezione **Sorgente degli aggiornamenti** è possibile selezionare una sorgente degli aggiornamenti per il punto di distribuzione:

  - **Sorgente degli aggiornamenti**

    Selezionare una sorgente degli aggiornamenti per il punto di distribuzione:

    - Per consentire al punto di distribuzione di ricevere gli aggiornamenti da Administration Server, selezionare **Recupera da Administration Server**:
    - Per consentire al punto di distribuzione di ricevere gli aggiornamenti tramite un'attività, selezionare **Usa l'attività di download degli aggiornamenti**, quindi specificare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione*:
      - Se tale attività esiste già nel dispositivo, selezionare l'attività nell'elenco.
      - Se tale attività non esiste ancora nel dispositivo, fare clic sul collegamento **Crea attività** per creare un'attività. Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

  - **Scarica file diff**

    Questa opzione consente di abilitare la funzionalità di download dei file diff.

    Per impostazione predefinita, questa opzione è abilitata.

- Se i punti di distribuzione utilizzano un server proxy durante la connessione a Internet, nella sottosezione **Impostazioni connessione Internet** è possibile specificare le seguenti impostazioni:

  - **Usa server proxy**

    Se questa casella di controllo è selezionata, nei campi di immissione è possibile configurare la connessione al server proxy.

    Per impostazione predefinita, questa casella di controllo è deselezionata.

  - **Indirizzo server proxy**

    Indirizzo del server proxy.

  - **Numero di porta**

    Il numero di porta utilizzato per la connessione.

  - **Ignora il server proxy per gli indirizzi locali**

    Se questa opzione è abilitata, non viene utilizzato alcun server proxy per la connessione ai dispositivi nella rete locale.

    Per impostazione predefinita, questa opzione è disabilitata.

- Autenticazione server proxy

  Se questa casella di controllo è selezionata, nei campi di immissione è possibile specificare le credenziali per l'autenticazione del server proxy.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- Nome utente

  Account utente con cui viene stabilita la connessione al server proxy.

- Password

  Password dell'account con cui verrà eseguita l'attività.

- Nella sezione **Proxy KSN** è possibile configurare l'applicazione per l'utilizzo del punto di distribuzione per l'inoltro delle richieste KSN dai dispositivi gestiti:

  - Abilita proxy KSN da parte del punto di distribuzione

    Il servizio proxy KSN viene eseguito nel dispositivo utilizzato come punto di distribuzione. Utilizzare questa funzionalità per ridistribuire e ottimizzare il traffico nella rete.

    Il punto di distribuzione invia le statistiche KSN, elencate nell'informativa di Kaspersky Security Network, a Kaspersky. Per impostazione predefinita, l'informativa KSN è disponibile in %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    Per impostazione predefinita, questa opzione è disabilitata. L'attivazione di questa opzione ha effetto solo se le opzioni **Usa Administration Server come server proxy** e **Accetto di utilizzare Kaspersky Security Network** sono abilitate nella finestra delle proprietà di Administration Server.

    È possibile assegnare il nodo di un cluster attivo-passivo a un punto di distribuzione e abilitare il proxy KSN in tale nodo.

  - Inoltra richieste KSN ad Administration Server

    Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti ad Administration Server.

    Per impostazione predefinita, questa opzione è abilitata.

  - Accedi a KSN Cloud/KPSN direttamente tramite Internet

    Il punto di distribuzione inoltra le richieste KSN dai dispositivi gestiti a KSN Cloud o KPSN. Anche le richieste KSN generate nello stesso punto di distribuzione vengono inviate direttamente a KSN Cloud o KPSN.

    I punti di distribuzione in cui è installato Network Agent versione 11 (o precedente) non possono accedere direttamente a KPSN. Se si desidera riconfigurare i punti di distribuzione per inviare richieste KSN a KPSN, abilitare l'opzione **Inoltra richieste KSN ad Administration Server** per ciascun punto di distribuzione.

    I punti di distribuzione in cui è installato Network Agent versione 12 (o successive) possono accedere direttamente a KPSN.

  - Ignora impostazioni del server proxy durante la connessione a KPSN

Abilitare questa opzione se le impostazioni del server proxy sono configurate nelle proprietà del punto di distribuzione o nel criterio di Network Agent ma l'architettura di rete richiede l'utilizzo diretto di KPSN. In caso contrario, le richieste dalle applicazioni gestite non possono raggiungere KPSN.

Questa opzione è disponibile se si seleziona l'opzione **Accedi a KSN Cloud/KPSN direttamente tramite Internet**.

- **Porta**

  Numero della porta TCP utilizzata dai dispositivi gestiti per la connessione al server proxy KSN. Il numero di porta predefinito è 13111.

- **Usa porta UDP**

  Se è necessario che i dispositivi gestiti si connettano al server proxy KSN attraverso una porta UDP, abilitare l'opzione **Usa porta UDP** e specificare il numero in Porta UDP. Per impostazione predefinita, questa opzione è abilitata.

- **Porta UDP**

  Numero della porta UDP utilizzata dai dispositivi gestiti per la connessione al server proxy KSN. La porta UDP predefinita per la connessione al server proxy KSN è la 15111.

- Se il punto di distribuzione funziona su un computer diverso da Administration Server, nella sezione **Gateway di connessione**, è possibile configurare il punto di distribuzione in modo che funga da gateway per la connessione tra le istanze di Network Agent e Administration Server:

  - **Gateway di connessione**

    Se non è possibile stabilire una connessione diretta tra Administration Server e Network Agent a causa dell'organizzazione della rete, è possibile utilizzare il punto di distribuzione come porta di connessione tra Administration Server e i Network Agent.

    Abilitare questa opzione se è necessario che il punto di distribuzione funga da gateway di connessione tra Network Agent e Administration Server. Per impostazione predefinita, questa opzione è disabilitata.

  - **Stabilisci connessione al gateway da Administration Server (se il gateway è in una rete perimetrale)**

    Se Administration Server si trova al di fuori della zona perimetrale (DMZ), sulla rete locale, i Network Agent installati nei dispositivi remoti non possono connettersi ad Administration Server. È possibile usare un punto di distribuzione come gateway di connessione con connettività inversa (Administration Server stabilisce una connessione al punto di distribuzione).

    Abilitare questa opzione se è necessario connettere Administration Server al gateway di connessione in DMZ.

  - **Apri porta locale per Kaspersky Security Center Web Console**

Abilitare questa opzione se è necessario che il gateway di connessione in DMZ apra una porta per la Web Console che si trova in DMZ o su Internet. Specificare il numero di porta che verrà utilizzato per la connessione da Web Console al punto di distribuzione. Il numero di porta predefinito è 13299.

Questa opzione è disponibile se si abilita l'opzione **Stabilisci connessione al gateway da Administration Server (se il gateway è in una rete perimetrale)**.

Quando i dispositivi mobili vengono connessi ad Administration Server tramite il punto di distribuzione che funge da gateway di connessione, è possibile abilitare le seguenti opzioni:

- **Apri porta per i dispositivi mobili (autenticazione SSL solo di Administration Server)**

  Abilitare questa opzione se è necessario che il gateway di connessione apra una porta per i dispositivi mobili e specificare il numero di porta che i dispositivi mobili utilizzeranno per la connessione al punto di distribuzione. Il numero di porta predefinito è 13292. Il dispositivo mobile controllerà il certificato di Administration Server. Quando si stabilisce la connessione, viene autenticato solo Administration Server.

- **Apri porta per i dispositivi mobili (autenticazione SSL bidirezionale)**

  Abilitare questa opzione se è necessario che il gateway di connessione apra una porta che verrà utilizzata per l'autenticazione bidirezionale di Administration Server e dei dispositivi mobili. Il dispositivo mobile controllerà il certificato di Administration Server e Administration Server controllerà il certificato del dispositivo mobile. Specificare i seguenti parametri:

  - Numero di porta che i dispositivi mobili useranno per la connessione al punto di distribuzione. Il numero di porta predefinito è 13293.
  - Nomi di dominio DNS del gateway di connessione che verranno utilizzati dai dispositivi mobili. Separare i nomi di dominio con virgole. I nomi di dominio specificati verranno inclusi nel certificato del punto di distribuzione. Se i nomi di dominio usati dai dispositivi mobili non corrispondono al nome comune nel certificato del punto di distribuzione, i dispositivi mobili non si connettono al punto di distribuzione.

    Il nome di dominio DNS predefinito è il nome di dominio completo del gateway di connessione.

In entrambi i casi, i certificati vengono verificati quando si stabilisce la sessione TLS solo nel punto di distribuzione. I certificati non vengono inoltrati per la verifica da parte dell'Administration Server. Dopo aver stabilito una sessione TLS con il dispositivo mobile, il punto di distribuzione utilizza il certificato di Administration Server per creare un tunnel per la sincronizzazione tra il dispositivo mobile e Administration Server. Se si apre la porta per l'autenticazione SSL bidirezionale, l'unico modo per distribuire il certificato del dispositivo mobile è tramite un pacchetto di installazione.

- Configurare il polling dei domini Windows, di Active Directory e degli intervalli IP da parte del punto di distribuzione:

  - **Domini Windows**

    È possibile abilitare la device discovery per i domini Windows e impostare la pianificazione per l'individuazione.

  - **Controller di dominio**

È possibile abilitare il polling della rete per Active Directory e impostare la pianificazione per il polling.

Se si utilizza un punto di distribuzione Windows, è possibile selezionare una delle seguenti opzioni:

- **Esegui il polling del dominio Active Directory corrente**.
- **Esegui il polling della foresta di dominio Active Directory**.
- **Esegui il polling dei domini Active Directory selezionati**. Se si seleziona questa opzione, aggiungere uno o più domini Active Directory all'elenco.

Se si utilizza un punto di distribuzione Linux con Network Agent versione 15 installato, è possibile eseguire il polling solo dei domini Active Directory per i quali si specificano l'indirizzo e le credenziali utente. Il polling del dominio Active Directory corrente e della foresta di domini Active Directory non è disponibile.

È possibile abilitare la device discovery per i controller di dominio.

Se si seleziona l'opzione **Abilita polling controller di dominio**, è possibile selezionare i controller di dominio per il polling e anche specificare la pianificazione del polling per gli stessi.

Se si utilizza un punto di distribuzione Linux, nella sezione **Esegui polling di domini specifici**, fare clic su **Aggiungi**, quindi specificare l'indirizzo e le credenziali utente del controller di dominio.

Se si utilizza un punto di distribuzione Windows, è possibile selezionare una delle seguenti opzioni:

- **Esegui polling dominio corrente**
- **Esegui polling di tutta la foresta di dominio**
- **Esegui polling di domini specifici**

- Intervalli IP

Adesso è possibile abilitare Device discovery per gli intervalli IPv4 e le reti IPv6.

Se si abilita l'opzione **Abilita polling intervallo**, è possibile aggiungere gli intervalli esaminati e impostare la relativa pianificazione. È possibile aggiungere intervalli IP all'elenco degli intervalli esaminati.

Se si abilita l'opzione **Usa Zeroconf per il polling delle reti IPv6**, il punto di distribuzione esegue automaticamente il polling della rete IPv6 utilizzando le reti zero-configuration (definite anche *Zeroconf*). In questo caso, gli intervalli IP specificati vengono ignorati perché il punto di distribuzione esegue il polling dell'intera rete. L'opzione **Usa Zeroconf per il polling delle reti IPv6** è disponibile se nel punto di distribuzione viene eseguito Linux. Per utilizzare il polling ipv6 Zeroconf, è necessario installare l'utilità avahi-browse nel punto di distribuzione.

- Nella sezione **Avanzate** specificare la cartella che il punto di distribuzione deve utilizzare per archiviare i dati distribuiti:

- Usa cartella predefinita

Se questa opzione è selezionata, l'applicazione utilizza la cartella di installazione di Network Agent nel punto di distribuzione.

- **Usa cartella specificata**

  Se questa opzione è selezionata, nel campo sottostante è possibile specificare il percorso della cartella. È possibile specificare una cartella locale nel punto di distribuzione oppure una cartella in qualsiasi dispositivo nella rete aziendale.

  L'account utente utilizzato nel punto di distribuzione per eseguire Network Agent deve disporre di accesso in lettura e scrittura alla cartella specificata.

10. Fare clic sul pulsante **OK**.

    I dispositivi selezionati opereranno come punti di distribuzione.

Modifica dell'elenco dei punti di distribuzione per un gruppo di amministrazione

È possibile visualizzare l'elenco dei punti di distribuzione assegnati a un gruppo di amministrazione specifico e modificare l'elenco aggiungendo o rimuovendo punti di distribuzione.

Per visualizzare e modificare l'elenco dei punti di distribuzione assegnati a un gruppo di amministrazione:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Nel campo **Percorso corrente** sopra l'elenco dei dispositivi gestiti, fare clic sul collegamento del percorso.
3. Nel riquadro visualizzato a sinistra, selezionare un gruppo di amministrazione per cui si desidera visualizzare i punti di distribuzione assegnati.

   Viene abilitata la voce di menu **Punti di distribuzione**.
4. Nel menu principale accedere a **Risorse (dispositivi)** → **Punti di distribuzione**.
5. Per aggiungere nuovi punti di distribuzione per il gruppo di amministrazione, fare clic sul pulsante **Assegna** sopra l'elenco dei dispositivi gestiti e selezionare i dispositivi nel riquadro visualizzato.
6. Per rimuovere i punti di distribuzione assegnati, selezionare i dispositivi nell'elenco e fare clic sul pulsante **Annulla assegnazione**.

A seconda delle modifiche, i nuovi punti di distribuzione verranno aggiunti all'elenco o i punti di distribuzione esistenti verranno rimossi dall'elenco.

Sincronizzazione forzata

Sebbene Kaspersky Security Center sincronizzi automaticamente lo stato, le impostazioni, le attività e i criteri per i dispositivi gestiti, in alcuni casi potrebbe essere necessario eseguire la sincronizzazione forzata per un dispositivo specifico. È possibile eseguire la sincronizzazione forzata per i seguenti dispositivi:

- Dispositivi in cui è installato Network Agent
- Dispositivi che eseguono KasperskyOS

  Prima di eseguire la sincronizzazione forzata per un dispositivo KasperskyOS, assicurarsi che il dispositivo sia incluso nell'ambito di un punto di distribuzione e che sia abilitato un server push nel punto di distribuzione.
- Dispositivi iOS
- Dispositivi Android

  Prima di eseguire la sincronizzazione forzata per un dispositivo Android, è necessario configurare Google Firebase Cloud Messaging.

Sincronizzazione di un singolo dispositivo

Per forzare la sincronizzazione tra Administration Server e un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo che si desidera sincronizzare con Administration Server.

   Verrà visualizzata una finestra delle proprietà con la sezione **Generale** selezionata.
3. Fare clic sul pulsante **Forza sincronizzazione**.

L'applicazione sincronizzerà il dispositivo selezionato con Administration Server.

Sincronizzazione di più dispositivi

Per forzare la sincronizzazione tra Administration Server e più dispositivi gestiti:

1. Aprire l'elenco dei dispositivi di un gruppo di amministrazione o una selezione dispositivi:
   - Nel menu principale, passare a **Risorse (dispositivi)** → **Dispositivi gestiti**, fare clic sul collegamento del percorso nel campo **Percorso corrente** sopra l'elenco dei dispositivi gestiti, quindi selezionare il gruppo di amministrazione che contiene i dispositivi da sincronizzare.
   - Eseguire una selezione dei dispositivi per visualizzare l'elenco dei dispositivi.
2. Selezionare le caselle di controllo accanto ai dispositivi che si desidera sincronizzare con Administration Server.

3. Sopra l'elenco dei dispositivi gestiti, fare clic sul pulsante con i puntini di sospensione (...), quindi fare clic sul pulsante **Forza sincronizzazione**.

   L'applicazione sincronizzerà i dispositivi selezionati con Administration Server.

4. Nell'elenco dei dispositivi verificare che per i dispositivi selezionati l'ora dell'ultima connessione ad Administration Server sia cambiata all'ora corrente. Se l'ora non è cambiata, aggiornare il contenuto della pagina facendo clic sul pulsante **Aggiorna**.

I dispositivi selezionati vengono sincronizzati con Administration Server.

Visualizzazione dell'ora di invio di un criterio

Dopo aver modificato un criterio per un'applicazione Kaspersky sull'Administration Server, l'amministratore può verificare se il criterio modificato è stato distribuito a uno specifico dispositivo gestito. Un criterio può essere distribuito durante una sincronizzazione periodica o una sincronizzazione forzata.

Per visualizzare la data e l'ora in cui un criterio dell'applicazione è stato distribuito a un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo che si desidera sincronizzare con Administration Server.

   Verrà visualizzata una finestra delle proprietà con la sezione **Generale** selezionata.

3. Selezionare la scheda **Applicazioni**.
4. Selezionare l'applicazione per cui si desidera visualizzare la data di sincronizzazione del criterio.

   Verrà visualizzata la finestra del criterio dell'applicazione, con la sezione **Generale** selezionata e la data e l'ora di distribuzione del criterio visualizzate.

Abilitazione di un server push

In Kaspersky Security Center un punto di distribuzione può fungere da server push per i dispositivi gestiti tramite il protocollo mobile e per i dispositivi gestiti da Network Agent. È ad esempio necessario abilitare un server push se si desidera forzare la sincronizzazione dei dispositivi KasperskyOS con Administration Server. Un server push ha lo stesso ambito dei dispositivi gestiti del punto di distribuzione in cui è abilitato il server push. Se sono stati assegnati più punti di distribuzione per lo stesso gruppo di amministrazione, è possibile abilitare il server push in ciascuno dei punti di distribuzione. In questo caso, Administration Server bilancia il carico tra i punti di distribuzione.

È consigliabile utilizzare i punti di distribuzione come server push per garantire la continuità della connessione tra un dispositivo gestito e Administration Server. La continuità della connessione è necessaria per alcune operazioni, come l'esecuzione e l'arresto di attività locali, la ricezione di statistiche per un'applicazione gestita o la creazione di un tunnel. Se si utilizza un punto di distribuzione come server push, non è necessario utilizzare l'opzione **Non eseguire la disconnessione da Administration Server** nei dispositivi gestiti o inviare pacchetti alla porta UDP di Network Agent.

Un server push supporta il carico massimo di 50.000 connessioni simultanee.

Per abilitare il server push in un punto di distribuzione:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Punti di distribuzione**.

3. Fare clic sul nome del punto di distribuzione in cui si desidera abilitare il server push.

   Verrà visualizzata la finestra delle proprietà del punto di distribuzione.

4. Nella sezione **Generale** abilitare l'opzione **Esegui server push**.

5. Nel campo **Porta server push** digitare il numero di porta. È possibile specificare il numero di qualsiasi porta non occupata.

6. Nel campo **Indirizzo per host remoti** specificare l'indirizzo IP o il nome del dispositivo del punto di distribuzione.

7. Fare clic sul pulsante **OK**.

Il server push è abilitato nel punto di distribuzione selezionato.

Gestione delle applicazioni di terzi nei dispositivi client

Questa sezione descrive le funzionalità di Kaspersky Security Center correlate alla gestione delle applicazioni di terze parti installate nei dispositivi client.

Installazione degli aggiornamenti software di terze parti

Kaspersky Security Center consente di gestire gli aggiornamenti del software di terze parti installato nei dispositivi gestiti e di correggere le vulnerabilità delle applicazioni Microsoft e di altri produttori di software tramite l'installazione degli aggiornamenti richiesti.

Kaspersky Security Center cerca gli aggiornamenti tramite l'attività *Trova vulnerabilità e aggiornamenti richiesti*. Al termine di questa attività, Administration Server riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi specificati nelle proprietà dell'attività. Dopo avere visualizzato le informazioni sugli aggiornamenti disponibili, è possibile installarli nei dispositivi.

Kaspersky Security Center aggiorna alcune applicazioni rimuovendo la versione precedente dell'applicazione e installando la nuova.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Per motivi di sicurezza, tutti gli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management vengono automaticamente analizzati alla ricerca di malware dalle tecnologie Kaspersky. Queste tecnologie vengono utilizzate per il controllo automatico dei file e includono la scansione virus, l'analisi statica, l'analisi dinamica, l'analisi del comportamento nell'ambiente sandbox e il machine learning.

Gli esperti Kaspersky non eseguono l'analisi manuale degli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management. Inoltre, gli esperti di Kaspersky non ricercano vulnerabilità (note o sconosciute) o funzionalità non documentate in tali aggiornamenti, né eseguono altri tipi di analisi degli aggiornamenti diversi da quelli specificati nel paragrafo precedente.

Attività per l'installazione degli aggiornamenti software di terze parti

Quando i metadati degli aggiornamenti software di terze parti vengono scaricati nell'archivio, è possibile installare gli aggiornamenti nei dispositivi client utilizzando le seguenti attività:

- L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*

  L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per installare gli aggiornamenti per le applicazioni Microsoft, inclusi gli aggiornamenti forniti dal servizio Windows Update, e gli aggiornamenti del software di altri produttori. Questa attività può essere creata solo se si dispone della licenza per la funzionalità Vulnerability e patch management.

  Al termine di questa attività, gli aggiornamenti vengono installati automaticamente nei dispositivi gestiti. Quando i metadati dei nuovi aggiornamenti vengono scaricati nell'archivio dell'Administration Server, Kaspersky Security Center verifica se gli aggiornamenti soddisfano i criteri specificati nelle regole per gli aggiornamenti. Tutti i nuovi aggiornamenti che soddisfano i criteri verranno scaricati e installati automaticamente alla successiva esecuzione dell'attività.

- L'attività *Installa aggiornamenti di Windows Update*

  L'attività *Installa aggiornamenti di Windows Update* non richiede una licenza, ma può essere utilizzata per installare solo gli aggiornamenti di Windows Update.

  Al termine di questa attività, vengono installati solo gli aggiornamenti specificati nelle proprietà dell'attività. Se in seguito si desidera installare i nuovi aggiornamenti scaricati nell'archivio dell'Administration Server, è necessario aggiungere gli aggiornamenti richiesti all'elenco degli aggiornamenti nell'attività esistente o creare una nuova attività Installa aggiornamenti di Windows Update.

Utilizzo di Administration Server come server WSUS

Le informazioni sugli aggiornamenti disponibili per Microsoft Windows sono fornite dal servizio Windows Update. Administration Server può essere utilizzato come server WSUS (Windows Server Update Services). Per utilizzare Administration Server come server WSUS, creare l'attività Esegui sincronizzazione di Windows Update e selezionare l'opzione **Usa Administration Server come server WSUS** nel criterio di Network Agent. Dopo avere configurato la sincronizzazione dei dati con Windows Update, Administration Server fornisce gli aggiornamenti ai servizi Windows Update nei dispositivi in modalità centralizzata e in base alla frequenza impostata.

Scenario: Aggiornamento di software di terze parti

Questa sezione fornisce uno scenario per l'aggiornamento del software di terze parti installato nei dispositivi client. Il software di terze parti include le applicazioni Microsoft e di altri fornitori di software. Gli aggiornamenti per le applicazioni Microsoft sono forniti dal servizio Windows Update.

Prerequisiti

Administration Server deve disporre di una connessione a Internet per installare gli aggiornamenti di software di terze parti diverso dal software Microsoft.

Per impostazione predefinita, non è richiesta la connessione Internet per l'installazione degli aggiornamenti software Microsoft nei dispositivi gestiti da parte di Administration Server. I dispositivi gestiti possono ad esempio scaricare gli aggiornamenti software Microsoft direttamente dai server Microsoft Update o da Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione. Administration Server deve essere connesso a Internet quando si utilizza Administration Server come server WSUS.

Passaggi

L'aggiornamento del software di terze parti prevede diversi passaggi:

1. **Ricerca degli aggiornamenti richiesti**

   Per trovare gli aggiornamenti software di terze parti richiesti per i dispositivi gestiti, eseguire l'attività *Trova vulnerabilità e aggiornamenti richiesti*. Al termine di questa attività, Kaspersky Security Center riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi specificati nelle proprietà dell'attività.

   L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente dall'Avvio rapido guidato di Administration Server. Se non è stata eseguita la procedura guidata, creare l'attività o eseguire l'Avvio rapido guidato.

   Istruzioni dettagliate:

   - Administration Console: Scansione delle applicazioni per rilevare la presenza di vulnerabilità, Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
   - Kaspersky Security Center Web Console: Creazione dell'attività Trova vulnerabilità e aggiornamenti richiesti, Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

2. **Analisi dell'elenco degli aggiornamenti rilevati**

   Visualizzare l'elenco **Aggiornamenti software** e decidere quali aggiornamenti si desidera installare. Per visualizzare informazioni dettagliate su ciascun aggiornamento, fare clic sul nome dell'aggiornamento nell'elenco. Per ogni aggiornamento nell'elenco, è anche possibile visualizzare le statistiche sull'installazione dell'aggiornamento nei dispositivi client.

   Istruzioni dettagliate:

   - Administration Console: Visualizzazione delle informazioni sugli aggiornamenti disponibili
   - Kaspersky Security Center Web Console: Visualizzazione delle informazioni sugli aggiornamenti software di terze parti disponibili

3. **Configurazione dell'installazione degli aggiornamenti**

   Quando Kaspersky Security Center ha ricevuto l'elenco degli aggiornamenti software di terze parti, è possibile installarli nei dispositivi client utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Installa aggiornamenti di Windows Update*. Creare una di queste attività. È possibile creare queste attività nella scheda **Attività** o utilizzando l'elenco **Aggiornamenti software**.

   L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per installare gli aggiornamenti per le applicazioni Microsoft, inclusi gli aggiornamenti forniti dal servizio Windows Update, e gli aggiornamenti del software di altri produttori. Questa attività può essere creata solo se si dispone della licenza per la funzionalità Vulnerability e patch management.

L'attività *Installa aggiornamenti di Windows Update* non richiede una licenza, ma può essere utilizzata per installare solo gli aggiornamenti di Windows Update.

Per installare alcuni aggiornamenti software, è necessario accettare il Contratto di licenza con l'utente finale (EULA) per il software da installare. Se non si accetta il Contratto di licenza con l'utente finale, l'aggiornamento software non verrà installato.

È possibile avviare un'attività di installazione degli aggiornamenti in base a una pianificazione. Quando si specifica la pianificazione dell'attività, assicurarsi che l'attività di installazione degli aggiornamenti venga avviata dopo il completamento dell'attività *Trova vulnerabilità e aggiornamenti richiesti*.

Istruzioni dettagliate:

- Administration Console: Correzione delle vulnerabilità delle applicazioni, Visualizzazione delle informazioni sugli aggiornamenti disponibili
- Kaspersky Security Center Web Console: Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità, Creazione dell'attività Installa aggiornamenti di Windows Update, Visualizzazione delle informazioni sugli aggiornamenti software di terze parti disponibili

4 Pianificazione delle attività

Per assicurarsi che l'elenco degli aggiornamenti sia sempre aggiornato, pianificare l'attività *Trova vulnerabilità e aggiornamenti richiesti* affinché venga eseguita periodicamente in modo automatico. Per impostazione predefinita, l'attività *Trova vulnerabilità e aggiornamenti richiesti* è impostata per l'avvio manuale.

Se è stata creata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile pianificarla in modo che venga eseguita con la stessa frequenza dell'attività *Trova vulnerabilità e aggiornamenti richiesti* o con una frequenza inferiore. Quando si pianifica l'attività *Installa aggiornamenti di Windows Update*, tenere presente che per questa attività è necessario definire l'elenco degli aggiornamenti ogni volta prima di avviare l'attività.

Durante la pianificazione delle attività, assicurarsi che un'attività di installazione degli aggiornamenti venga avviata dopo il completamento dell'attività *Trova vulnerabilità e aggiornamenti richiesti*.

5 Approvazione e rifiuto degli aggiornamenti software (facoltativo)

Se è stata creata l'attività Installa aggiornamenti richiesti e correggi vulnerabilità, è possibile specificare le regole per l'installazione degli aggiornamenti nelle proprietà dell'attività. Se è stata creata l'attività Installa aggiornamenti di Windows Update, ignorare questo passaggio.

Per ciascuna regola, è possibile definire gli aggiornamenti da installare in base allo stato dell'aggiornamento: *Indefinito*, *Approvato* o *Rifiutato*. Ad esempio, è possibile creare un'attività specifica per i server e impostare una regola per questa attività in modo da consentire l'installazione solo degli aggiornamenti di Windows Update e solo di quelli con stato *Approvato*. Successivamente, si imposta manualmente lo stato *Approvato* per gli aggiornamenti da installare. In questo caso, gli aggiornamenti di Windows Update con stato *Indefinito* o *Rifiutato* non verranno installati nei server specificati nell'attività.

L'utilizzo dello stato *Approvato* per gestire l'installazione degli aggiornamenti è efficace per una piccola quantità di aggiornamenti. Per installare più aggiornamenti, utilizzare le regole che è possibile configurare nell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. È consigliabile impostare lo stato *Approvato* solo per gli aggiornamenti specifici che non soddisfano i criteri specificati nelle regole. Quando si approva manualmente una grande quantità di aggiornamenti, le prestazioni di Administration Server si riducono e questo può causare un sovraccarico di Administration Server.

Per impostazione predefinita, gli aggiornamenti software scaricati hanno lo stato *Indefinito*. È possibile modificare lo stato in *Approvato* o *Rifiutato* nell'elenco **Aggiornamenti software** (**Operazioni → Gestione patch → Aggiornamenti software**).

Istruzioni dettagliate:

- Administration Console: Approvazione e rifiuto degli aggiornamenti software
- Kaspersky Security Center Web Console: Approvazione e rifiuto degli aggiornamenti software di terze parti

6. **Configurazione di Administration Server per operare come server WSUS (Windows Server Update Services) (facoltativo)**

   Per impostazione predefinita, gli aggiornamenti di Windows Update vengono scaricati nei dispositivi gestiti dai server Microsoft. È possibile modificare questa impostazione per utilizzare Administration Server come server WSUS. In questo caso, Administration Server sincronizza i dati sugli aggiornamenti con Windows Update con la frequenza specificata e fornisce gli aggiornamenti in modalità centralizzata a Windows Update nei dispositivi nella rete.

   Per utilizzare Administration Server come server WSUS, creare l'attività Esegui sincronizzazione di Windows Update e selezionare la casella di controllo **Usa Administration Server come server WSUS** nel criterio di Network Agent.

   Istruzioni dettagliate:

   - Administration Console: Sincronizzazione degli aggiornamenti da Windows Update con Administration Server, Configurazione degli aggiornamenti di Windows in un criterio di Network Agent
   - Kaspersky Security Center Web Console: Creazione dell'attività Esegui sincronizzazione di Windows Update

7. **Esecuzione di un'attività di installazione degli aggiornamenti**

   Avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Installa aggiornamenti di Windows Update*. Quando si avviano queste attività, gli aggiornamenti vengono scaricati e installati nei dispositivi gestiti. Al termine dell'attività, assicurarsi che questa abbia lo stato *Completato* nell'elenco attività.

8. **Creare il rapporto sui risultati dell'installazione degli aggiornamenti del software di terze parti (facoltativo)**

   Per visualizzare le statistiche dettagliate sull'installazione degli aggiornamenti, creare il **Rapporto sui risultati dell'installazione degli aggiornamenti software di terze parti**.

   Istruzioni dettagliate:

   - Administration Console: Creazione e visualizzazione di un rapporto
   - Kaspersky Security Center Web Console: Generazione e visualizzazione di un rapporto

Risultati

Se è stata creata e configurata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, gli aggiornamenti vengono installati automaticamente nei dispositivi gestiti. Quando i nuovi aggiornamenti vengono scaricati nell'archivio dell'Administration Server, Kaspersky Security Center verifica se soddisfano i criteri specificati nelle regole per gli aggiornamenti. Tutti i nuovi aggiornamenti che soddisfano i criteri verranno installati automaticamente alla successiva esecuzione dell'attività.

Se è stata creata l'attività *Installa aggiornamenti di Windows Update*, vengono installati solo gli aggiornamenti specificati nelle proprietà dell'attività *Installa aggiornamenti di Windows Update*. Se in seguito si desidera installare i nuovi aggiornamenti scaricati nell'archivio dell'Administration Server, è necessario aggiungere gli aggiornamenti richiesti all'elenco degli aggiornamenti nell'attività esistente o creare una nuova attività *Installa aggiornamenti di Windows Update*.

Installazione degli aggiornamenti software di terze parti

È possibile installare gli aggiornamenti software di terze parti nei dispositivi gestiti creando ed eseguendo una delle seguenti attività:

- *Installa aggiornamenti richiesti e correggi vulnerabilità*

  L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* può essere creata solo se si dispone di una licenza per la funzionalità Vulnerability e patch management. È possibile utilizzare questa attività per installare sia gli aggiornamenti di Windows Update forniti da Microsoft sia gli aggiornamenti del software di altri fornitori.

- *Installa aggiornamenti di Windows Update*

  È possibile utilizzare l'attività *Installa aggiornamenti di Windows Update* solo per installare gli aggiornamenti di Windows Update.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Facoltativamente, è possibile creare un'attività per installare gli aggiornamenti richiesti nei seguenti modi:

- Aprendo l'elenco degli aggiornamenti e specificando quali aggiornamenti installare.

  Verrà creata una nuova attività per l'installazione degli aggiornamenti selezionati. Facoltativamente è possibile aggiungere gli aggiornamenti selezionati a un'attività esistente.

- Eseguendo l'Installazione guidata aggiornamenti.

  L'Installazione guidata aggiornamenti è disponibile solo con la licenza per Vulnerability e patch management.

  La procedura guidata semplifica la creazione e la configurazione di un'attività di installazione degli aggiornamenti e consente di eliminare la creazione di attività ridondanti che contengono gli stessi aggiornamenti da installare.

Installazione degli aggiornamenti software di terze parti tramite l'elenco degli aggiornamenti

Per installare aggiornamenti software di terze parti utilizzando l'elenco degli aggiornamenti:

1. Aprire uno degli elenchi di aggiornamenti:

   - Per aprire l'elenco generale degli aggiornamenti nel menu principale, passare a **Operazioni → Gestione patch → Aggiornamenti software**.
   - Per aprire l'elenco degli aggiornamenti per un dispositivo gestito nel menu principale, passare a **Risorse (dispositivi) → Dispositivi gestiti →** <nome dispositivo> **→ Avanzate → Aggiornamenti disponibili**.
   - Per aprire l'elenco degli aggiornamenti per un'applicazione specifica nel menu principale, passare a **Operazioni → Applicazioni di terze parti → Registro delle applicazioni →** <nome applicazione> **→ Aggiornamenti disponibili**.

   Verrà visualizzato un elenco degli aggiornamenti disponibili.

2. Selezionare le caselle di controllo accanto agli aggiornamenti che si desidera installare.

3. Fare clic sul pulsante **Installa aggiornamenti**.

   Per installare alcuni aggiornamenti software, è necessario accettare il Contratto di licenza con l'utente finale (EULA). Se non si accetta il Contratto di licenza con l'utente finale, l'aggiornamento software non viene installato.

4. Selezionare una delle seguenti opzioni:

   - **Nuova attività**

     Verrà avviata la Creazione guidata nuova attività. Se si dispone della licenza Vulnerability e patch management, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* è pre-selezionata. Se non si dispone della licenza, l'attività *Installa aggiornamenti di Windows Update* è preselezionata. Seguire i passaggi della procedura guidata per completare la creazione dell'attività.

   - **Installa aggiornamento (aggiungi regola all'attività specificata)**

     Selezionare un'attività a cui aggiungere gli aggiornamenti selezionati. Se si dispone della licenza Vulnerability e patch management, selezionare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. Una nuova regola per installare gli aggiornamenti selezionati verrà automaticamente aggiunta all'attività selezionata. Se non si dispone della licenza, selezionare l'attività *Installa aggiornamenti di Windows Update*. Gli aggiornamenti selezionati verranno aggiunti alle proprietà dell'attività.

     Verrà visualizzata la finestra delle proprietà dell'attività. Fare clic sul pulsante **Salva** per applicare le modifiche.

   Se si è scelto di creare un'attività, l'attività viene creata e visualizzata nell'elenco delle attività in **Risorse (dispositivi) → Attività**. Se si è scelto di aggiungere gli aggiornamenti a un'attività esistente, gli aggiornamenti vengono salvati nelle proprietà dell'attività.

Per installare gli aggiornamenti software di terze parti, avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Installa aggiornamenti di Windows Update*. È possibile avviare queste attività manualmente o specificare le impostazioni di pianificazione nelle proprietà dell'attività avviata. Quando si specifica la pianificazione dell'attività, assicurarsi che l'attività di installazione degli aggiornamenti venga avviata dopo il completamento dell'attività *Trova vulnerabilità e aggiornamenti richiesti*.

Installazione degli aggiornamenti software di terze parti tramite l'Installazione guidata aggiornamenti

L'Installazione guidata aggiornamenti è disponibile solo con la licenza per Vulnerability e patch management.

Per creare un'attività per l'installazione degli aggiornamenti software di terze parti utilizzando l'Installazione guidata aggiornamenti:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Aggiornamenti software**.

   Verrà visualizzato un elenco degli aggiornamenti disponibili.

2. Selezionare la casella di controllo accanto all'aggiornamento che si desidera installare.

3. Fare clic sul pulsante **Esegui Installazione guidata aggiornamenti**.

   Verrà avviata l'Installazione guidata aggiornamenti. La pagina **Selezionare un'attività per l'installazione dell'aggiornamento** visualizza l'elenco di tutte le attività esistenti dei seguenti tipi:

   - *Installa aggiornamenti richiesti e correggi vulnerabilità*
   - *Installa aggiornamenti di Windows Update*
   - *Correggi vulnerabilità*

   Non è possibile modificare le attività degli ultimi due tipi per installare nuovi aggiornamenti. Per installare nuovi aggiornamenti, è possibile utilizzare solo le attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.

4. Se si desidera che la procedura guidata visualizzi solo le attività per l'installazione dell'aggiornamento selezionato, abilitare l'opzione **Mostra solo le attività che consentono di installare l'aggiornamento**.

5. Scegliere l'operazione da eseguire:

   - Per avviare un'attività, selezionare la casella di controllo accanto al nome dell'attività, quindi fare clic sul pulsante **Avvia**.

   - Per aggiungere una nuova regola a un'attività esistente:

     a. Selezionare la casella di controllo accanto al nome dell'attività, quindi fare clic sul pulsante **Aggiungi regola**.

     b. Nella pagina visualizzata configurare la nuova regola:

     - Regola di installazione per gli aggiornamenti di questo livello di importanza

       Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

       Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore alla criticità dell'aggiornamento selezionato (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

       Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

       Per impostazione predefinita, questa opzione è disabilitata.

     - Regola di installazione per gli aggiornamenti di questo livello di importanza in base a MSRC

       Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

       Se questa opzione è abilitata (disponibile solo per gli aggiornamenti di Windows Update), gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Microsoft Security Response Center (MSRC) è uguale o superiore al valore selezionato nell'elenco (**Basso**, **Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

       Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

       Per impostazione predefinita, questa opzione è disabilitata.

     - Regola di installazione per gli aggiornamenti in base a questo produttore

       Questa opzione è disponibile solo per gli aggiornamenti di applicazioni di terze parti. Kaspersky Security Center installa solo gli aggiornamenti relativi alle applicazioni sviluppate dallo stesso produttore dell'aggiornamento selezionato. Gli aggiornamenti rifiutati e gli aggiornamenti per le applicazioni sviluppate da altri produttori non vengono installati.

       Per impostazione predefinita, questa opzione è disabilitata.

     - **Regola di installazione per gli aggiornamenti del tipo**

- **Regola di installazione per l'aggiornamento selezionato**
- **Approvare gli aggiornamenti selezionati**

  L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Installa automaticamente tutti gli aggiornamenti precedenti dell'applicazione necessari per l'installazione degli aggiornamenti selezionati**

  Mantenere abilitata questa opzione se si desidera consentire l'installazione delle versioni intermedie delle applicazioni quando questa operazione è necessaria per l'installazione degli aggiornamenti selezionati.

  Se questa opzione è disabilitata, vengono installate solo le versioni delle applicazioni selezionate. Disabilitare questa opzione se si desidera aggiornare le applicazioni in modo diretto, senza tentare di installare le versioni successive in modo incrementale. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

  Si supponga di avere la versione 3 di un'applicazione installata in un dispositivo e di voler eseguire l'aggiornamento alla versione 5, ma la versione 5 di questa applicazione può essere installata solo sulla versione 4. Se questa opzione è abilitata, il software installa prima la versione 4 e quindi la versione 5. Se questa opzione è disabilitata, il software non riesce a eseguire l'aggiornamento l'applicazione.

  Per impostazione predefinita, questa opzione è abilitata.

c. Fare clic sul pulsante **Aggiungi**.

- Per creare un'attività:

  a. Fare clic sul pulsante **Nuova attività**.

  b. Nella pagina visualizzata configurare la nuova regola:

  - **Regola di installazione per gli aggiornamenti di questo livello di importanza**

    Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

    Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore alla criticità dell'aggiornamento selezionato (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

    Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Regola di installazione per gli aggiornamenti di questo livello di importanza in base a MSRC**

Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

Se questa opzione è abilitata (disponibile solo per gli aggiornamenti di Windows Update), gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Microsoft Security Response Center (MSRC) è uguale o superiore al valore selezionato nell'elenco (**Basso**, **Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

Per impostazione predefinita, questa opzione è disabilitata.

- Regola di installazione per gli aggiornamenti in base a questo produttore

  Questa opzione è disponibile solo per gli aggiornamenti di applicazioni di terze parti. Kaspersky Security Center installa solo gli aggiornamenti relativi alle applicazioni sviluppate dallo stesso produttore dell'aggiornamento selezionato. Gli aggiornamenti rifiutati e gli aggiornamenti per le applicazioni sviluppate da altri produttori non vengono installati.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Regola di installazione per gli aggiornamenti del tipo**

- **Regola di installazione per l'aggiornamento selezionato**

- Approvare gli aggiornamenti selezionati

  L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

  Per impostazione predefinita, questa opzione è disabilitata.

- Installa automaticamente tutti gli aggiornamenti precedenti dell'applicazione necessari per l'installazione degli aggiornamenti selezionati

  Mantenere abilitata questa opzione se si desidera consentire l'installazione delle versioni intermedie delle applicazioni quando questa operazione è necessaria per l'installazione degli aggiornamenti selezionati.

  Se questa opzione è disabilitata, vengono installate solo le versioni delle applicazioni selezionate. Disabilitare questa opzione se si desidera aggiornare le applicazioni in modo diretto, senza tentare di installare le versioni successive in modo incrementale. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

  Si supponga di avere la versione 3 di un'applicazione installata in un dispositivo e di voler eseguire l'aggiornamento alla versione 5, ma la versione 5 di questa applicazione può essere installata solo sulla versione 4. Se questa opzione è abilitata, il software installa prima la versione 4 e quindi la versione 5. Se questa opzione è disabilitata, il software non riesce a eseguire l'aggiornamento l'applicazione.

  Per impostazione predefinita, questa opzione è abilitata.

c. Fare clic sul pulsante **Aggiungi**.

Se è stato scelto di avviare un'attività, è possibile chiudere la procedura guidata. L'attività verrà completata in background. Non sono necessarie ulteriori operazioni.

Se si è scelto di aggiungere una regola a un'attività esistente, verrà visualizzata la finestra delle proprietà dell'attività. La nuova regola è già stata aggiunta alle proprietà dell'attività. È possibile visualizzare o modificare la regola o altre impostazioni dell'attività. Fare clic sul pulsante **Salva** per applicare le modifiche.

Se è stato scelto di creare un'attività, continuare a creare l'attività nella Creazione guidata nuova attività. La nuova regola aggiunta nell'Installazione guidata aggiornamenti viene visualizzata nella Creazione guidata nuova attività. Al termine della procedura guidata, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* verrà aggiunta all'elenco delle attività.

Creazione dell'attività Trova vulnerabilità e aggiornamenti richiesti

Tramite l'attività Trova vulnerabilità e aggiornamenti richiesti, Kaspersky Security Center riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi gestiti.

L'attività Trova vulnerabilità e aggiornamenti richiesti viene creata automaticamente durante l'esecuzione dell'Avvio rapido guidato. Se la procedura guidata non è stata eseguita, è possibile creare l'attività manualmente.

Per creare l'attività Trova vulnerabilità e aggiornamenti richiesti:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Trova vulnerabilità e aggiornamenti richiesti**.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare i dispositivi a cui assegnare l'attività.
6. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.
7. Fare clic sul pulsante **Crea**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.
8. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.
9. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività.

10. Nella scheda **Impostazioni applicazione** specificare le seguenti impostazioni:

- **Cerca vulnerabilità e aggiornamenti elencati da Microsoft**

  Durante la ricerca di vulnerabilità e aggiornamenti, Kaspersky Security Center utilizza le informazioni sugli aggiornamenti Microsoft applicabili della sorgente degli aggiornamenti di Microsoft e disponibili al momento.

  È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft e gli aggiornamenti delle applicazioni di terze parti.

  Per impostazione predefinita, questa opzione è abilitata.

  Le informazioni sugli aggiornamenti facoltativi di Microsoft Windows non vengono inviate ad Administration Server.

- **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati**

Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft. I seguenti server possono operare come sorgente degli aggiornamenti Microsoft:

- Kaspersky Security Center Administration Server (vedere le impostazioni del criterio di Network Agent)
- Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione
- Server degli aggiornamenti Microsoft

Se questa opzione è abilitata, Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft per aggiornare le informazioni sugli aggiornamenti di Microsoft Windows applicabili.

Se questa opzione è disabilitata, l'Agente di Windows Update in un dispositivo gestito utilizza le informazioni sugli aggiornamenti di Microsoft Windows applicabili ricevuti dalla sorgente degli aggiornamenti Microsoft in precedenza.

La connessione alla sorgente degli aggiornamenti Microsoft può comportare un notevole utilizzo di risorse. Potrebbe essere necessario disabilitare questa opzione se è stata impostata una connessione standard a questa sorgente degli aggiornamenti in un'altra attività o nelle proprietà del criterio Network Agent, nella sezione **Vulnerabilità e aggiornamenti software**. Se non si desidera disabilitare questa opzione, per ridurre l'overload del Server è possibile configurare la pianificazione delle attività in modo da utilizzare il ritardo casuale per l'avvio delle attività entro 360 minuti.

Per impostazione predefinita, questa opzione è abilitata.

La combinazione delle seguenti opzioni delle impostazioni del criterio di Network Agent definisce il modo in cui si ottengono gli aggiornamenti:

- In un dispositivo gestito, l'Agente di Windows Update si connette al server degli aggiornamenti per ottenere gli aggiornamenti solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è abilitata nelle proprietà dell'attività *Trova vulnerabilità e aggiornamenti richiesti* e l'opzione **Modalità di ricerca di Windows Update** è impostata su **Attiva** nelle impostazioni del criterio di Network Agent.
- Se non è necessario che Network Agent avvii una connessione alla sorgente degli aggiornamenti di Microsoft Windows e scarichi gli aggiornamenti durante l'esecuzione dell'attività *Scansione vulnerabilità*, è possibile impostare l'opzione **Modalità di ricerca di Windows Update** su **Passiva**, mentre l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** deve rimanere abilitata. In questo modo, è possibile risparmiare risorse e utilizzare gli aggiornamenti di Windows ricevuti in precedenza per la scansione delle vulnerabilità. È possibile utilizzare la modalità passiva se si configura la ricezione degli aggiornamenti DI Microsoft Windows in modo diverso. Se la ricezione degli aggiornamenti di Microsoft Windows non è configurata in altro modo, non impostare l'opzione **Modalità di ricerca di Windows Update** su **Passiva**, poiché in questo caso non si riceveranno le informazioni sugli aggiornamenti, in alcun caso.
- Indipendentemente dallo stato dell'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** (abilitata o disabilitata), se l'opzione **Modalità di ricerca di Windows Update** è impostata su **Disabilitata**, Kaspersky Security Center non richiede informazioni sugli aggiornamenti.

- Cerca vulnerabilità e aggiornamenti di terze parti elencati da Kaspersky

Se questa opzione è abilitata, Kaspersky Security Center esegue la ricerca delle vulnerabilità e degli aggiornamenti richiesti per le applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) nel Registro di sistema di Windows e nelle cartelle specificate con **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**. L'elenco completo delle applicazioni di terze parti supportate è gestito da Kaspersky.

Se questa opzione è disabilitata, Kaspersky Security Center non esegue la ricerca di vulnerabilità e aggiornamenti richiesti per le applicazioni di terze parti. È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft Windows e gli aggiornamenti delle applicazioni di terze parti.

Per impostazione predefinita, questa opzione è abilitata.

- **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**

  Cartelle in cui Kaspersky Security Center esegue la ricerca delle applicazioni di terze parti che richiedono la correzione delle vulnerabilità e l'installazione di aggiornamenti. È possibile utilizzare le variabili di sistema.

  Specificare le cartelle in cui sono installate le applicazioni. Per impostazione predefinita, l'elenco contiene le cartelle di sistema in cui viene installata la maggior parte delle applicazioni.

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive i file di traccia anche se la scrittura dei file di traccia è disabilitata per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

11. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Se i risultati dell'attività contengono l'avviso 0x80240033 "Errore di Windows Update Agent 80240033 ("Non è stato possibile scaricare le condizioni di licenza")", è possibile risolvere questo problema tramite il Registro di sistema di Windows.

Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente durante l'esecuzione dell'Avvio rapido guidato. Se la procedura guidata non è stata eseguita, è possibile creare l'attività manualmente.

Oltre alle impostazioni generali delle attività, è possibile specificare le seguenti impostazioni durante la creazione dell'attività *Trova vulnerabilità e aggiornamenti richiesti* o in un secondo momento, quando si configurano le proprietà dell'attività creata:

- **Cerca vulnerabilità e aggiornamenti elencati da Microsoft**

  Durante la ricerca di vulnerabilità e aggiornamenti, Kaspersky Security Center utilizza le informazioni sugli aggiornamenti Microsoft applicabili della sorgente degli aggiornamenti di Microsoft e disponibili al momento.

  È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft e gli aggiornamenti delle applicazioni di terze parti.

  Per impostazione predefinita, questa opzione è abilitata.

  Le informazioni sugli aggiornamenti facoltativi di Microsoft Windows non vengono inviate ad Administration Server.

- **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati**

Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft. I seguenti server possono operare come sorgente degli aggiornamenti Microsoft:

- Kaspersky Security Center Administration Server (vedere le impostazioni del criterio di Network Agent)
- Windows Server con Microsoft Windows Server Update Services (WSUS) distribuito nella rete dell'organizzazione
- Server degli aggiornamenti Microsoft

Se questa opzione è abilitata, Windows Update Agent in un dispositivo gestito si connette alla sorgente degli aggiornamenti Microsoft per aggiornare le informazioni sugli aggiornamenti di Microsoft Windows applicabili.

Se questa opzione è disabilitata, l'Agente di Windows Update in un dispositivo gestito utilizza le informazioni sugli aggiornamenti di Microsoft Windows applicabili ricevuti dalla sorgente degli aggiornamenti Microsoft in precedenza.

La connessione alla sorgente degli aggiornamenti Microsoft può comportare un notevole utilizzo di risorse. Potrebbe essere necessario disabilitare questa opzione se è stata impostata una connessione standard a questa sorgente degli aggiornamenti in un'altra attività o nelle proprietà del criterio Network Agent, nella sezione **Vulnerabilità e aggiornamenti software**. Se non si desidera disabilitare questa opzione, per ridurre l'overload del Server è possibile configurare la pianificazione delle attività in modo da utilizzare il ritardo casuale per l'avvio delle attività entro 360 minuti.

Per impostazione predefinita, questa opzione è abilitata.

La combinazione delle seguenti opzioni delle impostazioni del criterio di Network Agent definisce il modo in cui si ottengono gli aggiornamenti:

- In un dispositivo gestito, l'Agente di Windows Update si connette al server degli aggiornamenti per ottenere gli aggiornamenti solo se l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** è abilitata nelle proprietà dell'attività *Trova vulnerabilità e aggiornamenti richiesti* e l'opzione **Modalità di ricerca di Windows Update** è impostata su **Attiva** nelle impostazioni del criterio di Network Agent.
- Se non è necessario che Network Agent avvii una connessione alla sorgente degli aggiornamenti di Microsoft Windows e scarichi gli aggiornamenti durante l'esecuzione dell'attività *Scansione vulnerabilità*, è possibile impostare l'opzione **Modalità di ricerca di Windows Update** su **Passiva**, mentre l'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** deve rimanere abilitata. In questo modo, è possibile risparmiare risorse e utilizzare gli aggiornamenti di Windows ricevuti in precedenza per la scansione delle vulnerabilità. È possibile utilizzare la modalità passiva se si configura la ricezione degli aggiornamenti DI Microsoft Windows in modo diverso. Se la ricezione degli aggiornamenti di Microsoft Windows non è configurata in altro modo, non impostare l'opzione **Modalità di ricerca di Windows Update** su **Passiva**, poiché in questo caso non si riceveranno le informazioni sugli aggiornamenti, in alcun caso.
- Indipendentemente dallo stato dell'opzione **Stabilisci connessione al server degli aggiornamenti per aggiornare i dati** (abilitata o disabilitata), se l'opzione **Modalità di ricerca di Windows Update** è impostata su **Disabilitata**, Kaspersky Security Center non richiede informazioni sugli aggiornamenti.

- **Cerca vulnerabilità e aggiornamenti di terze parti elencati da Kaspersky**

  Se questa opzione è abilitata, Kaspersky Security Center esegue la ricerca delle vulnerabilità e degli aggiornamenti richiesti per le applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) nel Registro di sistema di Windows e nelle cartelle specificate con **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**. L'elenco completo delle applicazioni di terze parti supportate è gestito da Kaspersky.

  Se questa opzione è disabilitata, Kaspersky Security Center non esegue la ricerca di vulnerabilità e aggiornamenti richiesti per le applicazioni di terze parti. È ad esempio possibile disabilitare questa opzione se si dispone di diverse attività con differenti impostazioni per gli aggiornamenti di Microsoft Windows e gli aggiornamenti delle applicazioni di terze parti.

  Per impostazione predefinita, questa opzione è abilitata.

- **Specificare i percorsi per la ricerca avanzata delle applicazioni nel file system**

  Cartelle in cui Kaspersky Security Center esegue la ricerca delle applicazioni di terze parti che richiedono la correzione delle vulnerabilità e l'installazione di aggiornamenti. È possibile utilizzare le variabili di sistema.

  Specificare le cartelle in cui sono installate le applicazioni. Per impostazione predefinita, l'elenco contiene le cartelle di sistema in cui viene installata la maggior parte delle applicazioni.

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive i file di traccia anche se la scrittura dei file di traccia è disabilitata per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

Raccomandazioni relative alla pianificazione delle attività

Durante la pianificazione dell'attività *Trova vulnerabilità e aggiornamenti richiesti*, verificare che le due opzioni **Esegui attività non effettuate** e **Usa automaticamente il ritardo casuale per l'avvio delle attività** siano abilitate.

Per impostazione predefinita, l'attività *Trova vulnerabilità e aggiornamenti richiesti* è impostata per l'avvio alle 18:00. Se le regole dell'organizzazione per l'ambiente di lavoro prevedono lo spegnimento di tutti i dispositivi in tale orario, l'attività *Trova vulnerabilità e aggiornamenti richiesti* verrà eseguita dopo la riaccensione dei dispositivi, la mattina del giorno successivo. Un'attività di questo tipo potrebbe essere indesiderabile perché una Scansione vulnerabilità può aumentare il carico sui sottosistemi del disco e della CPU. È necessario impostare la pianificazione appropriata per l'attività in base alle regole per l'ambiente di lavoro adottate nell'organizzazione.

Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità

L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* è disponibile solo con la licenza per Vulnerability e Patch Management.

L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per aggiornare e correggere le vulnerabilità del software di terze parti, incluso il software Microsoft, installato nei dispositivi gestiti. Questa attività consente di installare più aggiornamenti e correggere più vulnerabilità in base a determinate regole.

Per installare aggiornamenti o correggere vulnerabilità utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile effettuare una delle seguenti operazioni:

- Eseguire l'Installazione guidata aggiornamenti o la Correzione guidata vulnerabilità.
- Creare un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.
- Aggiungere una regola per l'installazione dell'aggiornamento a un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* esistente.

Per creare un'attività Installa aggiornamenti richiesti e correggi vulnerabilità:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Installa aggiornamenti richiesti e correggi vulnerabilità**.

   Se l'attività non viene visualizzata, verificare se l'account dispone dei diritti di **lettura**, **modifica** ed **esecuzione** per l'area funzionale **Gestione sistema**: **Vulnerability e patch management**. Senza questi diritti di accesso, non è possibile creare e configurare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare i dispositivi a cui assegnare l'attività.

6. Specificare le regole per l'installazione dell'aggiornamento, quindi specificare le seguenti impostazioni:

- **Avvia l'installazione al riavvio o all'arresto del dispositivo**

  Se questa opzione è abilitata, gli aggiornamenti vengono installati al riavvio o all'arresto del dispositivo. In caso contrario, gli aggiornamenti vengono installati in base a una pianificazione.

  Utilizzare questa opzione se l'installazione degli aggiornamenti può influire sulle prestazioni del dispositivo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Installa i componenti generali del sistema richiesti**

  Se questa opzione è abilitata, prima di installare un aggiornamento l'applicazione installa automaticamente tutti i componenti di sistema generali (prerequisiti) richiesti per installare l'aggiornamento. Questi prerequisiti possono ad esempio essere aggiornamenti del sistema operativo.

  Se questa opzione è disabilitata, può essere necessario installare manualmente i prerequisiti.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Consenti l'installazione di nuove versioni dell'applicazione durante gli aggiornamenti**

  Se questa opzione è abilitata, gli aggiornamenti sono consentiti se implicano l'installazione di una nuova versione di un'applicazione software.

  Se questa opzione è disabilitata, l'upgrade del software non viene eseguito. È quindi possibile installare le nuove versioni del software manualmente o tramite un'altra attività. È ad esempio possibile utilizzare questa opzione se l'infrastruttura aziendale non è supportata da una nuova versione del software o se si desidera verificare un aggiornamento in un'infrastruttura di test.

  Per impostazione predefinita, questa opzione è abilitata.

  L'upgrade dell'applicazione può causare un malfunzionamento delle applicazioni dipendenti installate nei dispositivi client.

- **Scarica gli aggiornamenti nel dispositivo senza installarli**

  Se questa opzione è abilitata, l'applicazione scarica gli aggiornamenti nel dispositivo client ma non li installa automaticamente. È quindi possibile installare manualmente gli aggiornamenti scaricati.

  Gli aggiornamenti Microsoft vengono scaricati nell'archiviazione di sistema di Windows. Gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) vengono scaricati nella cartella specificata nel campo **Scarica aggiornamenti in**.

  Se questa opzione è disabilitata, gli aggiornamenti vengono installati automaticamente nel dispositivo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica aggiornamenti in**

  Questa cartella viene utilizzata per scaricare gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft).

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive i file di traccia anche se la scrittura dei file di traccia è disabilitata per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

7. Specificare le impostazioni per il riavvio del sistema operativo:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ripeti la richiesta ogni (min.)**

  Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

  Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

- **Riavvia dopo (min.)**

  Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

  Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Tempo di attesa prima della chiusura forzata delle applicazioni nelle sessioni bloccate (min.)**

Viene forzata la chiusura delle applicazioni quando il dispositivo dell'utente viene bloccato (automaticamente dopo un intervallo di inattività specificato o manualmente).

Se questa opzione è abilitata, viene forzata la chiusura delle applicazioni nel dispositivo bloccato alla scadenza dell'intervallo di tempo specificato nel campo di immissione.

Se questa opzione è disabilitata, le applicazioni nel dispositivo bloccato non vengono chiuse.

Per impostazione predefinita, questa opzione è disabilitata.

8. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

9. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.

10. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

11. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

12. Fare clic sul pulsante **Salva**.

    L'attività verrà creata e configurata.

Se i risultati dell'attività contengono l'avviso 0x80240033 "Errore di Windows Update Agent 80240033 ("Non è stato possibile scaricare le condizioni di licenza")", è possibile risolvere questo problema tramite il Registro di sistema di Windows.

Aggiunta delle regole per l'installazione dell'aggiornamento

Questa funzionalità è disponibile solo con la licenza Vulnerability e patch management.

Durante l'installazione di aggiornamenti software o la correzione di vulnerabilità del software tramite l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è necessario specificare le regole per l'installazione degli aggiornamenti. Queste regole determinano gli aggiornamenti da installare e le vulnerabilità da correggere.

Le esatte impostazioni dipendono dall'esigenza di aggiungere una regola per tutti gli aggiornamenti, per gli aggiornamenti di Windows Update o per gli aggiornamenti di applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft). Durante l'aggiunta di una regola per gli aggiornamenti di Windows Update o per gli aggiornamenti di applicazioni di terze parti, è possibile selezionare le specifiche applicazioni e versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Durante l'aggiunta di una regola per tutti gli aggiornamenti, è possibile selezionare gli specifici aggiornamenti da installare e le vulnerabilità che si desidera correggere tramite l'installazione degli aggiornamenti.

È possibile aggiungere una regola per l'installazione degli aggiornamenti nei modi seguenti:

- Aggiungendo una regola durante la creazione di una nuova attività Installa aggiornamenti richiesti e correggi vulnerabilità.
- Aggiungendo una regola nella scheda **Impostazioni applicazione** nella finestra delle proprietà di un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* esistente.
- Tramite l'Installazione guidata aggiornamenti o la Correzione guidata vulnerabilità.

Per aggiungere una nuova regola per tutti gli aggiornamenti:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per tutti gli aggiornamenti**.

3. Nella pagina **Criteri generali** utilizzare gli elenchi a discesa per specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Aggiornamenti** selezionare gli aggiornamenti da installare:

   - **Installa tutti gli aggiornamenti appropriati**

     Installa tutti gli aggiornamenti software che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

   - **Installa solo gli aggiornamenti nell'elenco**

     Installa solo gli aggiornamenti software che selezionati manualmente dall'elenco. Questo elenco contiene tutti gli aggiornamenti software disponibili.

     Ad esempio, è possibile selezionare aggiornamenti specifici nei seguenti casi: per verificarne l'installazione in un ambiente di test, per aggiornare solo le applicazioni critiche o per aggiornare solo specifiche applicazioni.

     - **Installa automaticamente tutti gli aggiornamenti precedenti dell'applicazione necessari per l'installazione degli aggiornamenti selezionati**

       Mantenere abilitata questa opzione se si desidera consentire l'installazione delle versioni intermedie delle applicazioni quando questa operazione è necessaria per l'installazione degli aggiornamenti selezionati.

       Se questa opzione è disabilitata, vengono installate solo le versioni delle applicazioni selezionate. Disabilitare questa opzione se si desidera aggiornare le applicazioni in modo diretto, senza tentare di installare le versioni successive in modo incrementale. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

       Si supponga di avere la versione 3 di un'applicazione installata in un dispositivo e di voler eseguire l'aggiornamento alla versione 5, ma la versione 5 di questa applicazione può essere installata solo sulla versione 4. Se questa opzione è abilitata, il software installa prima la versione 4 e quindi la versione 5. Se questa opzione è disabilitata, il software non riesce a eseguire l'aggiornamento l'applicazione.

       Per impostazione predefinita, questa opzione è abilitata.

5. Nella pagina **Vulnerabilità** selezionare le vulnerabilità da correggere tramite l'installazione degli aggiornamenti selezionati:

   - **Correggi tutte le vulnerabilità che corrispondono ad altri criteri**

     Verranno corrette tutte le vulnerabilità che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

   - **Correggi solo le vulnerabilità nell'elenco**

     Verranno corrette solo le vulnerabilità selezionate manualmente dall'elenco. Questo elenco contiene tutte le vulnerabilità rilevate.

     Ad esempio, è possibile selezionare vulnerabilità specifiche nei seguenti casi: per verificarne la correzione in un ambiente di test, per correggere solo le vulnerabilità di applicazioni critiche o per correggere le vulnerabilità solo in specifiche applicazioni.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Per aggiungere una nuova regola per gli aggiornamenti di Windows Update:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per Windows Update**.

3. Nella finestra **Criteri generali** specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

   - **Correggi le vulnerabilità con un livello di criticità MSRC uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Microsoft Security Response Center (MSRC) è uguale o superiore al valore selezionato nell'elenco (**Basso**, **Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Categorie di aggiornamenti** selezionare le categorie di aggiornamenti da installare. Queste categorie sono identiche a quelle del catalogo di Microsoft Update. Per impostazione predefinita, tutte le categorie sono selezionate.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Per aggiungere una nuova regola per gli aggiornamenti delle applicazioni di terze parti:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per gli aggiornamenti di terze parti**.

3. Nella finestra **Criteri generali** specificare le seguenti impostazioni:

   - Set di aggiornamenti da installare

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - Correggi le vulnerabilità con un livello di criticità uguale o superiore a

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione Impostazioni della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Creazione dell'attività Installa aggiornamenti di Windows Update

L'attività *Installa aggiornamenti di Windows Update* consente di installare gli aggiornamenti software forniti dal servizio Windows Update nei dispositivi gestiti.

Se non si dispone della licenza per Vulnerability e patch management, non è possibile creare nuove attività di tipo *Installa aggiornamenti di Windows Update*. Per installare nuovi aggiornamenti, è possibile aggiungerli a un'attività *Installa aggiornamenti di Windows Update* esistente. È consigliabile utilizzare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* anziché l'attività *Installa aggiornamenti di Windows Update*. L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* consente di installare automaticamente più aggiornamenti e correggere più vulnerabilità, in base alle regole definite. Inoltre, questa attività consente di installare aggiornamenti da fornitori di software diversi da Microsoft.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Per creare l'attività Installa aggiornamenti di Windows Update:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Installa aggiornamenti di Windows Update**.
4. Specificare il nome dell'attività che si intende creare.

   Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare i dispositivi a cui assegnare l'attività.
6. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzato l'elenco degli aggiornamenti.
7. Selezionare gli aggiornamenti di Windows Update che si desidera installare, quindi fare clic su **OK**.

8. Specificare le impostazioni per il riavvio del sistema operativo:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ripeti la richiesta ogni (min.)**

  Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

  Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

- **Riavvia dopo (min.)**

  Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

  Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

9. Specificare le impostazioni per l'account:

- **Account predefinito**

  L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

  Per impostazione predefinita, questa opzione è selezionata.

- **Specifica account**

  Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

- **Account**

  Account tramite il quale viene eseguita l'attività.

- **Password**

  Password dell'account con cui verrà eseguita l'attività.

10. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

11. Fare clic sul pulsante **Fine**.

    L'attività verrà creata e visualizzata nell'elenco delle attività.

12. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

13. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

14. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Visualizzazione delle informazioni sugli aggiornamenti software di terze parti disponibili

È possibile visualizzare l'elenco degli aggiornamenti disponibili per il software di terze parti, incluso il software Microsoft, installato nei dispositivi client.

Per visualizzare un elenco degli aggiornamenti disponibili per le applicazioni di terze parti installate nei dispositivi client:

Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Aggiornamenti software**.

Verrà visualizzato un elenco degli aggiornamenti disponibili.

È possibile specificare un filtro per visualizzare l'elenco degli aggiornamenti software. Fare clic sull'icona **Filtro** ( ) nell'angolo superiore destro dell'elenco degli aggiornamenti software per gestire il filtro. È anche possibile selezionare uno dei filtri preimpostati dall'elenco a discesa **Filtri preimpostati** sopra l'elenco delle vulnerabilità del software.

Per visualizzare le proprietà di un aggiornamento:

1. Fare clic sul nome dell'aggiornamento software richiesto.
2. Verrà visualizzata la finestra delle proprietà dell'aggiornamento, in cui sono visualizzate informazioni raggruppate nelle seguenti schede:

   - **Generale**

     Questa scheda mostra i dettagli generali dell'aggiornamento selezionato:

     - Stato di approvazione dell'aggiornamento. (può essere modificato manualmente selezionando un nuovo stato nell'elenco a discesa)
     - Categoria WSUS (Windows Server Update Services) a cui appartiene l'aggiornamento
     - Data e ora di registrazione dell'aggiornamento
     - Data e ora di creazione dell'aggiornamento
     - Livello di importanza dell'aggiornamento
     - Requisiti di installazione imposti dall'aggiornamento
     - Famiglia di applicazioni a cui appartiene l'aggiornamento
     - Applicazione a cui si applica l'aggiornamento
     - Numero di revisione dell'aggiornamento

   - **Attributi**

Questa scheda visualizza un set di attributi che è possibile utilizzare per ottenere ulteriori informazioni sull'aggiornamento selezionato. Questo set varia a seconda che l'aggiornamento sia pubblicato da Microsoft o da un fornitore di terze parti.

La scheda visualizza le seguenti informazioni per un aggiornamento Microsoft:

- Livello di importanza dell'aggiornamento secondo Microsoft Security Response Center (MSRC)
- Collegamento all'articolo nella Microsoft Knowledge Base in cui viene descritto l'aggiornamento
- Collegamento all'articolo nel Bollettino Microsoft sulla sicurezza in cui viene descritto l'aggiornamento
- ID di aggiornamento

La scheda visualizza le seguenti informazioni per un aggiornamento di terze parti:

- Se l'aggiornamento è una patch o un pacchetto di distribuzione completo
- Lingua di localizzazione dell'aggiornamento
- Se l'aggiornamento viene installato automaticamente o manualmente
- Se l'aggiornamento è stato revocato dopo l'applicazione
- Collegamento per scaricare l'aggiornamento

- **Dispositivi**

  Questa scheda visualizza un elenco di dispositivi in cui è stato installato l'aggiornamento selezionato.

- **Vulnerabilità risolte**

  Questa scheda visualizza un elenco di vulnerabilità che l'aggiornamento selezionato è in grado di correggere.

- **Crossover degli aggiornamenti**

  Questa scheda visualizza i possibili crossover tra i vari aggiornamenti pubblicati per la stessa applicazione, ovvero se l'aggiornamento selezionato può sostituire altri aggiornamenti o, viceversa, essere sostituito da altri aggiornamenti (disponibile solo per gli aggiornamenti Microsoft).

- **Attività per l'installazione dell'aggiornamento**

  Questa scheda visualizza un elenco di attività il cui ambito include l'installazione dell'aggiornamento selezionato. La scheda consente inoltre di creare una nuova attività di installazione remota per l'aggiornamento.

Per visualizzare le statistiche relative all'installazione di un aggiornamento:

1. Selezionare la casella di controllo accanto all'aggiornamento software richiesto.

2. Fare clic sul pulsante **Statistiche degli stati di installazione aggiornamenti**.

   Verrà visualizzato il diagramma degli stati di installazione dell'aggiornamento. Facendo clic su uno stato, viene aperto un elenco dei dispositivi in cui l'aggiornamento ha lo stato selezionato.

È possibile visualizzare le informazioni sugli aggiornamenti software disponibili per il software di terze parti, incluso il software Microsoft, installato nel dispositivo gestito selezionato che esegue Windows.

Per visualizzare un elenco degli aggiornamenti disponibili per il software di terze parti installato nel dispositivo gestito selezionato:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo per cui si desidera visualizzare gli aggiornamenti software di terze parti.

   Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.

3. Nella finestra delle proprietà del dispositivo selezionato selezionare la scheda **Avanzate**.

4. Nel riquadro sinistro selezionare la sezione **Aggiornamenti disponibili**. Per visualizzare solo gli aggiornamenti installati, abilitare l'opzione **Mostra aggiornamenti installati**.

   Verrà visualizzato l'elenco degli aggiornamenti software di terze parti disponibili per il dispositivo selezionato.

Esportazione dell'elenco degli aggiornamenti software disponibili in un file

È possibile esportare l'elenco degli aggiornamenti per il software di terze parti, incluso il software Microsoft, che viene attualmente visualizzato nei file CSV o TXT. È ad esempio possibile utilizzare questi file per inviarli al responsabile della sicurezza delle informazioni o per archiviarli a fini statistici.

Per esportare in un file di testo l'elenco degli aggiornamenti disponibili per il software di terze parti installato in tutti i dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Aggiornamenti software**.

   La pagina visualizza un elenco degli aggiornamenti disponibili per il software di terze parti installato in tutti i dispositivi gestiti.

2. Fare clic sul pulsante **Esporta in TXT** o **Esporta in CSV**, a seconda del formato preferito per l'esportazione.

   Il file contenente l'elenco degli aggiornamenti disponibili per il software di terze parti, incluso il software Microsoft, verrà scaricato nel dispositivo in uso.

Per esportare in un file di testo l'elenco degli aggiornamenti disponibili per il software di terze parti installato nel dispositivo gestito selezionato:

1. Aprire l'elenco degli aggiornamenti software di terze parti disponibili nel dispositivo gestito selezionato.
2. Selezionare gli aggiornamenti software da esportare.

   Ignorare questo passaggio se si desidera esportare un elenco completo degli aggiornamenti software.

   Se si desidera esportare un elenco completo degli aggiornamenti software, verranno esportati solo gli aggiornamenti visualizzati nella pagina corrente.

   Per esportare solo gli aggiornamenti installati, selezionare la casella di controllo **Mostra aggiornamenti installati**.
3. Fare clic sul pulsante **Esporta in TXT** o **Esporta in CSV**, a seconda del formato preferito per l'esportazione.

Il file contenente l'elenco degli aggiornamenti per il software di terze parti, incluso il software Microsoft, installati nel dispositivo gestito selezionato verrà scaricato nel dispositivo in uso.

Approvazione e rifiuto degli aggiornamenti software di terze parti

Quando si configura l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile creare una regola che richiede uno stato specifico degli aggiornamenti che devono essere installati. Ad esempio, una regola di aggiornamento può consentire l'installazione dei seguenti elementi:

- Solo gli aggiornamenti approvati
- Solo gli aggiornamenti approvati e non definiti
- Tutti gli aggiornamenti, indipendentemente dai relativi stati

È possibile approvare gli aggiornamenti da installare e rifiutare quelli che non devono essere installati.

L'utilizzo dello stato *Approvato* per gestire l'installazione degli aggiornamenti è efficace per una piccola quantità di aggiornamenti. Per installare più aggiornamenti, utilizzare le regole che è possibile configurare nell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. È consigliabile impostare lo stato *Approvato* solo per gli aggiornamenti specifici che non soddisfano i criteri specificati nelle regole. Quando si approva manualmente una grande quantità di aggiornamenti, le prestazioni di Administration Server si riducono e questo può causare un sovraccarico di Administration Server.

Per approvare o rifiutare uno o più aggiornamenti:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Aggiornamenti software**.

   Verrà visualizzato un elenco degli aggiornamenti disponibili.
2. Selezionare gli aggiornamenti che si desidera accettare o rifiutare.
3. Fare clic su **Approva** per approvare gli aggiornamenti selezionati o su **Rifiuta** per rifiutare gli aggiornamenti selezionati.

   Il valore predefinito è *Indefinito*.

Gli aggiornamenti selezionati hanno gli stati che sono stati definiti.

Facoltativamente è possibile modificare lo stato di approvazione nelle proprietà di un aggiornamento specifico.

Per approvare o rifiutare un aggiornamento nelle relative proprietà:

1. Nel menu principale accedere a **Operazioni → Gestione patch → Aggiornamenti software**.

   Verrà visualizzato un elenco degli aggiornamenti disponibili.

2. Fare clic sul nome dell'aggiornamento che si desidera approvare o rifiutare.

   Verrà visualizzata la finestra delle proprietà dell'aggiornamento.

3. Nella sezione **Generale** selezionare uno stato per l'aggiornamento modificando l'opzione **Stato di approvazione dell'aggiornamento**. È possibile selezionare lo stato *Approvato*, *Rifiutato* o *Indefinito*.

4. Fare clic sul pulsante **Salva** per applicare le modifiche.

L'aggiornamento selezionato ha lo stato che è stato definito.

Se si imposta lo stato **Rifiutato** per gli aggiornamenti software di terze parti, tali aggiornamenti non verranno installati nei dispositivi in cui l'installazione era stata pianificata ma non ancora eseguita. Gli aggiornamenti rimarranno nei dispositivi in cui erano già installati. Se è necessario eliminarli, è possibile eliminarli manualmente in locale.

Creazione dell'attività Esegui sincronizzazione di Windows Update

L'attività *Esegui sincronizzazione di Windows Update* è disponibile solo con la licenza per Vulnerability e Patch Management.

L'attività *Esegui sincronizzazione di Windows Update* è necessaria se si desidera utilizzare Administration Server come server WSUS. In questo caso, Administration Server scarica gli aggiornamenti di Windows nel database e fornisce gli aggiornamenti a Windows Update nei dispositivi client in modalità centralizzata tramite i Network Agent. Se la rete non utilizza un server WSUS, ogni dispositivo client scarica gli aggiornamenti Microsoft da server esterni in modo indipendente.

L'attività *Esegui sincronizzazione di Windows Update* scarica solo metadati dai server Microsoft. Kaspersky Security Center scarica gli aggiornamenti quando si esegue un'attività di installazione degli aggiornamenti e solo gli aggiornamenti selezionati per l'installazione.

Durante l'esecuzione dell'attività **Esegui sincronizzazione di Windows Update** l'applicazione riceve un elenco degli aggiornamenti correnti da un server di aggiornamento Microsoft. Kaspersky Security Center compila quindi un elenco degli aggiornamenti che sono diventati obsoleti. Al successivo avvio dell'attività **Trova vulnerabilità e aggiornamenti richiesti**, Kaspersky Security Center contrassegna tutti gli aggiornamenti obsoleti e ne imposta l'ora di eliminazione. Al successivo avvio dell'attività **Esegui sincronizzazione di Windows Update**, vengono eliminati tutti gli aggiornamenti contrassegnati per l'eliminazione 30 giorni prima. Kaspersky Security Center verifica inoltre se sono presenti aggiornamenti obsoleti contrassegnati per l'eliminazione più di 180 giorni prima ed elimina gli aggiornamenti meno recenti.

Quando viene completata l'attività **Esegui sincronizzazione di Windows Update** e gli aggiornamenti obsoleti vengono eliminati, il database può ancora salvare i codici hash relativi ai file degli aggiornamenti eliminati, nonché i file corrispondenti nei file %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles files (se sono stati scaricati in precedenza). È possibile eseguire l'attività **Manutenzione di Administration Server** per eliminare i record obsoleti dal database e dai file corrispondenti.

Per creare l'attività Esegui sincronizzazione di Windows Update:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Esegui sincronizzazione di Windows Update**.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Abilitare l'opzione **Scarica i file di installazione rapida** se si desidera scaricare i file per l'aggiornamento rapido durante l'esecuzione dell'attività.

   Quando Kaspersky Security Center sincronizza gli aggiornamenti con i server di Microsoft Windows Update, le informazioni su tutti i file vengono salvate nel database di Administration Server. Anche tutti i file richiesti per un aggiornamento vengono scaricati nell'unità durante l'interazione con l'Agente di Windows Update. In particolare, Kaspersky Security Center salva le informazioni sui file per l'aggiornamento rapido nel database e li scarica se necessario. Il download dei file per l'aggiornamento rapido comporta una riduzione dello spazio su disco.

   Per evitare la diminuzione dello spazio su disco e ridurre il traffico, disabilitare l'opzione **Scarica i file di installazione rapida**.
6. Selezionare l'applicazione per cui si desidera scaricare gli aggiornamenti.

   Se la casella di controllo **Tutte le applicazioni** è selezionata, verranno scaricati gli aggiornamenti per tutte le applicazioni esistenti e per tutte le applicazioni che potrebbero essere rilasciate in futuro.
7. Selezionare le categorie di aggiornamenti da scaricare in Administration Server.

   Se la casella di controllo **Tutte le categorie** è selezionata, gli aggiornamenti verranno scaricati per tutte le categorie di aggiornamenti esistenti e per tutte le categorie che possono presentarsi in futuro.
8. Selezionare le lingue di localizzazione per gli aggiornamenti da scaricare in Administration Server. Selezionare una delle seguenti opzioni:

   - **Scarica tutte le lingue, incluse quelle nuove**

     Se questa opzione è selezionata, tutte le lingue di localizzazione disponibili degli aggiornamenti verranno scaricate in Administration Server. Per impostazione predefinita, questa opzione è selezionata.

   - **Scarica le lingue selezionate**

     Se questa opzione è selezionata, è possibile selezionare dall'elenco le lingue di localizzazione degli aggiornamenti da scaricare in Administration Server.

9. Specificare l'account da utilizzare durante l'esecuzione dell'attività. Selezionare una delle seguenti opzioni:

   - **Account predefinito**

     L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Specifica account**

     Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

10. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

11. Fare clic sul pulsante **Fine**.

    L'attività verrà creata e visualizzata nell'elenco delle attività.

12. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

13. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

14. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Aggiornamento automatico delle applicazioni di terze parti

Alcune applicazioni di terze parti possono essere aggiornate automaticamente. Il fornitore dell'applicazione definisce se l'applicazione supporta o meno la funzionalità di aggiornamento automatico. Se un'applicazione di terze parti installata in un dispositivo gestito supporta l'aggiornamento automatico, è possibile specificare l'impostazione di aggiornamento automatico nelle proprietà dell'applicazione. Dopo aver modificato l'impostazione di aggiornamento automatico, i Network Agent applicano la nuova impostazione in ogni dispositivo gestito in cui è installata l'applicazione.

L'impostazione di aggiornamento automatico è indipendente dagli altri oggetti e dalle impostazioni della funzionalità Vulnerability e patch management. Questa impostazione non dipende ad esempio da uno stato di approvazione degli aggiornamenti o dalle attività di installazione degli aggiornamenti, come *Installa aggiornamenti richiesti e correggi vulnerabilità*, *Installa aggiornamenti di Windows Update* e *Correggi vulnerabilità*.

Per configurare l'impostazione di aggiornamento automatico per un'applicazione di terze parti:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Registro delle applicazioni**.

2. Fare clic sul nome dell'applicazione per la quale si desidera modificare l'impostazione di aggiornamento automatico.

   Per semplificare la ricerca, è possibile filtrare l'elenco in base alla colonna **Stato degli aggiornamenti automatici**.

   Verrà visualizzata la finestra delle proprietà dell'applicazione.

3. Nella sezione **Generale** selezionare un valore per la seguente impostazione:

   Stato degli aggiornamenti automatici

   Selezionare una delle seguenti opzioni:

   - **Indefinito**

     La funzionalità di aggiornamento automatico è disabilitata. Kaspersky Security Center installa gli aggiornamenti delle applicazioni di terze parti utilizzando le attività: *Installa aggiornamenti richiesti e correggi vulnerabilità*, *Installa aggiornamenti di Windows Update* e *Correggi vulnerabilità*.

   - **Consentito**

     Dopo che il fornitore rilascia un aggiornamento per l'applicazione, questo aggiornamento viene installato automaticamente nei dispositivi gestiti. Non sono necessarie operazioni aggiuntive.

   - **Bloccato**

     Questi aggiornamenti dell'applicazione non vengono installati automaticamente. Kaspersky Security Center installa gli aggiornamenti delle applicazioni di terze parti utilizzando le attività: *Installa aggiornamenti richiesti e correggi vulnerabilità*, *Installa aggiornamenti di Windows Update* e *Correggi vulnerabilità*.

4. Fare clic sul pulsante **Salva** per applicare le modifiche.

L'impostazione di aggiornamento automatico viene applicata all'applicazione selezionata.

Correzione delle vulnerabilità del software di terze parti

Questa sezione descrive le funzionalità di Kaspersky Security Center relative alla correzione delle vulnerabilità del software installato nei dispositivi gestiti.

Scenario: Individuazione e correzione delle vulnerabilità del software di terze parti

Questa sezione fornisce uno scenario per individuare e correggere le vulnerabilità nei dispositivi gestiti che eseguono Windows. È possibile individuare e correggere le vulnerabilità del software nel sistema operativo e nel software di terze parti, incluso il software Microsoft.

Prerequisiti

- Kaspersky Security Center viene distribuito nell'organizzazione.
- Nell'organizzazione sono presenti dispositivi gestiti che eseguono Windows.
- È necessaria una connessione Internet affinché Administration Server esegua le seguenti attività:
  - Per creare un elenco di correzioni consigliate per le vulnerabilità del software Microsoft. L'elenco viene creato e aggiornato regolarmente dagli specialisti Kaspersky.
  - Per correggere le vulnerabilità in software di terze parti diverso dal software Microsoft.

Passaggi

L'individuazione e la correzione delle vulnerabilità del software prevede diversi passaggi:

1. **Ricerca delle vulnerabilità del software installato nei dispositivi gestiti**

   Per individuare le vulnerabilità del software installato nei dispositivi gestiti, eseguire l'attività *Trova vulnerabilità e aggiornamenti richiesti*. Al termine di questa attività, Kaspersky Security Center riceve gli elenchi delle vulnerabilità rilevate e degli aggiornamenti richiesti per il software di terze parti installato nei dispositivi specificati nelle proprietà dell'attività.

   L'attività *Trova vulnerabilità e aggiornamenti richiesti* viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. Se la procedura guidata non è stata eseguita, avviarla ora o creare l'attività manualmente.

   Istruzioni dettagliate:

   - Administration Console: Scansione delle applicazioni per rilevare la presenza di vulnerabilità, Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti
   - Kaspersky Security Center Web Console: Creazione dell'attività Trova vulnerabilità e aggiornamenti richiesti, Impostazioni dell'attività Trova vulnerabilità e aggiornamenti richiesti

2. **Analisi dell'elenco delle vulnerabilità del software rilevate**

   Visualizzare l'elenco **Vulnerabilità del software** e decidere quali vulnerabilità devono essere corrette. Per visualizzare informazioni dettagliate su ciascuna vulnerabilità, fare clic sul nome della vulnerabilità nell'elenco. Per ogni vulnerabilità nell'elenco, è anche possibile visualizzare le statistiche sulla vulnerabilità nei dispositivi gestiti.

   Istruzioni dettagliate:

   - Administration Console: Visualizzazione delle informazioni sulle vulnerabilità del software, Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti
   - Kaspersky Security Center Web Console: Visualizzazione delle informazioni sulle vulnerabilità del software, Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti

3. **Configurazione della correzione delle vulnerabilità**

   Quando vengono rilevate le vulnerabilità del software, è possibile correggere le vulnerabilità del software nei dispositivi gestiti utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità*.

L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per aggiornare e correggere le vulnerabilità del software di terze parti, incluso il software Microsoft, installato nei dispositivi gestiti. Questa attività consente di installare più aggiornamenti e correggere più vulnerabilità in base a determinate regole. Questa attività può essere creata solo se si dispone della licenza per la funzionalità Vulnerability e patch management. Per correggere le vulnerabilità del software l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* utilizza gli aggiornamenti software consigliati.

L'attività *Correggi vulnerabilità* non richiede l'opzione di licenza per la funzionalità Vulnerability e patch management. Per utilizzare questa attività è necessario specificare manualmente le correzioni dell'utente per le vulnerabilità del software di terze parti elencato nelle impostazioni dell'attività. L'attività *Correggi vulnerabilità* utilizza le correzioni consigliate per il software Microsoft e le correzioni dell'utente per software di terze parti.

È possibile avviare la Correzione guidata vulnerabilità che crea automaticamente una di queste attività oppure è possibile creare una di queste attività manualmente.

Istruzioni dettagliate:

- Administration Console: Selezione di correzioni utente per le vulnerabilità del software di terze parti, Correzione delle vulnerabilità delle applicazioni
- Kaspersky Security Center Web Console: Selezione di correzioni utente per le vulnerabilità del software di terze parti, Correzione delle vulnerabilità del software di terze parti, Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità

4 Pianificazione delle attività

Per assicurarsi che l'elenco delle vulnerabilità sia sempre aggiornato, pianificare l'attività *Trova vulnerabilità e aggiornamenti richiesti* affinché venga eseguita periodicamente in modo automatico. La frequenza media consigliata è una volta alla settimana.

Se è stata creata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile pianificarla in modo che venga eseguita con la stessa frequenza dell'attività *Trova vulnerabilità e aggiornamenti richiesti* o con una frequenza inferiore. Quando si pianifica l'attività *Correggi vulnerabilità*, tenere presente che è necessario selezionare le correzioni per il software Microsoft o specificare ogni volta le correzioni utente per il software di terze parti prima di avviare l'attività.

Quando si pianificano le attività, assicurarsi che al termine dell'attività *Trova vulnerabilità e aggiornamenti richiesti* venga avviata un'attività per correggere la vulnerabilità.

5 Ignorare le vulnerabilità del software (facoltativo)

Se lo si desidera, è possibile ignorare le vulnerabilità del software da correggere in tutti i dispositivi gestiti o solo nei dispositivi gestiti selezionati.

Istruzioni dettagliate:

- Administration Console: Ignorare le vulnerabilità del software
- Kaspersky Security Center Web Console: Ignorare le vulnerabilità del software

6 Esecuzione di un'attività di correzione della vulnerabilità

Avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità*. Al termine dell'attività, assicurarsi che questa abbia lo stato *Completato* nell'elenco attività.

7 Creare il rapporto sui risultati della correzione delle vulnerabilità del software (facoltativo)

Per visualizzare le statistiche dettagliate sulla correzione delle vulnerabilità, generare il Rapporto sulle vulnerabilità. Il rapporto visualizza informazioni sulle vulnerabilità del software che non sono state corrette. In tal modo è possibile avere un'idea sulla ricerca e la correzione delle vulnerabilità del software di terze parti, incluso il software Microsoft, presente nell'organizzazione.

Istruzioni dettagliate:

- Administration Console: Creazione e visualizzazione di un rapporto
- Kaspersky Security Center Web Console: Generazione e visualizzazione di un rapporto

8. **Verifica della configurazione e individuazione e correzione delle vulnerabilità del software di terze parti**

   Assicurarsi di avere eseguito le seguenti operazioni:

   - Avere ottenuto e rivisto l'elenco delle vulnerabilità del software nei dispositivi gestiti
   - Avere eventualmente ignorato le vulnerabilità del software
   - Avere configurato l'attività per correggere le vulnerabilità
   - Avere pianificato le attività per individuare e correggere le vulnerabilità del software in modo che vengano avviate in sequenza
   - Aver controllato che sia stata eseguita l'attività per correggere le vulnerabilità del software

Risultati

Se è stata creata e configurata l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, le vulnerabilità vengono corrette automaticamente nei dispositivi gestiti. Quando viene eseguita, l'attività collega l'elenco degli aggiornamenti software disponibili alle regole specificate nelle impostazioni dell'attività. Tutti gli aggiornamenti software che soddisfano i criteri nelle regole verranno scaricati nell'archivio di Administration Server e verranno installati per correggere le vulnerabilità del software.

Se è stata creata l'attività *Correggi vulnerabilità*, vengono corrette solo le vulnerabilità del software nel software Microsoft.

Informazioni sulla ricerca e la correzione delle vulnerabilità del software

Kaspersky Security Center rileva e corregge le vulnerabilità del software nei dispositivi gestiti che eseguono i sistemi operativi delle famiglie Microsoft Windows. Le vulnerabilità vengono rilevate nel sistema operativo e nel software di terze parti, incluso il software Microsoft.

> Le funzionalità di aggiornamento (compresa la fornitura degli aggiornamenti delle firme anti-virus e della base di codice) e la funzionalità KSN potrebbero non essere disponibili nel software negli Stati Uniti.

Individuazione delle vulnerabilità del software

Per individuare le vulnerabilità del software, Kaspersky Security Center utilizza le caratteristiche del database delle vulnerabilità note. Questo database viene creato dagli specialisti di Kaspersky. Contiene informazioni sulle vulnerabilità, come la descrizione della vulnerabilità, la data di rilevamento della vulnerabilità, il livello di criticità della vulnerabilità. Per informazioni dettagliate sulle vulnerabilità del software, visitare il sito Web di Kaspersky.

Kaspersky Security Center utilizza l'attività *Trova vulnerabilità e aggiornamenti richiesti* per rilevare le vulnerabilità del software.

In alcuni casi le vulnerabilità rilevate in un sistema operativo Microsoft Windows possono essere corrette utilizzando uno dei seguenti metodi:

- Installazione di un aggiornamento per il sistema operativo.
- Aggiornamento del sistema operativo a una versione più recente (ad esempio da Windows 10 a Windows 11).

In questo scenario Kaspersky Security Center mostra due voci per la stessa vulnerabilità.

Correzione delle vulnerabilità del software

Per correggere le vulnerabilità del software Kaspersky Security Center utilizza gli aggiornamenti software rilasciati dai relativi fornitori. I metadati degli aggiornamenti software vengono scaricati nell'archivio di Administration Server a seguito dell'esecuzione delle seguenti attività:

- *Scarica aggiornamenti nell'archivio dell'Administration Server*. Questa attività ha lo scopo di scaricare i metadati degli aggiornamenti per software Kaspersky e di terze parti. Questa attività viene creata automaticamente dall'Avvio rapido guidato di Kaspersky Security Center. È possibile creare manualmente l'attività Scarica aggiornamenti nell'archivio dell'Administration Server.
- *Esegui sincronizzazione di Windows Update*. Questa attività ha lo scopo di scaricare i metadati degli aggiornamenti per il software Microsoft.

Gli aggiornamenti software per correggere le vulnerabilità possono essere rappresentati come patch o pacchetti o di distribuzione completi. Gli aggiornamenti software che correggono le vulnerabilità del software vengono denominati *correzioni*. Le *correzioni consigliate* sono quelle consigliate per l'installazione dagli specialisti di Kaspersky. Le *correzioni dell'utente* sono quelle specificate manualmente per l'installazione da parte degli utenti. Per installare una correzione dell'utente, è necessario creare un pacchetto di installazione contenente questa correzione.

Se si dispone della licenza di Kaspersky Security Center con la funzionalità Vulnerability e patch management, per correggere le vulnerabilità del software è possibile utilizzare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. Questa attività corregge automaticamente più vulnerabilità installando le correzioni consigliate. Per questa attività è possibile configurare manualmente determinate regole per correggere più vulnerabilità.

Se non si dispone della licenza di Kaspersky Security Center con la funzionalità Vulnerability e patch management, per correggere le vulnerabilità del software è possibile utilizzare l'attività *Correggi vulnerabilità*. Tramite questa attività è possibile correggere le vulnerabilità installando le correzioni consigliate per il software Microsoft e le correzioni dell'utente per altri software di terze parti.

Per motivi di sicurezza, tutti gli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management vengono automaticamente analizzati alla ricerca di malware dalle tecnologie Kaspersky. Queste tecnologie vengono utilizzate per il controllo automatico dei file e includono la scansione virus, l'analisi statica, l'analisi dinamica, l'analisi del comportamento nell'ambiente sandbox e il machine learning.

Gli esperti Kaspersky non eseguono l'analisi manuale degli aggiornamenti software di terzi installati utilizzando la funzionalità Vulnerability e patch management. Inoltre, gli esperti di Kaspersky non ricercano vulnerabilità (note o sconosciute) o funzionalità non documentate in tali aggiornamenti, né eseguono altri tipi di analisi degli aggiornamenti diversi da quelli specificati nel paragrafo precedente.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Per correggere alcune vulnerabilità del software, è necessario accettare il Contratto di licenza con l'utente finale (EULA) per l'installazione del software, se è richiesta l'accettazione del Contratto di licenza con l'utente finale. Se non si accetta il Contratto di licenza con l'utente finale, la vulnerabilità del software non viene corretta.

Correzione delle vulnerabilità del software di terze parti

Dopo aver ottenuto l'elenco delle vulnerabilità del software, è possibile correggere le vulnerabilità del software nei dispositivi gestiti che eseguono Windows. È possibile correggere le vulnerabilità del software nel sistema operativo e nel software di terze parti, incluso il software Microsoft, creando ed eseguendo l'attività *Correggi vulnerabilità* o l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Facoltativamente, è possibile creare un'attività per correggere le vulnerabilità del software nei modi seguenti:

- Aprendo l'elenco delle vulnerabilità e specificando quali vulnerabilità correggere.

  Verrà creata una nuova attività per correggere le vulnerabilità del software. Facoltativamente è possibile aggiungere le vulnerabilità selezionate a un'attività esistente.

- Eseguendo la Correzione guidata vulnerabilità.

  La Correzione guidata vulnerabilità è disponibile solo con la licenza per Vulnerability e patch management.

  La procedura guidata semplifica la creazione e la configurazione di un'attività di correzione delle vulnerabilità e consente di eliminare la creazione di attività ridondanti che contengono gli stessi aggiornamenti da installare.

Correzione delle vulnerabilità del software tramite l'elenco delle vulnerabilità

Per correggere le vulnerabilità del software:

1. Aprire uno degli elenchi di vulnerabilità:

   - Per aprire l'elenco generale delle vulnerabilità nel menu principale, passare a **Operazioni** → **Gestione patch** → **Vulnerabilità del software**.
   - Per aprire l'elenco delle vulnerabilità per un dispositivo gestito, passare a **Risorse (dispositivi)** → **Dispositivi gestiti** → <nome dispositivo> → **Avanzate** → **Vulnerabilità del software**.
   - Per aprire l'elenco delle vulnerabilità per un'applicazione specifica nel menu principale, passare a **Operazioni** → **Applicazioni di terze parti** → **Registro delle applicazioni** → <nome applicazione> → **Vulnerabilità**.

   Verrà visualizzata una pagina con un elenco delle vulnerabilità del software di terze parti.

2. Selezionare una o più vulnerabilità nell'elenco, quindi fare clic sul pulsante **Correggi vulnerabilità**.

   Se un aggiornamento software consigliato per correggere una delle vulnerabilità selezionate è assente, viene visualizzato un messaggio informativo.

   Per correggere alcune vulnerabilità del software, è necessario accettare il Contratto di licenza con l'utente finale (EULA) per l'installazione del software, se è richiesta l'accettazione del Contratto di licenza con l'utente finale. Se non si accetta il Contratto di licenza con l'utente finale, la vulnerabilità del software non viene corretta.

3. Selezionare una delle seguenti opzioni:

   - **Nuova attività**

     Verrà avviata la Creazione guidata nuova attività. Se si dispone della licenza Vulnerability e Patch Management, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* è pre-selezionata. Se non si dispone della licenza, l'attività *Correggi vulnerabilità* è pre-selezionata. Seguire i passaggi della procedura guidata per completare la creazione dell'attività.

   - **Correggi vulnerabilità (aggiungi regola all'attività specificata)**

     Selezionare un'attività a cui aggiungere le vulnerabilità selezionate. Se si dispone della licenza Vulnerability e Patch Management, selezionare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. Una nuova regola per correggere le vulnerabilità selezionate verrà automaticamente aggiunta all'attività selezionata. Se non si dispone della licenza, selezionare l'attività *Correggi vulnerabilità*. Le vulnerabilità selezionate verranno aggiunte alle proprietà dell'attività.

     Verrà visualizzata la finestra delle proprietà dell'attività. Fare clic sul pulsante **Salva** per applicare le modifiche.

   Se si è scelto di creare un'attività, l'attività viene creata e visualizzata nell'elenco delle attività in **Risorse (dispositivi)** → **Attività**. Se si è scelto di aggiungere le vulnerabilità a un'attività esistente, le vulnerabilità vengono salvate nelle proprietà dell'attività.

Per correggere le vulnerabilità del software di terze parti, avviare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* o l'attività *Correggi vulnerabilità*. Se è stata creata l'attività *Correggi vulnerabilità*, è necessario specificare manualmente gli aggiornamenti software per correggere le vulnerabilità del software elencate nelle impostazioni dell'attività.

Correzione delle vulnerabilità del software tramite la Correzione guidata vulnerabilità

La Correzione guidata vulnerabilità è disponibile solo con la licenza per Vulnerability e patch management.

Per correggere le vulnerabilità del software utilizzando la Correzione guidata vulnerabilità:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Vulnerabilità del software**.

   Verrà visualizzata una pagina con un elenco delle vulnerabilità del software di terze parti installato nei dispositivi gestiti.

2. Selezionare la casella di controllo accanto alla vulnerabilità da correggere.

3. Fare clic sul pulsante **Esegui Correzione guidata vulnerabilità**.

   Verrà avviata la Correzione guidata vulnerabilità. La pagina **Selezionare l'attività per la correzione della vulnerabilità** visualizza l'elenco di tutte le attività esistenti dei seguenti tipi:

   - *Installa aggiornamenti richiesti e correggi vulnerabilità*
   - *Installa aggiornamenti di Windows Update*
   - *Correggi vulnerabilità*

   Non è possibile modificare gli ultimi due tipi di attività per installare nuovi aggiornamenti. Per installare nuovi aggiornamenti, è possibile utilizzare solo l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.

4. Se si desidera che la procedura guidata visualizzi solo le attività per la correzione della vulnerabilità selezionata, abilitare l'opzione **Mostra solo le attività che consentono di correggere la vulnerabilità**.

5. Scegliere l'operazione da eseguire:

   - Per avviare un'attività, selezionare la casella di controllo accanto al nome dell'attività, quindi fare clic sul pulsante **Avvia**.

   - Per aggiungere una nuova regola a un'attività esistente:

     a. Selezionare la casella di controllo accanto al nome dell'attività, quindi fare clic sul pulsante **Aggiungi regola**.

     b. Nella pagina visualizzata configurare la nuova regola:

     - Regola per la correzione delle vulnerabilità di questo livello di criticità

       Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

       Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore alla criticità dell'aggiornamento selezionato (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

       Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

       Per impostazione predefinita, questa opzione è disabilitata.

     - **Regola per la correzione delle vulnerabilità tramite gli aggiornamenti dello stesso tipo dell'aggiornamento definito come consigliato per la vulnerabilità selezionata** (disponibile solo per le vulnerabilità del software Microsoft)

     - **Regola per la correzione delle vulnerabilità nelle applicazioni in base al fornitore selezionato** (disponibile solo per vulnerabilità del software di terze parti)

     - **Regola per la correzione di una vulnerabilità in tutte le versioni dell'applicazione selezionata** (disponibile solo per vulnerabilità software di terze parti)

     - **Regola per la correzione della vulnerabilità selezionata**

     - Approva aggiornamenti in grado di correggere la vulnerabilità

       L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

       Per impostazione predefinita, questa opzione è disabilitata.

     c. Fare clic sul pulsante **Aggiungi**.

   - Per creare un'attività:

     a. Fare clic sul pulsante **Nuova attività**.

b. Nella pagina visualizzata configurare la nuova regola:

- **Regola per la correzione delle vulnerabilità di questo livello di criticità**

  Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

  Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore alla criticità dell'aggiornamento selezionato (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

  Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Regola per la correzione delle vulnerabilità tramite gli aggiornamenti dello stesso tipo dell'aggiornamento definito come consigliato per la vulnerabilità selezionata** (disponibile solo per le vulnerabilità del software Microsoft)

- **Regola per la correzione delle vulnerabilità nelle applicazioni in base al fornitore selezionato** (disponibile solo per vulnerabilità del software di terze parti)

- **Regola per la correzione di una vulnerabilità in tutte le versioni dell'applicazione selezionata** (disponibile solo per vulnerabilità software di terze parti)

- **Regola per la correzione della vulnerabilità selezionata**

- **Approva aggiornamenti in grado di correggere la vulnerabilità**

  L'aggiornamento selezionato verrà approvato per l'installazione. Abilitare questa opzione se alcune delle regole applicate per l'installazione degli aggiornamenti consentono solo l'installazione degli aggiornamenti approvati.

  Per impostazione predefinita, questa opzione è disabilitata.

c. Fare clic sul pulsante **Aggiungi**.

Se è stato scelto di avviare un'attività, è possibile chiudere la procedura guidata. L'attività verrà completata in background. Non sono necessarie ulteriori operazioni.

Se si è scelto di aggiungere una regola a un'attività esistente, verrà visualizzata la finestra delle proprietà dell'attività. La nuova regola è già stata aggiunta alle proprietà dell'attività. È possibile visualizzare o modificare la regola o altre impostazioni dell'attività. Fare clic sul pulsante **Salva** per applicare le modifiche.

Se è stato scelto di creare un'attività, continuare a creare l'attività nella Creazione guidata nuova attività. La nuova regola aggiunta nella Correzione guidata vulnerabilità viene visualizzata nella Creazione guidata nuova attività. Al termine della procedura guidata, l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* verrà aggiunta all'elenco delle attività.

Creazione dell'attività Correggi vulnerabilità

L'attività *Correggi vulnerabilità* consente di correggere le vulnerabilità del software nei dispositivi gestiti che eseguono Windows. È possibile correggere le vulnerabilità del software di terze parti, incluso il software Microsoft.

Se non si dispone della licenza per Vulnerability e Patch Management, non è possibile creare nuove attività di tipo *Correggi vulnerabilità*. Per correggere nuove vulnerabilità, è possibile aggiungerle a un'attività *Correggi vulnerabilità* esistente. È consigliabile utilizzare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* anziché l'attività *Correggi vulnerabilità*. L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* consente di installare automaticamente più aggiornamenti e correggere più vulnerabilità, in base alle regole definite.

Può essere richiesta l'interazione con l'utente quando si aggiorna un'applicazione di terze parti o si corregge una vulnerabilità in un'applicazione di terze parti in un dispositivo gestito. All'utente può ad esempio essere richiesto di chiudere l'applicazione di terze parti se aperta al momento.

Per creare l'attività Correggi vulnerabilità:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Correggi vulnerabilità**.
4. Specificare il nome dell'attività che si intende creare.

   Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare i dispositivi a cui assegnare l'attività.
6. Fare clic sul pulsante **Aggiungi**.

   Verrà visualizzato l'elenco delle vulnerabilità.
7. Selezionare le vulnerabilità che si desidera correggere, quindi fare clic su **OK**.

   Le vulnerabilità del software Microsoft in genere dispongono di correzioni consigliate. Non sono necessarie ulteriori azioni per tali vulnerabilità. Per le vulnerabilità del software di altri produttori, è prima necessario specificare una correzione utente per ogni vulnerabilità da correggere. Sarà quindi possibile aggiungere tali vulnerabilità nell'attività *Correggi vulnerabilità*.

8. Specificare le impostazioni per il riavvio del sistema operativo:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ripeti la richiesta ogni (min.)**

  Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

  Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

- **Riavvia dopo (min.)**

  Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

  Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Forza la chiusura delle applicazioni nelle sessioni bloccate**

L'esecuzione di applicazioni potrebbe impedire il riavvio del dispositivo client. Ad esempio, se un documento viene modificato in un'applicazione per l'elaborazione di testo e non viene salvato, l'applicazione non consente il riavvio del dispositivo.

Se questa opzione è abilitata, viene forzata la chiusura di tali applicazioni in un dispositivo bloccato prima del riavvio del dispositivo. Come risultato, gli utenti possono perdere le modifiche non salvate.

Se questa opzione è disabilitata, un dispositivo bloccato non viene riavviato. Lo stato dell'attività nel dispositivo indica che è necessario un riavvio del dispositivo. Gli utenti devono chiudere manualmente tutte le applicazioni in esecuzione nei dispositivi bloccati e riavviare questi dispositivi.

Per impostazione predefinita, questa opzione è disabilitata.

9. Specificare le impostazioni per l'account:

- **Account predefinito**

  L'attività verrà eseguita tramite lo stesso account dell'applicazione che esegue l'attività.

  Per impostazione predefinita, questa opzione è selezionata.

- **Specifica account**

  Compilare i campi **Account** e **Password** per specificare i dettagli di un account con cui viene eseguita l'attività. L'account deve disporre di diritti sufficienti per questa attività.

- **Account**

  Account tramite il quale viene eseguita l'attività.

- **Password**

  Password dell'account con cui verrà eseguita l'attività.

10. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

11. Fare clic sul pulsante **Fine**.

    L'attività verrà creata e visualizzata nell'elenco delle attività.

12. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

13. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

14. Fare clic sul pulsante **Salva**.

L'attività verrà creata e configurata.

Creazione dell'attività Installa aggiornamenti richiesti e correggi vulnerabilità

L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* è disponibile solo con la licenza per Vulnerability e Patch Management.

L'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* viene utilizzata per aggiornare e correggere le vulnerabilità del software di terze parti, incluso il software Microsoft, installato nei dispositivi gestiti. Questa attività consente di installare più aggiornamenti e correggere più vulnerabilità in base a determinate regole.

Per installare aggiornamenti o correggere vulnerabilità utilizzando l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è possibile effettuare una delle seguenti operazioni:

- Eseguire l'Installazione guidata aggiornamenti o la Correzione guidata vulnerabilità.
- Creare un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.
- Aggiungere una regola per l'installazione dell'aggiornamento a un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* esistente.

Per creare un'attività Installa aggiornamenti richiesti e correggi vulnerabilità:

1. Nella finestra principale dell'applicazione, passare a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.
3. Per l'applicazione Kaspersky Security Center, selezionare il tipo di attività **Installa aggiornamenti richiesti e correggi vulnerabilità**.

   Se l'attività non viene visualizzata, verificare se l'account dispone dei diritti di **lettura**, **modifica** ed **esecuzione** per l'area funzionale **Gestione sistema**: **Vulnerability e patch management**. Senza questi diritti di accesso, non è possibile creare e configurare l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*.
4. Specificare il nome dell'attività che si intende creare. Il nome di un'attività non può superare i 100 caratteri e non può includere caratteri speciali ("*<>?\:|).
5. Selezionare i dispositivi a cui assegnare l'attività.

6. Specificare le regole per l'installazione dell'aggiornamento, quindi specificare le seguenti impostazioni:

- **Avvia l'installazione al riavvio o all'arresto del dispositivo**

  Se questa opzione è abilitata, gli aggiornamenti vengono installati al riavvio o all'arresto del dispositivo. In caso contrario, gli aggiornamenti vengono installati in base a una pianificazione.

  Utilizzare questa opzione se l'installazione degli aggiornamenti può influire sulle prestazioni del dispositivo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Installa i componenti generali del sistema richiesti**

  Se questa opzione è abilitata, prima di installare un aggiornamento l'applicazione installa automaticamente tutti i componenti di sistema generali (prerequisiti) richiesti per installare l'aggiornamento. Questi prerequisiti possono ad esempio essere aggiornamenti del sistema operativo.

  Se questa opzione è disabilitata, può essere necessario installare manualmente i prerequisiti.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Consenti l'installazione di nuove versioni dell'applicazione durante gli aggiornamenti**

  Se questa opzione è abilitata, gli aggiornamenti sono consentiti se implicano l'installazione di una nuova versione di un'applicazione software.

  Se questa opzione è disabilitata, l'upgrade del software non viene eseguito. È quindi possibile installare le nuove versioni del software manualmente o tramite un'altra attività. È ad esempio possibile utilizzare questa opzione se l'infrastruttura aziendale non è supportata da una nuova versione del software o se si desidera verificare un aggiornamento in un'infrastruttura di test.

  Per impostazione predefinita, questa opzione è abilitata.

  > L'upgrade dell'applicazione può causare un malfunzionamento delle applicazioni dipendenti installate nei dispositivi client.

- **Scarica gli aggiornamenti nel dispositivo senza installarli**

  Se questa opzione è abilitata, l'applicazione scarica gli aggiornamenti nel dispositivo client ma non li installa automaticamente. È quindi possibile installare manualmente gli aggiornamenti scaricati.

  Gli aggiornamenti Microsoft vengono scaricati nell'archiviazione di sistema di Windows. Gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft) vengono scaricati nella cartella specificata nel campo **Scarica aggiornamenti in**.

  Se questa opzione è disabilitata, gli aggiornamenti vengono installati automaticamente nel dispositivo.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Scarica aggiornamenti in**

  Questa cartella viene utilizzata per scaricare gli aggiornamenti delle applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft).

- **Abilita diagnostica avanzata**

  Se questa funzionalità è abilitata, Network Agent scrive i file di traccia anche se la scrittura dei file di traccia è disabilitata per Network Agent nell'utilità di diagnostica remota di Kaspersky Security Center. Le tracce vengono scritte alternativamente in due file. Le dimensioni totali di entrambi i file dipendono dal valore **Dimensione massima (in MB) dei file di diagnostica avanzata**. Quando entrambi i file sono completi, Network Agent avvia nuovamente la scrittura in tali file. I file con le tracce sono archiviati nella cartella %WINDIR%\Temp. Questi file sono accessibili nell'utilità di diagnostica remota. È possibile scaricarli o eliminarli tramite tale utilità.

  Se questa funzionalità è disabilitata, Network Agent scrive le tracce in base alle impostazioni nell'utilità di diagnostica remota di Kaspersky Security Center. Non viene eseguita la scrittura di ulteriori tracce.

  Durante la creazione di un'attività, non è necessario abilitare la diagnostica avanzata. È possibile utilizzare questa funzionalità in un secondo momento, ad esempio se l'esecuzione di un'attività non riesce in alcuni dispositivi e si desidera recuperare informazioni aggiuntive durante l'esecuzione di un'altra attività.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Dimensione massima (in MB) dei file di diagnostica avanzata**

  Il valore predefinito è 100 MB e i valori disponibili sono compresi tra 1 MB e 2048 MB. Gli specialisti del Servizio di assistenza tecnica di Kaspersky potrebbero richiedere di modificare il valore predefinito quando le informazioni nei file di diagnostica avanzata inviati non sono sufficienti per risolvere il problema.

7. Specificare le impostazioni per il riavvio del sistema operativo:

- **Non riavviare il dispositivo**

  I dispositivi client non vengono riavviati automaticamente al termine dell'operazione. Per completare l'operazione, è necessario riavviare un dispositivo (ad esempio, manualmente o tramite l'attività di gestione di un dispositivo). Le informazioni sul riavvio richiesto vengono salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**

  I dispositivi client vengono sempre riavviati automaticamente quando è richiesto un riavvio per il completamento dell'operazione. Questa opzione è utile per le attività nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**

  Sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). Questa opzione è adatta per le workstation in cui gli utenti devono essere in grado di selezionare l'orario che preferiscono per un riavvio del sistema.

  Per impostazione predefinita, questa opzione è selezionata.

- **Ripeti la richiesta ogni (min.)**

  Se questa opzione è abilitata, l'applicazione richiede all'utente di riavviare il sistema operativo con la frequenza specificata.

  Per impostazione predefinita, questa opzione è abilitata. L'intervallo predefinito è di 5 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

  Se questa opzione è disabilitata, la richiesta viene visualizzata una sola volta.

- **Riavvia dopo (min.)**

  Dopo la richiesta all'utente, l'applicazione forza il riavvio del sistema operativo al termine dell'intervallo di tempo specificato.

  Per impostazione predefinita, questa opzione è abilitata. Il ritardo predefinito è di 30 minuti. I valori disponibili sono compresi tra 1 e 1440 minuti.

- **Tempo di attesa prima della chiusura forzata delle applicazioni nelle sessioni bloccate (min.)**

Viene forzata la chiusura delle applicazioni quando il dispositivo dell'utente viene bloccato (automaticamente dopo un intervallo di inattività specificato o manualmente).

Se questa opzione è abilitata, viene forzata la chiusura delle applicazioni nel dispositivo bloccato alla scadenza dell'intervallo di tempo specificato nel campo di immissione.

Se questa opzione è disabilitata, le applicazioni nel dispositivo bloccato non vengono chiuse.

Per impostazione predefinita, questa opzione è disabilitata.

8. Se si desidera modificare le impostazioni predefinite dell'attività, abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** nella pagina **Completare la creazione dell'attività**. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

9. Fare clic sul pulsante **Fine**.

   L'attività verrà creata e visualizzata nell'elenco delle attività.

10. Fare clic sul nome dell'attività creata per aprire la finestra delle proprietà dell'attività.

11. Nella finestra delle proprietà dell'attività specificare le impostazioni generali dell'attività in base alle proprie esigenze.

12. Fare clic sul pulsante **Salva**.

    L'attività verrà creata e configurata.

Se i risultati dell'attività contengono l'avviso 0x80240033 "Errore di Windows Update Agent 80240033 ("Non è stato possibile scaricare le condizioni di licenza")", è possibile risolvere questo problema tramite il Registro di sistema di Windows.

Aggiunta delle regole per l'installazione dell'aggiornamento

Questa funzionalità è disponibile solo con la licenza Vulnerability e patch management.

Durante l'installazione di aggiornamenti software o la correzione di vulnerabilità del software tramite l'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*, è necessario specificare le regole per l'installazione degli aggiornamenti. Queste regole determinano gli aggiornamenti da installare e le vulnerabilità da correggere.

Le esatte impostazioni dipendono dall'esigenza di aggiungere una regola per tutti gli aggiornamenti, per gli aggiornamenti di Windows Update o per gli aggiornamenti di applicazioni di terze parti (applicazioni fornite da produttori di software diversi da Kaspersky e Microsoft). Durante l'aggiunta di una regola per gli aggiornamenti di Windows Update o per gli aggiornamenti di applicazioni di terze parti, è possibile selezionare le specifiche applicazioni e versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Durante l'aggiunta di una regola per tutti gli aggiornamenti, è possibile selezionare gli specifici aggiornamenti da installare e le vulnerabilità che si desidera correggere tramite l'installazione degli aggiornamenti.

È possibile aggiungere una regola per l'installazione degli aggiornamenti nei modi seguenti:

- Aggiungendo una regola durante la creazione di una nuova attività Installa aggiornamenti richiesti e correggi vulnerabilità.
- Aggiungendo una regola nella scheda **Impostazioni applicazione** nella finestra delle proprietà di un'attività *Installa aggiornamenti richiesti e correggi vulnerabilità* esistente.
- Tramite l'Installazione guidata aggiornamenti o la Correzione guidata vulnerabilità.

Per aggiungere una nuova regola per tutti gli aggiornamenti:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per tutti gli aggiornamenti**.

3. Nella pagina **Criteri generali** utilizzare gli elenchi a discesa per specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Aggiornamenti** selezionare gli aggiornamenti da installare:

   - **Installa tutti gli aggiornamenti appropriati**

     Installa tutti gli aggiornamenti software che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

   - **Installa solo gli aggiornamenti nell'elenco**

     Installa solo gli aggiornamenti software che selezionati manualmente dall'elenco. Questo elenco contiene tutti gli aggiornamenti software disponibili.

     Ad esempio, è possibile selezionare aggiornamenti specifici nei seguenti casi: per verificarne l'installazione in un ambiente di test, per aggiornare solo le applicazioni critiche o per aggiornare solo specifiche applicazioni.

     - **Installa automaticamente tutti gli aggiornamenti precedenti dell'applicazione necessari per l'installazione degli aggiornamenti selezionati**

       Mantenere abilitata questa opzione se si desidera consentire l'installazione delle versioni intermedie delle applicazioni quando questa operazione è necessaria per l'installazione degli aggiornamenti selezionati.

       Se questa opzione è disabilitata, vengono installate solo le versioni delle applicazioni selezionate. Disabilitare questa opzione se si desidera aggiornare le applicazioni in modo diretto, senza tentare di installare le versioni successive in modo incrementale. Se l'installazione degli aggiornamenti selezionati non è possibile senza installare le versioni precedenti delle applicazioni, l'aggiornamento dell'applicazione non riesce.

       Si supponga di avere la versione 3 di un'applicazione installata in un dispositivo e di voler eseguire l'aggiornamento alla versione 5, ma la versione 5 di questa applicazione può essere installata solo sulla versione 4. Se questa opzione è abilitata, il software installa prima la versione 4 e quindi la versione 5. Se questa opzione è disabilitata, il software non riesce a eseguire l'aggiornamento l'applicazione.

       Per impostazione predefinita, questa opzione è abilitata.

5. Nella pagina **Vulnerabilità** selezionare le vulnerabilità da correggere tramite l'installazione degli aggiornamenti selezionati:

   - **Correggi tutte le vulnerabilità che corrispondono ad altri criteri**

     Verranno corrette tutte le vulnerabilità che soddisfano i criteri specificati nella pagina **Criteri generali** della procedura guidata. Opzione selezionata per impostazione predefinita.

   - **Correggi solo le vulnerabilità nell'elenco**

     Verranno corrette solo le vulnerabilità selezionate manualmente dall'elenco. Questo elenco contiene tutte le vulnerabilità rilevate.

     Ad esempio, è possibile selezionare vulnerabilità specifiche nei seguenti casi: per verificarne la correzione in un ambiente di test, per correggere solo le vulnerabilità di applicazioni critiche o per correggere le vulnerabilità solo in specifiche applicazioni.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Per aggiungere una nuova regola per gli aggiornamenti di Windows Update:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per Windows Update**.

3. Nella finestra **Criteri generali** specificare le seguenti impostazioni:

   - **Set di aggiornamenti da installare**

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - **Correggi le vulnerabilità con un livello di criticità uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

   - **Correggi le vulnerabilità con un livello di criticità MSRC uguale o superiore a**

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Microsoft Security Response Center (MSRC) è uguale o superiore al valore selezionato nell'elenco (**Basso**, **Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Categorie di aggiornamenti** selezionare le categorie di aggiornamenti da installare. Queste categorie sono identiche a quelle del catalogo di Microsoft Update. Per impostazione predefinita, tutte le categorie sono selezionate.

6. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione **Impostazioni** della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Per aggiungere una nuova regola per gli aggiornamenti delle applicazioni di terze parti:

1. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione regole guidata. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Nella pagina **Tipo di regola** selezionare **Regola per gli aggiornamenti di terze parti**.

3. Nella finestra **Criteri generali** specificare le seguenti impostazioni:

   - Set di aggiornamenti da installare

     Selezionare gli aggiornamenti che devono essere installati nei dispositivi client:

     - **Installa solo gli aggiornamenti approvati**. Verranno installati solo gli aggiornamenti approvati.
     - **Installa tutti gli aggiornamenti (tranne quelli rifiutati)**. Verranno installati gli aggiornamenti con lo stato di approvazione *Approvato* o *Indefinito*.
     - **Installa tutti gli aggiornamenti (inclusi quelli rifiutati)**. Verranno installati tutti gli aggiornamenti, indipendentemente dal relativo stato di approvazione. Prestare attenzione quando si seleziona questa opzione. Ad esempio, utilizzare questa opzione se si desidera controllare l'installazione di alcuni aggiornamenti rifiutati in un'infrastruttura di test.

   - Correggi le vulnerabilità con un livello di criticità uguale o superiore a

     Talvolta gli aggiornamenti software possono compromettere l'esperienza utente con il software. In questi casi, è possibile decidere di installare solo gli aggiornamenti critici per l'esecuzione del software e ignorare gli altri aggiornamenti.

     Se questa opzione è abilitata, gli aggiornamenti correggono solo le vulnerabilità per cui il livello di criticità impostato da Kaspersky è uguale o superiore al valore selezionato nell'elenco (**Medio**, **Alto** o **Critico**). Le vulnerabilità con un livello di criticità inferiore al valore selezionato non vengono corrette.

     Se questa opzione è disabilitata, gli aggiornamenti correggono tutte le vulnerabilità, indipendentemente dal livello di criticità.

     Per impostazione predefinita, questa opzione è disabilitata.

4. Nella pagina **Applicazioni** selezionare le applicazioni e le versioni delle applicazioni per cui si desidera installare gli aggiornamenti. Per impostazione predefinita, tutte le applicazioni sono selezionate.

5. Nella pagina **Nome** specificare il nome della regola che si intende creare. È possibile modificare questo nome in un secondo momento nella sezione Impostazioni della finestra delle proprietà dell'attività creata.

Al termine della Creazione regole guidata, la nuova regola verrà aggiunta e visualizzata nell'elenco delle regole nella Creazione guidata nuova attività o nelle proprietà dell'attività.

Selezione di correzioni utente per le vulnerabilità del software di terze parti

Per utilizzare l'attività *Correggi vulnerabilità*, è necessario specificare manualmente gli aggiornamenti software per correggere le vulnerabilità del software di terze parti elencato nelle impostazioni dell'attività. L'attività *Correggi vulnerabilità* utilizza le correzioni consigliate per il software Microsoft e le correzioni dell'utente per altri software di terze parti. Le *correzioni dell'utente* sono aggiornamenti software per correggere le vulnerabilità che l'amministratore specifica manualmente per l'installazione.

Per selezionare le correzioni utente per le vulnerabilità del software di terze parti:

1. Nel menu principale accedere a **Operazioni → Gestione patch → Vulnerabilità del software**.

   La pagina visualizzerà l'elenco delle vulnerabilità del software rilevate nei dispositivi client.

2. Nell'elenco delle vulnerabilità del software fare clic sul collegamento con il nome della vulnerabilità del software per cui si desidera specificare una correzione utente.

   Verrà visualizzata la finestra delle proprietà della vulnerabilità.

3. Nel riquadro sinistro selezionare la sezione **Correzioni utente e altre correzioni**.

   Verrà visualizzato l'elenco delle correzioni utente per la vulnerabilità del software selezionata.

4. Fare clic su **Aggiungi**.

   Verrà visualizzato l'elenco dei pacchetti di installazione disponibili. L'elenco dei pacchetti di installazione visualizzati corrisponde all'elenco **Operazioni → Archivi → Pacchetti di installazione**. Se non è stato creato un pacchetto di installazione contenente una correzione utente per la vulnerabilità selezionata, è possibile creare il pacchetto subito avviando la Creazione guidata nuovo pacchetto.

5. Selezionare un pacchetto di installazione (o più pacchetti) contenente una correzione utente (o correzioni utente) per la vulnerabilità del software di terze parti.

6. Fare clic su **Salva**.

Vengono specificati i pacchetti di installazione contenenti le correzioni utente per la vulnerabilità del software. Quando l'attività *Correggi vulnerabilità* viene avviata, il pacchetto di installazione verrà installato e la vulnerabilità del software verrà corretta.

Visualizzazione delle informazioni sulle vulnerabilità del software rilevate in tutti i dispositivi gestiti

Dopo aver eseguito la scansione del software nei dispositivi gestiti per individuare eventuali vulnerabilità, è possibile visualizzare l'elenco delle vulnerabilità del software rilevate in tutti i dispositivi gestiti. Se si esegue l'attività per la gerarchia di Administration Server, è possibile visualizzare l'elenco dei dispositivi gestiti con vulnerabilità rilevate solo per l'Administration Server selezionato.

Per visualizzare l'elenco delle vulnerabilità del software rilevate in tutti i dispositivi gestiti:

Nel menu principale accedere a **Operazioni → Gestione patch → Vulnerabilità del software**.

La pagina visualizzerà l'elenco delle vulnerabilità del software rilevate nei dispositivi client.

È anche possibile generare e visualizzare un Rapporto sulle vulnerabilità.

È possibile specificare un filtro per visualizzare l'elenco delle vulnerabilità del software. Fare clic sull'icona **Filtro** ( ) nell'angolo superiore destro dell'elenco delle vulnerabilità del software per gestire il filtro. È anche possibile selezionare uno dei filtri preimpostati dall'elenco a discesa **Filtri preimpostati** sopra l'elenco delle vulnerabilità del software.

È possibile ottenere informazioni dettagliate su qualsiasi vulnerabilità nell'elenco.

Per ottenere informazioni su una vulnerabilità del software:

Nell'elenco delle vulnerabilità del software fare clic sul collegamento con il nome della vulnerabilità.

Verrà visualizzata la finestra delle proprietà della vulnerabilità del software.

Visualizzazione delle informazioni sulle vulnerabilità del software rilevate nel dispositivo gestito selezionato

È possibile visualizzare le informazioni sulle vulnerabilità del software rilevate nel dispositivo gestito selezionato che esegue Windows.

Per visualizzare l'elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato:

1. Nel menu principale, accedere a **Risorse (dispositivi)** →**Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo per cui si desidera visualizzare le vulnerabilità del software rilevate.

   Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.

3. Nella finestra delle proprietà del dispositivo selezionato selezionare la scheda **Avanzate**.

4. Nel riquadro sinistro selezionare la sezione **Vulnerabilità del software**.

Verrà visualizzato l'elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato.

Per visualizzare le proprietà della vulnerabilità del software selezionata:

Fare clic sul collegamento con il nome della vulnerabilità del software nell'elenco delle vulnerabilità del software.

Verrà visualizzata la finestra delle proprietà della vulnerabilità del software selezionata.

Visualizzazione delle statistiche delle vulnerabilità nei dispositivi gestiti

È possibile visualizzare le statistiche per ogni vulnerabilità del software nei dispositivi gestiti. Le statistiche sono rappresentate sotto forma di diagramma. Il diagramma mostra il numero di dispositivi con i seguenti stati:

- *Ignorato in: <numero di dispositivi>*. Questo stato viene assegnato se, nelle proprietà della vulnerabilità, è stata impostata manualmente l'opzione per ignorare la vulnerabilità.
- *Corretto in: <numero di dispositivi>*. Questo stato viene assegnato se l'attività di correzione della vulnerabilità è stata completata.
- *Correzione pianificata in data: <numero di dispositivi>*. Questo stato viene assegnato se è stata creata l'attività per correggere la vulnerabilità ma l'attività non è ancora stata eseguita.
- *Patch applicata in: <numero di dispositivi>*. Questo stato viene assegnato se è stato selezionato manualmente un aggiornamento software per correggere la vulnerabilità ma questo software aggiornato non ha corretto la vulnerabilità.
- *È necessaria una correzione in: <numero di dispositivi>*. Questo stato viene assegnato se la vulnerabilità è stata corretta solo in alcuni dispositivi gestiti e deve essere corretta in più dispositivi gestiti.

Per visualizzare le statistiche di una vulnerabilità nei dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Vulnerabilità del software**.

   La pagina visualizza un elenco delle vulnerabilità nelle applicazioni rilevate nei dispositivi gestiti.

2. Selezionare la casella di controllo accanto alla vulnerabilità richiesta.
3. Fare clic sul pulsante **Statistiche di vulnerabilità nei dispositivi**

Verrà visualizzato un diagramma degli stati della vulnerabilità. Facendo clic su uno stato, viene aperto un elenco dei dispositivi in cui la vulnerabilità ha lo stato selezionato.

Esportazione dell'elenco delle vulnerabilità del software in un file

È possibile esportare l'elenco visualizzato delle vulnerabilità in file CSV o TXT. È ad esempio possibile utilizzare questi file per inviarli al responsabile della sicurezza delle informazioni o per archiviarli a fini statistici.

Per esportare in un file di testo l'elenco delle vulnerabilità del software rilevate in tutti i dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Vulnerabilità del software**.

   La pagina visualizza un elenco delle vulnerabilità nelle applicazioni rilevate nei dispositivi gestiti.

2. Fare clic sul pulsante **Esporta in TXT** o **Esporta in CSV**, a seconda del formato preferito per l'esportazione.

Il file contenente l'elenco delle vulnerabilità del software verrà scaricato nel dispositivo in uso.

Per esportare in un file di testo l'elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato:

1. Aprire l'elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato.
2. Selezionare le vulnerabilità del software che si desidera esportare.

   Ignorare questo passaggio se si desidera esportare un elenco completo delle vulnerabilità del software rilevate nel dispositivo gestito.

   Se si desidera esportare l'elenco completo delle vulnerabilità del software rilevate nel dispositivo gestito, verranno esportate solo le vulnerabilità visualizzate nella pagina corrente.
3. Fare clic sul pulsante **Esporta in TXT** o **Esporta in CSV**, a seconda del formato preferito per l'esportazione.

Il file contenente l'elenco delle vulnerabilità del software rilevate nel dispositivo gestito selezionato verrà scaricato nel dispositivo in uso.

Ignorare le vulnerabilità del software

È possibile ignorare le vulnerabilità del software da correggere. I motivi per ignorare le vulnerabilità del software potrebbero essere, ad esempio, i seguenti:

- La vulnerabilità del software non viene considerata critica per l'organizzazione.
- Si ritiene che la correzione della vulnerabilità del software possa danneggiare i dati relativi al software per cui era necessaria la correzione della vulnerabilità.
- Si ha la certezza che la vulnerabilità del software non sia pericolosa per la rete dell'organizzazione in quanto si utilizzano altre misure per proteggere i dispositivi gestiti.

È possibile ignorare una vulnerabilità del software in tutti i dispositivi gestiti o solo nei dispositivi gestiti selezionati.

Per ignorare una vulnerabilità del software in tutti i dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni** → **Gestione patch** → **Vulnerabilità del software**.

   La pagina visualizzerà l'elenco delle vulnerabilità del software rilevate nei dispositivi gestiti.
2. Nell'elenco delle vulnerabilità del software fare clic sul collegamento con il nome della vulnerabilità del software che si desidera ignorare.

   Verrà visualizzata la finestra delle proprietà delle vulnerabilità del software.
3. Nella scheda **Generale** abilitare l'opzione **Ignora vulnerabilità**.
4. Fare clic sul pulsante **Salva**.

   Verrà chiusa la finestra delle proprietà delle vulnerabilità del software.

La vulnerabilità del software viene ignorata in tutti i dispositivi gestiti.

Per ignorare una vulnerabilità del software nel dispositivo gestito selezionato:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.

2. Nell'elenco dei dispositivi gestiti fare clic sul collegamento con il nome del dispositivo in cui si desidera ignorare una vulnerabilità del software.

   Verrà visualizzata la finestra delle proprietà del dispositivo.

3. Nella finestra delle proprietà del dispositivo selezionare la scheda **Avanzate**.

4. Nel riquadro sinistro selezionare la sezione **Vulnerabilità del software**.

   Verrà visualizzato l'elenco delle vulnerabilità del software rilevate nel dispositivo.

5. Nell'elenco delle vulnerabilità del software selezionare la vulnerabilità che si desidera ignorare nel dispositivo selezionato.

   Verrà visualizzata la finestra delle proprietà delle vulnerabilità del software.

6. Nella finestra delle proprietà della vulnerabilità del software, nella scheda **Generale**, abilitare l'opzione **Ignora vulnerabilità**.

7. Fare clic sul pulsante **Salva**.

   Verrà chiusa la finestra delle proprietà delle vulnerabilità del software.

8. Chiudere la finestra delle proprietà del dispositivo.

La vulnerabilità del software viene ignorata nel dispositivo selezionato.

La vulnerabilità del software ignorata non verrà corretta dopo il completamento dell'attività *Correggi vulnerabilità* o dell'attività *Installa aggiornamenti richiesti e correggi vulnerabilità*. È possibile escludere le vulnerabilità del software ignorate dall'elenco delle vulnerabilità utilizzando il filtro.

Gestione delle applicazioni in esecuzione nei dispositivi client

Questa sezione descrive le funzionalità di Kaspersky Security Center relative alla gestione delle applicazioni eseguite nei dispositivi client.

Utilizzo di Controllo Applicazioni per gestire i file eseguibili

È possibile utilizzare il componente Controllo Applicazioni per consentire o bloccare l'avvio dei file eseguibili nei dispositivi dell'utente. Il componente Controllo Applicazioni supporta i sistemi operativi basati su Windows e Linux.

Per i sistemi operativi basati su Linux, il componente Application Control è disponibile a partire da Kaspersky Endpoint Security 11.2 per Linux. Inoltre, il componente è disponibile per Kaspersky Embedded Systems Security per Windows 3.0 o versioni successive.

Prerequisiti

- Kaspersky Security Center viene distribuito nell'organizzazione.
- Il criterio di Kaspersky Endpoint Security for Windows o Kaspersky Endpoint Security for Linux è stato creato ed è attivo.
- Il criterio di Kaspersky Embedded Systems Security for Windows o Kaspersky Embedded Systems Security for Linux è stato creato ed è attivo.

Passaggi

Lo scenario di utilizzo di Controllo Applicazioni prevede diversi passaggi:

1. **Creazione e visualizzazione dell'elenco dei file eseguibili nei dispositivi client**

   Questo passaggio consente di scoprire quali file eseguibili sono presenti nei dispositivi gestiti. Visualizzare l'elenco dei file eseguibili e confrontarlo con l'elenco dei file eseguibili consentiti e non consentiti. Le restrizioni relative all'utilizzo dei file eseguibili possono essere correlate ai criteri di sicurezza delle informazioni dell'organizzazione.

   Istruzioni dettagliate:

   - Administration Console: Inventario dei file eseguibili
   - Kaspersky Security Center Web Console: Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client

2. **Creazione di categorie per i file eseguibili utilizzati nell'organizzazione**

   Analizzare gli elenchi dei file eseguibili archiviati nei dispositivi gestiti. In base all'analisi, creare categorie per i file eseguibili. È consigliabile creare una categoria "Applicazioni di lavoro" che includa il set standard di file eseguibili utilizzati nell'organizzazione. Se differenti gruppi di sicurezza utilizzano i propri set di file eseguibili nel proprio lavoro, è possibile creare una categoria distinta per ciascun gruppo di sicurezza.

   Istruzioni dettagliate:

   - Administration Console: Creazione di una categoria di applicazioni con contenuto aggiunto manualmente, Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati, Creazione di una categoria di applicazioni che include i file eseguibili in una cartella selezionata.
   - Kaspersky Security Center Web Console: Creazione di una categoria di applicazioni con contenuto aggiunto manualmente, Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati, Creazione di una categoria di applicazioni che include i file eseguibili in una cartella specifica.

3. **Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security**

   Configurare il componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security utilizzando le categorie create nel passaggio precedente.

   Istruzioni dettagliate:

   - Administration Console: Configurazione della gestione dell'avvio delle applicazioni nei dispositivi client
   - Kaspersky Security Center Web Console: Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

4. **Configurazione di Controllo Applicazioni nel criterio dell'applicazione Kaspersky Embedded Systems Security**

Configurare il componente Controllo applicazioni nel criterio Kaspersky Embedded Systems Security for Windows utilizzando le categorie create. Per ulteriori informazioni sul componente Controllo applicazioni, fare riferimento alla Guida di Kaspersky Embedded Systems Security for Windows o alla Guida di Kaspersky Embedded Systems Security for Linux.

Se si utilizza un numero elevato di regole, potrebbe verificarsi un errore durante il caricamento del criterio. È possibile aumentare la dimensione massima della richiesta in byte utilizzando i seguenti comandi:

- Per la richiesta JSON:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfJsonRequestInBytes -v <max_request_size> -t d
  ```

- Per la richiesta HTTP:

  ```
  klscflag -fset -pv ".core/.independent" -s KLLIM -n
  LP_KLOAPI_MaxSizeOfHttpRequestInBytes -v <max_request_size> -t d
  ```

  Dove `<max_request_size>` è la dimensione massima della richiesta in byte (ad esempio, `200000000`).

5. **Attivazione del componente Controllo Applicazioni in modalità di test**

   Per garantire che le regole di Controllo Applicazioni non blocchino i file eseguibili richiesti per il lavoro dell'utente, è consigliabile abilitare il test delle regole di Controllo Applicazioni e analizzarne il funzionamento dopo aver creato le nuove regole. Quando il test è abilitato, Kaspersky Endpoint Security for Windows o Kaspersky Embedded Systems Security non bloccherà i file eseguibili il cui avvio non è consentito dalle regole di Controllo Applicazioni, ma invierà invece notifiche sul relativo avvio ad Administration Server.

   Durante il test delle regole di Controllo Applicazioni, è consigliabile eseguire le seguenti azioni:

   - Determinare il periodo di test. Il periodo di test può variare da alcuni giorni a due mesi.
   - Esaminare gli eventi risultanti dal test del funzionamento di Controllo Applicazioni.

   Istruzioni dettagliate per Kaspersky Security Center Web Console: Configurazione del componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows. Seguire queste istruzioni e abilitare l'opzione **Modalità test** nel processo di configurazione.

6. **Modifica delle impostazioni delle categorie del componente Controllo Applicazioni**

   Se necessario, apportare modifiche alle impostazioni di Controllo Applicazioni. In base ai risultati del test, è possibile aggiungere i file eseguibili correlati agli eventi del componente Controllo Applicazioni a una categoria con contenuto aggiunto manualmente.

   Istruzioni dettagliate:

   - Administration Console: Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni
   - Kaspersky Security Center Web Console: Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni

7. **Applicazione delle regole di Controllo Applicazioni in modalità operativa**

   Dopo aver testato le regole di Controllo Applicazioni e completato la configurazione delle categorie, è possibile applicare le regole di Controllo Applicazioni in modalità operativa.

   Istruzioni dettagliate per Kaspersky Security Center Web Console: Configurazione del componente Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows. Seguire queste istruzioni e disabilitare l'opzione **Modalità test** nel processo di configurazione.

8. **Verifica della configurazione di Controllo Applicazioni**

   Assicurarsi di avere eseguito le seguenti operazioni:

- Categorie create per i file eseguibili.
- Configurazione di Controllo Applicazioni tramite le categorie.
- Applicazione delle regole di Controllo Applicazioni in modalità operativa.

Risultati

Al termine dello scenario, viene controllato l'avvio dei file eseguibili nei dispositivi gestiti. Gli utenti possono eseguire solo i file eseguibili consentiti nell'organizzazione e non possono eseguire quelli non consentiti.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Guida di Kaspersky Embedded Systems Security for Windows
- Guida di Kaspersky Embedded Systems Security for Linux

Modalità e categorie di Controllo Applicazioni

Il componente Controllo Applicazioni monitora i tentativi degli utenti di avviare i file eseguibili. È possibile utilizzare le regole di Controllo Applicazioni per controllare l'avvio dei file eseguibili.

Il componente Controllo Applicazioni è disponibile per Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security 11.2 for Linux e versioni successive e per Kaspersky Security for Virtualization Light Agent. Tutte le istruzioni in questa sezione descrivono la configurazione di Controllo Applicazioni per Kaspersky Endpoint Security for Windows.

L'avvio di file eseguibili le cui impostazioni non corrispondono ad alcuna delle regole di Controllo Applicazioni è regolato dalla modalità operativa selezionata del componente:

- *Lista vietati*. La modalità viene utilizzata se si desidera consentire l'avvio di tutti i file eseguibili tranne quelli specificati nelle regole di blocco. Questa modalità è selezionata per impostazione predefinita.
- *Lista consentiti*. La modalità viene utilizzata se si desidera bloccare l'avvio di tutti i file eseguibili tranne quelli specificati nelle regole di permesso.

Le regole di Controllo Applicazioni sono implementate tramite categorie per i file eseguibili. In Kaspersky Security Center, esistono tre tipi di categorie:

- Categoria con contenuto aggiunto manualmente. Vengono definite le condizioni (ad esempio, metadati del file, codice hash del file, certificato del file, categoria KL o percorso del file) per includere i file eseguibili nella categoria.
- Categoria che include i file eseguibili dei dispositivi selezionati. Viene specificato un dispositivo che contiene i file eseguibili inclusi automaticamente nella categoria.
- Categoria che include i file eseguibili in una cartella selezionata. Viene specificata una cartella che contiene i file eseguibili inclusi automaticamente nella categoria.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Guida di Kaspersky Embedded Systems Security for Windows
- Guida di Kaspersky Embedded Systems Security for Linux

Recupero e visualizzazione di un elenco dei file eseguibili archiviati nei dispositivi client

È possibile ottenere l'elenco dei file eseguibili archiviati sui dispositivi client in uno dei seguenti modi:

- Abilitazione delle notifiche sull'avvio delle applicazioni nel criterio di Kaspersky Endpoint Security.
- Creazione di un'attività di inventario.

Abilitazione delle notifiche sull'avvio delle applicazioni nel criterio di Kaspersky Endpoint Security

Per abilitare le notifiche sull'avvio delle applicazioni:

1. Aprire le impostazioni dei criteri di Kaspersky Endpoint Security, quindi passare a **Impostazioni generali** → **Rapporti e archivi**.
2. Nel gruppo di impostazioni **Trasferimento dati ad Administration Server**, selezionare la casella di controllo **Informazioni sulle applicazioni avviate** e salvare le modifiche.

Quando un utente tenta di avviare file eseguibili, le informazioni su tali file vengono aggiunte all'elenco dei file eseguibili su un dispositivo client. Kaspersky Endpoint Security invia queste informazioni a Network Agent, che a sua volta le invia ad Administration Server.

Creazione di un'attività di inventario

La funzione di inventario dei file eseguibili è disponibile per le seguenti applicazioni:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux versione 11.2 e successive
- Kaspersky Security for Virtualization 4.0 Light Agent e versioni successive

È possibile ridurre il carico sul database mentre si ottengono informazioni sulle applicazioni installate. Per risparmiare spazio nel database, eseguire un'attività di inventario sui dispositivi di riferimento in cui è installato un set standard di software. Il numero preferibile di dispositivi è 1-3.

Si sconsiglia vivamente di eseguire l'attività di inventario quando si utilizzano i seguenti database: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (tutte le edizioni).

Per creare un'attività di inventario per i file eseguibili nei dispositivi client:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.

   Verrà visualizzato l'elenco delle attività.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività. Seguire le istruzioni della procedura guidata.

3. Nella pagina **Impostazioni nuova attività**, nell'elenco a discesa **Applicazione**, selezionare Kaspersky Endpoint Security for Windows o Kaspersky Endpoint Security for Linux, a seconda del tipo di sistema operativo dei dispositivi client.

4. Nell'elenco a discesa **Tipo di attività** selezionare **Inventario**.

5. Nella pagina **Completare la creazione dell'attività** fare clic sul pulsante **Fine**.

   Al termine della Creazione guidata nuova attività, l'attività **Inventario** sarà creata e configurata. Se si desidera, è possibile modificare le impostazioni per l'attività creata. La nuova attività creata verrà visualizzata nell'elenco delle attività.

Per una descrizione dettagliata dell'attività di inventario, fare riferimento alle seguenti Guide:

- Guida di Kaspersky Endpoint Security for Windows
- Guida di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Dopo l'esecuzione dell'attività **Inventario**, viene formato l'elenco dei file eseguibili archiviati nei dispositivi gestiti ed è possibile visualizzarlo.

Durante l'esecuzione dell'attività di inventario, è possibile rilevare file eseguibili nei seguenti formati (a seconda dell'opzione selezionata nelle proprietà dell'attività di inventario): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Visualizzazione dell'elenco dei file eseguibili archiviati nei dispositivi gestiti

Per visualizzare l'elenco dei file eseguibili archiviati nei dispositivi client:

Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → File eseguibili**.

La pagina visualizzerà l'elenco dei file eseguibili archiviati nei dispositivi client.

Se necessario, è possibile inviare il file eseguibile del dispositivo gestito al dispositivo su cui è aperta Kaspersky Security Center Web Console.

Per inviare un file eseguibile:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → File eseguibili**.
2. Fare clic sul collegamento del file eseguibile che si desidera inviare.
3. Nella finestra visualizzata, accedere alla sezione **Dispositivi**, quindi selezionare la casella di controllo del dispositivo gestito da cui si desidera inviare il file eseguibile.

   Prima di inviare il file eseguibile, assicurarsi che il dispositivo gestito disponga di una connessione diretta ad Administration Server selezionando la casella di controllo **Non eseguire la disconnessione da Administration Server**.

4. Fare clic sul pulsante **Invia**.

   Il file eseguibile selezionato viene scaricato per essere inviato al dispositivo su cui è aperta Kaspersky Security Center Web Console.

Creazione di una categoria di applicazioni con contenuto aggiunto manualmente

È possibile specificare un set di criteri come modello per i file eseguibili di cui consentire o bloccare l'avvio nell'organizzazione. In base ai file eseguibili corrispondenti ai criteri, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per creare una categoria di applicazioni con contenuto aggiunto manualmente:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Categorie di applicazioni**.

   Verrà visualizzata la pagina con un elenco di categorie di applicazioni.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nel passaggio **Selezionare il metodo di creazione della categoria**, selezionare l'opzione **Categoria con contenuto aggiunto manualmente. I dati dei file eseguibili vengono aggiunti alla categoria in modo manuale**.

4. Nel passaggio **Condizioni**, fare clic sul pulsante **Aggiungi** per aggiungere un criterio di condizione per includere i file nella creazione della categoria.

5. Nel passaggio **Criteri condizione** selezionare un tipo di regola per la creazione della categoria dall'elenco:

- **Da categoria KL**

  Se questa opzione è selezionata, è possibile specificare una categoria di applicazioni Kaspersky come condizione per l'aggiunta di applicazioni alla categoria utente. Le applicazioni della categoria Kaspersky specificata verranno aggiunte alla categoria utente di applicazioni.

- **Seleziona certificato dall'archivio**

  Se questa opzione è selezionata, è possibile specificare i certificati dell'archivio. La condizione di categoria corrisponde solo ai file eseguibili firmati dal certificato specificato.

  I certificati vengono aggiunti all'archivio se è stata creata e avviata un'attività di inventario o se è stata selezionata la casella di controllo **Informazioni sulle applicazioni avviate** nel criterio di Kaspersky Endpoint Security. È possibile eseguire entrambe le azioni.

- **Specificare il percorso dell'applicazione (maschere supportate)**

  Se questa opzione è selezionata, è possibile specificare il percorso di un file o una cartella nel dispositivo client che contiene i file eseguibili da aggiungere alla categoria utente di applicazioni. È possibile utilizzare espressioni regolari come *C:\path_to_exe**, ad esempio: *C:\Program Files\Internet Explorer**.

- **Unità rimovibile**

  Se questa opzione è selezionata, è possibile specificare il tipo di supporto (qualsiasi unità o unità rimovibile) in cui viene eseguita l'applicazione. Le applicazioni che sono state eseguite nel tipo di unità selezionato verranno aggiunte alla categoria utente di applicazioni.

- **Hash, metadati o certificato**:

  - **Selezionare dall'elenco dei file eseguibili**

    Se questa opzione è selezionata, è possibile utilizzare l'elenco dei file eseguibili nel dispositivo client per selezionare e aggiungere applicazioni alla categoria.

  - **Selezionare dal registro delle applicazioni**

Se questa opzione è selezionata, viene visualizzato il registro delle applicazioni. Dopo aver selezionato un'applicazione dal registro, viene aperta una finestra con i parametri compilati con i metadati dell'applicazione selezionata:

- Nome file.
- Versione file. È possibile specificare un valore preciso per la versione o descrivere una condizione, ad esempio "maggiore di 5.0".
- Nome applicazione.
- Versione applicazione. È possibile specificare un valore preciso per la versione o descrivere una condizione, ad esempio "maggiore di 5.0".
- Vendor.

Viene bloccato solo l'avvio dei file eseguibili che soddisfano i parametri specificati, non l'avvio dell'applicazione selezionata. Se i metadati dell'applicazione selezionata corrispondono a quelli del file eseguibile avviato all'avvio dell'applicazione, è possibile procedere al passaggio successivo. In caso contrario, è necessario modificare manualmente i valori in modo che corrispondano ai metadati del file eseguibile.

- **Specificare manualmente**

Se questa opzione è selezionata, è necessario specificare l'hash del file, i metadati o un certificato come condizione per l'aggiunta di applicazioni alla categoria utente.

Hash del file

A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center per i file di questa categoria. Le informazioni sui valori hash calcolati dalle funzioni hash vengono memorizzate nel database di Administration Server.

SHA256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive supportano il calcolo di SHA256. Il calcolo della funzione hash MD5 è supportato da tutte le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center per i file della categoria:

- Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive, selezionare la casella di controllo **SHA256**. Non è consigliabile aggiungere categorie create in base al criterio dell'hash SHA256 di un file eseguibile per le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Questo può generare errori durante l'esecuzione dell'applicazione di protezione. In questo caso, è possibile utilizzare la funzione hash di criptaggio MD5 per i file della categoria.

- Se nella rete sono installate versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, selezionare **Hash MD5**. Non è possibile aggiungere una categoria che è stata creata in base al criterio del checksum MD5 di un file eseguibile per Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive. In questo caso, è possibile utilizzare la funzione hash di criptaggio SHA256 per i file della categoria.

- Se diversi dispositivi della rete utilizzano versioni precedenti e successive di Kaspersky Endpoint Security 10, selezionare sia la casella di controllo **SHA256** che la casella di controllo **Hash MD5**.

Metadati

Se questa opzione è selezionata, è possibile specificare i metadati del file, come il nome del file, la versione del file o il fornitore. La condizione di categoria corrisponde solo ai file eseguibili con gli stessi metadati.

Certificato

Se questa opzione è selezionata, è possibile specificare i certificati dell'archivio. La condizione di categoria corrisponde solo ai file eseguibili firmati dal certificato specificato.

I certificati vengono aggiunti all'archivio se è stata creata e avviata un'attività di inventario o se è stata selezionata la casella di controllo **Informazioni sulle applicazioni avviate** nel criterio di Kaspersky Endpoint Security. È possibile eseguire entrambe le azioni.

- **Da file o pacchetto MSI/cartella archiviata**

  Se questa opzione è selezionata, è possibile specificare il file di un programma di installazione MSI come condizione per l'aggiunta di applicazioni alla categoria utente. I metadati del programma di installazione dell'applicazione verranno inviati ad Administration Server. Le applicazioni per cui i metadati del programma di installazione corrispondono a quelli del programma di installazione MSI specificato verranno aggiunte alla categoria utente di applicazioni.

Il criterio selezionato viene aggiunto all'elenco delle condizioni.

È possibile aggiungere tutti i criteri necessari per la creazione della categoria di applicazioni.

6. Nel passaggio **Esclusioni**, fare clic sul pulsante **Aggiungi** per aggiungere un criterio di condizione esclusivo per escludere i file dalla categoria creata.

7. Nel passaggio **Criteri condizione** selezionare un tipo di regola dall'elenco, nello stesso modo in cui è stato selezionato un tipo di regola per la creazione della categoria.

Al termine della procedura guidata, viene creata la categoria di applicazioni. La regola è visualizzata nell'elenco delle categorie di applicazioni. È possibile utilizzare la categoria di applicazioni creata durante la configurazione di Controllo Applicazioni.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Guida di Kaspersky Embedded Systems Security for Windows
- Guida di Kaspersky Embedded Systems Security for Linux

Creazione di una categoria di applicazioni che include i file eseguibili nei dispositivi selezionati

È possibile utilizzare i file eseguibili nei dispositivi selezionati come modello per i file eseguibili da consentire o bloccare. In base ai file eseguibili nei dispositivi selezionati, è possibile creare una categoria e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per recuperare l'elenco dei file eseguibili dai dispositivi:

1. Assicurarsi che il criterio di Kaspersky Endpoint Security for Windows o Kaspersky Endpoint Security for Linux sia stato creato e sia attivo. Abilitare il componente Controllo Applicazioni nel criterio.

2. Recuperare un elenco dei file eseguibili archiviati nei dispositivi client.

Per creare una categoria che include i file eseguibili nei dispositivi selezionati:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Categorie di applicazioni**.

   Verrà visualizzata la pagina con un elenco di categorie.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nel passaggio **Selezionare il metodo di creazione della categoria**, specificare il nome della categoria e selezionare l'opzione **Categoria che include i file eseguibili dei dispositivi selezionati. Tali file eseguibili sono elaborati automaticamente e le relative metriche vengono aggiunte alla categoria**.

4. Fare clic su **Aggiungi**.

5. Nella finestra visualizzata, selezionare uno o più dispositivi che contengono i file eseguibili da utilizzare per creare la categoria.

6. Specificare le seguenti impostazioni:

- **Algoritmo di calcolo del valore hash**

  A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center per i file di questa categoria. Le informazioni sui valori hash calcolati dalle funzioni hash vengono memorizzate nel database di Administration Server.

  SHA256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive supportano il calcolo di SHA256. Il calcolo della funzione hash MD5 è supportato da tutte le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

  Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center per i file della categoria:

  - Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive, selezionare la casella di controllo **SHA256**. Non è consigliabile aggiungere categorie create in base al criterio dell'hash SHA256 di un file eseguibile per le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Questo può generare errori durante l'esecuzione dell'applicazione di protezione. In questo caso, è possibile utilizzare la funzione hash di criptaggio MD5 per i file della categoria.

  - Se nella rete sono installate versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, selezionare **Hash MD5**. Non è possibile aggiungere una categoria che è stata creata in base al criterio del checksum MD5 di un file eseguibile per Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive. In questo caso, è possibile utilizzare la funzione hash di criptaggio SHA256 per i file della categoria.

  Se diversi dispositivi della rete utilizzano versioni precedenti e successive di Kaspersky Endpoint Security 10, selezionare sia la casella di controllo **SHA256** che la casella di controllo **Hash MD5**.

  La casella di controllo **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)** è selezionata per impostazione predefinita.

  La casella di controllo **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** è deselezionata per impostazione predefinita.

- **Sincronizza i dati con l'archivio dell'Administration Server**

  Selezionare questa opzione se si desidera che Administration Server controlli periodicamente le modifiche nelle cartelle specificate.

  Per impostazione predefinita, questa opzione è disabilitata.

  Se si abilita questa opzione, specificare il periodo (in ore) per la verifica delle modifiche nelle cartelle specificate. Per impostazione predefinita, l'intervallo per la scansione è di 24 ore.

- **Tipo di file**

In questa sezione è possibile specificare il tipo di file utilizzato per creare la categoria di applicazioni.

Tutti i file. Durante la creazione della categoria vengono presi in considerazione tutti i file. Per impostazione predefinita, questa opzione è selezionata.

Solo i file esterni alle categorie di applicazioni. Durante la creazione della categoria vengono presi in considerazione solo i file esterni alle categorie di applicazioni.

- **Cartelle**

  In questa sezione è possibile specificare quali cartelle nei dispositivi selezionati contengono i file utilizzati per creare la categoria di applicazioni.

  Tutte le cartelle. Per la creazione della categoria vengono prese in considerazione tutte le cartelle. Per impostazione predefinita, questa opzione è selezionata.

  Cartella specificata. Per la creazione della categoria viene presa in considerazione solo la cartella specificata. Se si seleziona questa opzione, è necessario specificare il percorso della cartella.

Al termine della procedura guidata, viene creata la categoria di file eseguibili. La regola è visualizzata nell'elenco delle categorie. È possibile utilizzare la categoria creata durante la configurazione di Controllo Applicazioni.

Creazione di una categoria di applicazioni che include i file eseguibili in una cartella selezionata

È possibile utilizzare i file eseguibili in una cartella selezionata come standard per i file eseguibili da consentire o bloccare nell'organizzazione. In base ai file eseguibili nella cartella selezionata, è possibile creare una categoria di applicazioni e utilizzarla nella configurazione del componente Controllo Applicazioni.

Per creare una categoria che include i file eseguibili in una cartella selezionata:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Categorie di applicazioni**.

   Verrà visualizzata la pagina con un elenco di categorie.

2. Fare clic sul pulsante **Aggiungi**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

3. Nel passaggio **Selezionare il metodo di creazione della categoria** specificare il nome della categoria e selezionare l'opzione **Categoria che include file eseguibili di una cartella specifica. I file eseguibili delle applicazioni copiati nella cartella specificata sono elaborati automaticamente e le relative metriche vengono aggiunte alla categoria**.

4. Specificare la cartella i cui file eseguibili verranno utilizzati per creare la categoria.

5. Definire le seguenti impostazioni:

- **Includi librerie di collegamento dinamico (DLL) in questa categoria**

  La categoria di applicazioni include le librerie di collegamento dinamico (file in formato DLL) e il componente Controllo Applicazioni registra le azioni di tali librerie in esecuzione nel sistema. L'inclusione dei file DLL nella categoria può ridurre le prestazioni di Kaspersky Security Center.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Includi i dati degli script in questa categoria**

  La categoria di applicazioni include i dati sugli script e gli script non vengono bloccati da Protezione minacce Web. L'inclusione dei dati sugli script nella categoria può ridurre le prestazioni di Kaspersky Security Center.

  Per impostazione predefinita, questa casella di controllo è deselezionata.

- **Algoritmo di calcolo del valore hash**: **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive) / Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

A seconda della versione dell'applicazione di protezione installata nei dispositivi della rete, è necessario selezionare un algoritmo per il calcolo del valore hash da parte di Kaspersky Security Center per i file di questa categoria. Le informazioni sui valori hash calcolati dalle funzioni hash vengono memorizzate nel database di Administration Server.

SHA256 è una funzione hash di criptaggio: non sono state rilevate vulnerabilità nell'algoritmo, pertanto è considerata la più affidabile funzione di criptaggio attualmente disponibile. Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive supportano il calcolo di SHA256. Il calcolo della funzione hash MD5 è supportato da tutte le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selezionare una delle opzioni di calcolo del valore hash da parte di Kaspersky Security Center per i file della categoria:

- Se tutte le istanze delle applicazioni di protezione installate nella rete sono Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive, selezionare la casella di controllo **SHA256**. Non è consigliabile aggiungere categorie create in base al criterio dell'hash SHA256 di un file eseguibile per le versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Questo può generare errori durante l'esecuzione dell'applicazione di protezione. In questo caso, è possibile utilizzare la funzione hash di criptaggio MD5 per i file della categoria.

- Se nella rete sono installate versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows, selezionare **Hash MD5**. Non è possibile aggiungere una categoria che è stata creata in base al criterio del checksum MD5 di un file eseguibile per Kaspersky Endpoint Security 10 Service Pack 2 for Windows o versioni successive. In questo caso, è possibile utilizzare la funzione hash di criptaggio SHA256 per i file della categoria.

Se diversi dispositivi della rete utilizzano versioni precedenti e successive di Kaspersky Endpoint Security 10, selezionare sia la casella di controllo **SHA256** che la casella di controllo **Hash MD5**.

La casella di controllo **Calcola SHA256 per i file di questa categoria (supportato da Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versioni successive)** è selezionata per impostazione predefinita.

La casella di controllo **Calcola MD5 per i file di questa categoria (supportato dalle versioni precedenti a Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** è deselezionata per impostazione predefinita.

- **Forza scansione delle modifiche nella cartella**

Se questa opzione è abilitata, l'applicazione controlla periodicamente la presenza di modifiche nella cartella di aggiunta di contenuto nelle categorie. È possibile specificare la frequenza dei controlli (in ore) nel campo di immissione accanto alla casella di controllo. Per impostazione predefinita, l'intervallo di tempo fra i controlli forzati è di 24 ore.

Se questa opzione è disabilitata, non verranno forzati controlli della cartella. Il server tenta di accedere ai file modificati, aggiunti o eliminati.

Per impostazione predefinita, questa opzione è disabilitata.

Al termine della procedura guidata, viene creata la categoria di file eseguibili. La regola è visualizzata nell'elenco delle categorie. È possibile utilizzare la categoria nella configurazione di Controllo Applicazioni.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

- Guida di Kaspersky Embedded Systems Security for Windows
- Guida di Kaspersky Embedded Systems Security for Linux

Visualizzazione dell'elenco delle categorie di applicazioni

È possibile visualizzare l'elenco delle categorie di file eseguibili configurate e le impostazioni di ciascuna categoria.

Per visualizzare l'elenco delle categorie di applicazioni:

Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Categorie di applicazioni**.

Verrà visualizzata la pagina con un elenco di categorie.

Per visualizzare le proprietà di una categoria di applicazioni:

Fare clic sul nome della categoria.

Verrà visualizzata la finestra delle proprietà della categoria. Le proprietà sono raggruppate in diverse schede.

Aggiunta di file eseguibili relativi agli eventi alla categoria di applicazioni

Dopo aver configurato Controllo Applicazioni nei criteri di Kaspersky Endpoint Security for Windows, i seguenti eventi verranno visualizzati nell'elenco degli eventi:

- **Avvio dell'applicazione non consentito** (evento *Critico*). Questo evento viene visualizzato se è stato configurato Controllo Applicazioni per l'applicazione delle regole.
- **Avvio dell'applicazione non consentito in modalità test** (evento *Informazioni*). Questo evento viene visualizzato se è stato configurato Controllo Applicazioni per il test delle regole.
- **Messaggio all'amministratore sul divieto di avvio dell'applicazione** (evento di *avviso*). Questo evento viene visualizzato se è stato configurato Controllo Applicazioni per l'applicazione delle regole e un utente ha richiesto l'accesso a un'applicazione che è bloccata all'avvio.

È consigliabile creare selezioni eventi per visualizzare gli eventi relativi all'esecuzione di Controllo Applicazioni.

È possibile aggiungere i file eseguibili relativi agli eventi di Controllo Applicazioni a una categoria di applicazioni esistente o a una nuova categoria di applicazioni. È possibile aggiungere i file eseguibili solo a una categoria di applicazioni con contenuto aggiunto manualmente.

Per aggiungere file eseguibili relativi agli eventi di Controllo Applicazioni a una categoria di applicazioni:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.

   Verrà visualizzato l'elenco di selezioni eventi.

2. Selezionare la selezione eventi per visualizzare gli eventi relativi a Controllo Applicazioni e avviare questa selezione eventi.

   Se non è stata creata la selezione eventi correlata a Controllo Applicazioni, è possibile selezionare e avviare una selezione predefinita, ad esempio **Eventi recenti**.

   Verrà visualizzato l'elenco degli eventi.

3. Selezionare gli eventi di cui si desidera aggiungere i file eseguibili associati alla categoria di applicazioni, quindi fare clic sul pulsante **Assegna a categoria**.

   Verrà avviata la Creazione guidata nuova categoria. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Nella pagina della procedura guidata, specificare le impostazioni appropriate:

- Nella sezione **Azione sul file eseguibile relativo all'evento** selezionare una delle seguenti opzioni:
  - Aggiungi a una nuova categoria di applicazioni

    Selezionare questa opzione se si desidera creare una nuova categoria di applicazioni basata sui file eseguibili correlati agli eventi.

    Per impostazione predefinita, questa opzione è selezionata.

    Se è stata selezionata questa opzione, specificare un nuovo nome di categoria.

  - Aggiungi a una categoria di applicazioni esistente

    Selezionare questa opzione se si desidera aggiungere i file eseguibili correlati agli eventi a una categoria di applicazioni esistente.

    Per impostazione predefinita, questa opzione non è selezionata.

    Se è stata selezionata questa opzione, selezionare la categoria di applicazioni con contenuto aggiunto manualmente a cui si desidera aggiungere file eseguibili.

- Nella sezione **Tipo di regola** selezionare una delle seguenti opzioni:
  - **Regole per l'aggiunta alle inclusioni**
  - **Regole per l'aggiunta alle esclusioni**
- Nella sezione **Parametro utilizzato come condizione** selezionare una delle seguenti opzioni:
  - Dettagli del certificato (o hash SHA256 per i file senza certificato)

    I file possono essere firmati con un certificato. Più file possono essere firmati con lo stesso certificato. Ad esempio, lo stesso certificato può essere utilizzato per firmare differenti versioni della stessa applicazione o diverse applicazioni dello stesso fornitore. Quando si seleziona un certificato, possono essere inserite nella categoria diverse versioni di un'applicazione o diverse applicazioni dello stesso fornitore.

    Ogni file dispone di una specifica funzione hash SHA256 univoca. Quando si seleziona una funzione hash SHA256, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

    Selezionare questa opzione se si desidera aggiungere alle regole della categoria i dettagli del certificato di un file eseguibile (o la funzione hash SHA256 per i file senza certificato).

    Per impostazione predefinita, questa opzione è selezionata.

  - Dettagli del certificato (i file senza certificato verranno ignorati)

I file possono essere firmati con un certificato. Più file possono essere firmati con lo stesso certificato. Ad esempio, lo stesso certificato può essere utilizzato per firmare differenti versioni della stessa applicazione o diverse applicazioni dello stesso fornitore. Quando si seleziona un certificato, possono essere inserite nella categoria diverse versioni di un'applicazione o diverse applicazioni dello stesso fornitore.

Selezionare questa opzione se si desidera aggiungere i dettagli del certificato di un file eseguibile alle regole della categoria. Se il file eseguibile non dispone di alcun certificato, verrà ignorato. Nessuna informazione sul file verrà aggiunta alla categoria.

- **Solo SHA256 (i file senza hash verranno ignorati)**

  Ogni file dispone di una specifica funzione hash SHA256 univoca. Quando si seleziona una funzione hash SHA256, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

  Selezionare questa opzione se si desidera aggiungere solo i dettagli della funzione hash SHA256 del file eseguibile.

- **Solo MD5 (modalità non più disponibile, solo per Kaspersky Endpoint Security 10 versione Service Pack 1)**

  Ogni file dispone di una specifica funzione hash MD5 univoca. Quando si seleziona una funzione hash MD5, viene inserito nella categoria un solo file corrispondente (ad esempio, la versione dell'applicazione definita).

  Selezionare questa opzione se si desidera aggiungere solo i dettagli della funzione hash MD5 del file eseguibile. Il calcolo della funzione hash MD5 è supportato da Kaspersky Endpoint Security 10 Service Pack 1 for Windows e da tutte le versioni precedenti.

5. Fare clic su **OK**.

   Al termine della procedura guidata, i file eseguibili relativi agli eventi di Controllo Applicazioni vengono aggiunti alla categoria di applicazioni esistente o a una nuova categoria di applicazioni. È possibile visualizzare le impostazioni della categoria di applicazioni che è stata modificata o creata.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Guida di Kaspersky Embedded Systems Security for Windows
- Guida di Kaspersky Embedded Systems Security for Linux

Configurazione di Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

Dopo aver creato le categorie di Controllo Applicazioni, è possibile utilizzarle per configurare Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows.

Per configurare Controllo Applicazioni nel criterio di Kaspersky Endpoint Security for Windows

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

   Verrà visualizzata una pagina con un elenco di criteri.

2. Fare clic sul criterio **Kaspersky Endpoint Security for Windows**.

   Verrà visualizzata la finestra delle impostazioni del criterio.

3. Passare a **Impostazioni applicazione** → **Security Controls** → **Application Control**.

   Verrà visualizzata la finestra **Controllo Applicazioni** con le impostazioni di Controllo Applicazioni.

4. L'opzione **Controllo Applicazioni** è abilitata per impostazione predefinita. Assicurarsi che l'interruttore **Controllo Applicazioni DISABILITATO** viene spostato nella posizione di disabilitazione.

5. Nelle impostazioni del blocco **Impostazioni di Controllo Applicazioni**, abilitare la modalità operativa per applicare le regole di Controllo applicazioni e consentire a Kaspersky Endpoint Security for Windows di bloccare l'avvio delle applicazioni.

   Se si desidera testare le regole di Controllo Applicazioni, nella sezione **Impostazioni di Controllo Applicazioni**, abilitare la modalità di test. In modalità di test, Kaspersky Endpoint Security for Windows non blocca l'avvio delle applicazioni, ma registra le informazioni sulle regole attivate nel rapporto. Fare clic sul collegamento **Visualizza rapporto** per visualizzare queste informazioni.

6. Abilitare l'opzione **Controlla il caricamento dei moduli DLL** se si desidera che Kaspersky Endpoint Security for Windows monitori il caricamento dei moduli DLL all'avvio delle applicazioni da parte degli utenti.

   Le informazioni sul modulo e sull'applicazione che ha caricato il modulo verranno salvate in un rapporto.

   Kaspersky Endpoint Security for Windows monitora solo i moduli DLL e i driver caricati dopo che è stata selezionata l'opzione **Controlla il caricamento dei moduli DLL**. Riavviare il dispositivo dopo aver selezionato l'opzione **Controlla il caricamento dei moduli DLL** se si desidera che Kaspersky Endpoint Security for Windows monitori tutti i moduli DLL e i driver, inclusi quelli caricati prima dell'avvio di Kaspersky Endpoint Security for Windows.

7. (Facoltativo) Nella sezione **Modelli di messaggi** modificare il modello del messaggio visualizzato quando l'avvio di un'applicazione è bloccato e il modello del messaggio e-mail inviato.

8. Nelle impostazioni del gruppo **Modalità Controllo Applicazioni**, selezionare la modalità **Lista vietati** o **Lista consentiti**.

   Per impostazione predefinita, è selezionata la modalità **Lista vietati**.

9. Fare clic sul collegamento **Impostazioni elenchi di regole**.

   Verrà visualizzata la finestra **Liste vietati e Liste consentiti** per consentire di aggiungere una categoria di applicazioni. Per impostazione predefinita, è selezionata la scheda **Lista vietati** se è selezionata la modalità **Lista vietati** e la scheda **Lista consentiti** se è selezionata la modalità **Lista consentiti**.

10. Nella finestra **Liste vietati e liste consentiti** fare clic sul pulsante **Aggiungi**.

    Verrà visualizzata la finestra **Regola di Controllo Applicazioni**.

11. Fare clic sul collegamento **Scegliere una categoria**.

    Verrà visualizzata la finestra **Categoria di applicazioni**.

12. Aggiungere una o più categorie di applicazioni create in precedenza.

    È possibile modificare le impostazioni di una categoria creata facendo clic sul pulsante **Modifica**.

    È possibile creare una nuova categoria facendo clic sul pulsante **Aggiungi**.

    È possibile eliminare una categoria dall'elenco facendo clic sul pulsante **Elimina**.

13. Al termine della creazione dell'elenco delle categorie di applicazioni, fare clic sul pulsante **OK**.

    La finestra **Categoria di applicazioni** verrà chiusa.

14. Nella finestra **Regola di Controllo Applicazioni**, nella sezione **Soggetti e relativi diritti**, creare un elenco di utenti e gruppi di utenti a cui applicare la regola di Controllo Applicazioni.

15. Fare clic sul pulsante **OK** per salvare le impostazioni e chiudere la finestra **Regola di Controllo Applicazioni**.

16. Fare clic sul pulsante **OK** per salvare le impostazioni e chiudere la finestra **Liste vietati e liste consentiti**.

17. Fare clic sul pulsante **OK** per salvare le impostazioni e chiudere la finestra **Controllo Applicazioni**.

18. Chiudere la finestra con le impostazioni dei criteri di Kaspersky Endpoint Security for Windows.

    Controllo Applicazioni è configurato. Una volta propagato il criterio ai dispositivi client, viene gestito l'avvio dei file eseguibili.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Guida di Kaspersky Embedded Systems Security for Windows
- Guida di Kaspersky Embedded Systems Security for Linux

Recupero e visualizzazione di un elenco delle applicazioni installate nei dispositivi client

Kaspersky Security Center esegue l'inventario di tutto il software installato nei dispositivi client gestiti che eseguono Linux e Windows.

Network Agent compila un elenco delle applicazioni installate in un dispositivo, quindi trasmette questo elenco ad Administration Server. Sono necessari circa 10-15 minuti affinché Network Agent aggiorni l'elenco delle applicazioni.

Per i dispositivi client basati su Windows, Network Agent riceve la maggior parte delle informazioni sulle applicazioni installate dal Registro di sistema di Windows. Per i dispositivi client basati su Linux, gli strumenti di gestione di pacchetti forniscono informazioni sulle applicazioni installate a Network Agent.

Se un'applicazione nella sezione **Registro delle applicazioni** è stata rilevata in un dispositivo Linux, le proprietà dell'applicazione non contengono informazioni sui file eseguibili correlati.

Per visualizzare l'elenco delle applicazioni installate nei dispositivi gestiti:

1. Nel menu principale accedere a **Operazioni → Applicazioni di terze parti → Registro delle applicazioni**.

   Nella pagina viene visualizzata una tabella con le applicazioni installate nei dispositivi gestiti. Selezionare l'applicazione per visualizzarne le proprietà, ad esempio il nome del fornitore, il numero di versione, l'elenco dei file eseguibili, l'elenco dei dispositivi in cui è installata l'applicazione, l'elenco degli aggiornamenti software disponibili e l'elenco delle vulnerabilità del software rilevate.

2. È possibile raggruppare e filtrare i dati della tabella con le applicazioni installate come segue:

   - Fare clic sull'icona delle impostazioni ( ) nell'angolo superiore destro della tabella.

     Nel menu **Impostazioni colonne** richiamato, selezionare le colonne da visualizzare nella tabella. Per visualizzare il tipo di sistema operativo dei dispositivi client in cui è installata l'applicazione, selezionare la colonna **Tipo di sistema operativo**.

   - Fare clic sull'icona del filtro ( ) nell'angolo superiore destro della tabella, quindi specificare e applicare il criterio di filtro nel menu richiamato.

     Viene visualizzata la tabella filtrata delle applicazioni installate.

Per visualizzare l'elenco delle applicazioni installate in un dispositivo gestito specifico:

Nel menu principale accedere a **Dispositivi → Dispositivi gestiti → <nome dispositivo> → Avanzate → Registro delle applicazioni**. In questo menu, è possibile esportare l'elenco delle applicazioni in un file CSV o TXT.

Per informazioni dettagliate su Controllo Applicazioni, fare riferimento ai seguenti argomenti della Guida:

- Guida in linea di Kaspersky Endpoint Security for Windows
- Guida in linea di Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Guida di Kaspersky Embedded Systems Security for Windows
- Guida di Kaspersky Embedded Systems Security for Linux

Creazione di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky

Kaspersky Security Center Web Console consente di eseguire l'installazione remota delle applicazioni di terze parti utilizzando i pacchetti di installazione. Tali applicazioni di terze parti sono incluse in un database Kaspersky dedicato. Questo database viene creato automaticamente quando si esegue l'attività *Scarica aggiornamenti nell'archivio dell'Administration Server* per la prima volta.

Per creare un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky:

1. Nel menu principale accedere a **Individuazione e distribuzione → Distribuzione e assegnazione → Pacchetti di installazione**.

2. Fare clic sul pulsante **Aggiungi**.

3. Nella pagina Creazione guidata nuovo pacchetto visualizzata selezionare l'opzione **Selezionare un'applicazione dal database di Kaspersky per creare un pacchetto di installazione**, quindi fare clic su **Avanti**.

4. Nell'elenco delle applicazioni visualizzato selezionare l'applicazione attinente, quindi fare clic su **Avanti**.

5. Selezionare la lingua di localizzazione attinente nell'elenco a discesa, quindi fare clic su **Avanti**.

   Questo passaggio viene visualizzato solo se l'applicazione offre più opzioni di lingua.

6. Se viene richiesto di accettare un Contratto di licenza per l'installazione, nella pagina **Contratto di licenza con l'utente finale** visualizzata fare clic sul collegamento per leggere il Contratto di licenza nel sito Web del produttore, quindi selezionare la casella di controllo **Confermo di aver letto, compreso e accettato i termini e le condizioni del presente Contratto di licenza con l'utente finale**.

7. Nella pagina **Nome del nuovo pacchetto di installazione** visualizzata, nel campo **Nome pacchetto**, immettere il nome del pacchetto di installazione, quindi fare clic su **Avanti**.

Attendere il caricamento del nuovo pacchetto di installazione creato in Administration Server. Quando la Creazione guidata nuovo pacchetto visualizza il messaggio per informare che il processo di creazione del pacchetto è andato a buon fine, fare clic su **Fine**.

Il nuovo pacchetto di installazione creato viene visualizzato nell'elenco dei pacchetti di installazione. È possibile selezionare questo pacchetto durante la creazione o la riconfigurazione dell'attività *Installa l'applicazione in remoto*.

Visualizzazione e modifica delle impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky

Se in precedenza sono stati creati pacchetti di installazione di applicazioni di terze parti elencate nel database Kaspersky, successivamente è possibile visualizzare e modificare le impostazioni di questi pacchetti.

La modifica delle impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky è disponibile solo con la licenza Vulnerability e patch management.

Per visualizzare e modificare le impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Pacchetti di installazione**.

2. Nell'elenco dei pacchetti di installazione visualizzato fare clic sul nome del pacchetto attinente.

3. Nella pagina delle proprietà visualizzata modificare le impostazioni, se necessario.

4. Fare clic sul pulsante **Salva**.

Le impostazioni modificate vengono salvate.

Impostazioni di un pacchetto di installazione di un'applicazione di terze parti dal database Kaspersky

Le impostazioni di un pacchetto di installazione di un'applicazione di terze parti sono raggruppate nelle seguenti schede:

Per impostazione predefinita viene visualizzata solo una parte delle impostazioni elencate di seguito, quindi è possibile aggiungere le colonne corrispondenti facendo clic sul pulsante **Filtro** e selezionando i nomi delle colonne attinenti dall'elenco.

- Scheda **Generale**:
  - Campo di immissione che contiene il nome del pacchetto di installazione che può essere modificato manualmente
  - Applicazione

    Il nome dell'applicazione di terze parti per cui viene creato il pacchetto di installazione.
  - Versione

    Il numero di versione dell'applicazione di terze parti per cui è stato creato il pacchetto di installazione.
  - Dimensione

    Le dimensioni del pacchetto di installazione di terze parti (in kilobyte).
  - Data creazione

    La data e l'ora in cui è stato creato il pacchetto di installazione di terze parti.
  - Percorso

    Percorso della cartella di rete in cui è archiviato il pacchetto di installazione di terze parti.
- Scheda **Procedura di installazione**:
  - Installa i componenti generali del sistema richiesti

    Se questa opzione è abilitata, prima di installare un aggiornamento l'applicazione installa automaticamente tutti i componenti di sistema generali (prerequisiti) richiesti per installare l'aggiornamento. Questi prerequisiti possono ad esempio essere aggiornamenti del sistema operativo.

    Se questa opzione è disabilitata, può essere necessario installare manualmente i prerequisiti.

    Per impostazione predefinita, questa opzione è disabilitata.
  - Tabella che mostra le proprietà dell'aggiornamento e che contiene le seguenti colonne:

- **Nome**

  Nome dell'aggiornamento.

- **Descrizione**

  Descrizione dell'aggiornamento.

- **Origine**

  Origine dell'aggiornamento, ovvero se è stato rilasciato da Microsoft o da un altro sviluppatore di terze parti.

- **Tipo**

  Tipo di aggiornamento, ovvero se è destinato a un driver o a un'applicazione.

- **Categoria**

  Categoria WSUS (Windows Server Update Services) visualizzata per gli aggiornamenti Microsoft (Aggiornamenti critici, Aggiornamenti definizione, Driver, Feature Pack, Aggiornamenti della protezione, Service Pack, Strumenti, Aggiornamenti cumulativi, Aggiornamenti o Upgrade).

- **Livello di importanza in base a MSRC**

  Livello di importanza dell'aggiornamento definito da Microsoft Security Response Center (MSRC).

- **Livello di importanza**

  Livello di importanza dell'aggiornamento definito da Kaspersky.

- **Livello di importanza patch**

  Livello di importanza della patch, se è destinata a un'applicazione Kaspersky.

- **Articolo**

  Identificatore (ID) dell'articolo nella Knowledge Base che descrive l'aggiornamento.

- **Bollettino**

  ID del bollettino sulla sicurezza che descrive l'aggiornamento.

- **Non assegnato per installazione (nuova versione)**

  Indica se l'aggiornamento ha lo stato Non assegnato per l'installazione.

- **Da installare**

Indica se l'aggiornamento ha lo stato Da installare.

- **Installazione in corso**

  Indica se l'aggiornamento ha lo stato Installazione in corso.

- **Installato**

  Indica se l'aggiornamento ha lo stato Installato.

- **Non riuscito**

  Indica se l'aggiornamento ha lo stato Non riuscito.

- **È necessario il riavvio**

  Indica se l'aggiornamento ha lo stato È necessario il riavvio.

- **Registrato**

  Indica la data e l'ora in cui è stato registrato l'aggiornamento.

- **Installato in modalità interattiva**

  Indica se l'aggiornamento richiede l'interazione con l'utente durante l'installazione.

- **Revocato**

  Indica la data e l'ora in cui l'aggiornamento è stato revocato.

- **Stato di approvazione dell'aggiornamento**

  Indica se l'aggiornamento è approvato per l'installazione.

- **Revisione**

  Indica il numero di revisione corrente dell'aggiornamento.

- **ID aggiornamento**

  Indica l'ID dell'aggiornamento.

- **Versione applicazione**

  Indica il numero di versione a cui deve essere aggiornata l'applicazione.

- **Sostituiti**

Indica altri aggiornamenti che possono sostituire l'aggiornamento.

- **Sostituzione**

  Indica altri aggiornamenti che possono essere sostituiti dall'aggiornamento.

- **È necessario accettare i termini del Contratto di licenza**

  Indica se l'aggiornamento richiede l'accettazione dei termini di un Contratto di licenza con l'utente finale (EULA).

- **URL descrizione**

  Indica il nome del fornitore dell'aggiornamento.

- **Famiglia di applicazioni**

  Indica il nome della famiglia di applicazioni a cui appartiene l'aggiornamento.

- **Applicazione**

  Indica il nome dell'applicazione a cui appartiene l'aggiornamento.

- **Lingua localizzazione**

  Indica la lingua della localizzazione dell'aggiornamento.

- **Non assegnato per installazione (nuova versione)**

  Indica se l'aggiornamento ha lo stato Non assegnato per l'installazione (nuova versione).

- **Richiede l'installazione dei prerequisiti**

  Indica se l'aggiornamento ha lo stato Richiede l'installazione dei prerequisiti.

- **Modalità di download**

  Indica la modalità di download dell'aggiornamento.

- **È una patch**

  Indica se l'aggiornamento è una patch.

- **Non installato**

  Indica se l'aggiornamento ha lo stato Non installato.

- Scheda **Impostazioni** che mostra le impostazioni del pacchetto di installazione, con i relativi nomi, descrizioni e valori, utilizzate come parametri della riga di comando durante l'installazione. Se il pacchetto non fornisce tali impostazioni, viene visualizzato il messaggio corrispondente. È possibile modificare i valori di queste impostazioni.

- Scheda **Cronologia revisioni** che mostra le revisioni del pacchetto di installazione e contiene le seguenti colonne:

  - **Revisione**—Il numero di revisione dei pacchetti di installazione.

  - **Data/ora**—Data e ora in cui sono state modificate le impostazioni del pacchetto di installazione.

  - **Utente**—Nome dell'utente che ha modificato le impostazioni del pacchetto di installazione.

  - **Azione**—Azione eseguita sul pacchetto di installazione all'interno della revisione.

  - **Descrizione**—Descrizione della revisione relativa alla modifica apportata alle impostazioni del pacchetto di installazione.

    Per impostazione predefinita, la descrizione della revisione è vuota. Per aggiungere una descrizione a una revisione, selezionare la revisione desiderata, quindi fare clic sul pulsante **Modifica descrizione**. Nella finestra aperta, immettere il testo relativo alla descrizione della revisione.

Tag applicazione

Kaspersky Security Center consente di assegnare tag alle applicazioni dal registro delle applicazioni. Un tag è l'etichetta di un'applicazione che può essere utilizzata per raggruppare o cercare le applicazioni. Un tag assegnato alle applicazioni può essere utilizzato come condizione nelle selezioni dispositivi.

È ad esempio possibile creare il tag `[Browser]` e assegnarlo a tutti i browser, quali Microsoft Internet Explorer, Google Chrome, Mozilla Firefox.

Creazione di un tag applicazione

Per creare un tag applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Tag applicazione**.

2. Fare clic su **Aggiungi**.

   Verrà visualizzata una finestra per il nuovo tag.

3. Immettere il nome del tag.

4. Fare clic su **OK** per salvare le modifiche.

Il nuovo tag verrà visualizzato nell'elenco dei tag applicazione.

Ridenominazione di un tag applicazione

Per rinominare un tag applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Tag applicazione**.
2. Selezionare la casella di controllo accanto al tag che si desidera rinominare, quindi fare clic su **Modifica**.

   Verrà visualizzata una finestra delle proprietà del tag.
3. Modificare il nome del tag.
4. Fare clic su **OK** per salvare le modifiche.

Il tag aggiornato verrà visualizzato nell'elenco dei tag applicazione.

Assegnazione di tag a un'applicazione

Per assegnare uno o più tag a un'applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Registro delle applicazioni**.
2. Fare clic sul nome dell'applicazione a cui si desidera assegnare i tag.
3. Fare clic sulla scheda **Tag**.

   La scheda mostra tutti i tag delle applicazioni presenti in Administration Server. Per i tag assegnati all'applicazione selezionata, la casella di controllo nella colonna **Tag assegnato** è selezionata.
4. Per i tag che si desidera assegnare, selezionare le caselle di controllo nella colonna **Tag assegnato**.
5. Fare clic su **Salva** per salvare le modifiche.

I tag verranno assegnati all'applicazione.

Rimozione dei tag assegnati a un'applicazione

Per rimuovere uno o più tag da un'applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Registro delle applicazioni**.
2. Fare clic sul nome dell'applicazione da cui si desidera rimuovere i tag.
3. Fare clic sulla scheda **Tag**.

   La scheda mostra tutti i tag delle applicazioni presenti in Administration Server. Per i tag assegnati all'applicazione selezionata, la casella di controllo nella colonna **Tag assegnato** è selezionata.

4. Per i tag che si desidera rimuovere, deselezionare le caselle di controllo nella colonna **Tag assegnato**.
5. Fare clic su **Salva** per salvare le modifiche.

I tag verranno rimossi dall'applicazione.

I tag dell'applicazione rimossi non vengono eliminati. Se si desidera, è possibile eliminarli manualmente.

Eliminazione di un tag applicazione

Per eliminare un tag applicazione:

1. Nel menu principale accedere a **Operazioni** → **Applicazioni di terze parti** → **Tag applicazione**.
2. Selezionare dall'elenco il tag applicazione da eliminare.
3. Fare clic sul pulsante **Elimina**.
4. Nella finestra visualizzata fare clic su **OK**.

Il tag applicazione verrà eliminato. Il tag eliminato viene rimosso automaticamente da tutte le applicazioni a cui è stato assegnato.

Monitoraggio e generazione dei rapporti

Questa sezione illustra le funzionalità di monitoraggio e reportistica di Kaspersky Security Center. Queste funzionalità offrono una panoramica dell'infrastruttura, degli stati di protezione e delle statistiche.

Dopo la distribuzione di Kaspersky Security Center o durante l'esecuzione, è possibile configurare le funzionalità di monitoraggio e generazione dei rapporti in base alle esigenze.

Scenario: monitoraggio e generazione dei rapporti

Questa sezione fornisce uno scenario per la configurazione della funzionalità di monitoraggio e generazione dei rapporti in Kaspersky Security Center.

Prerequisiti

Dopo aver distribuito Kaspersky Security Center nella rete di un'organizzazione, è possibile iniziare a monitorarlo e generare rapporti sul relativo funzionamento.

Il monitoraggio e la generazione dei rapporti nella rete di un'organizzazione prevede diversi passaggi:

1. **Configurazione del passaggio degli stati del dispositivo**

Acquisire familiarità con le impostazioni per gli stati del dispositivo in base a condizioni specifiche. Modificando queste impostazioni, è possibile modificare il numero di eventi con livelli di importanza *Critico* o *Avviso*. Durante la configurazione del passaggio degli stati del dispositivo, verificare quanto segue:

- Le nuove impostazioni non sono in conflitto con i criteri di sicurezza delle informazioni dell'organizzazione.
- Si è in grado di reagire tempestivamente agli eventi di sicurezza importanti nella rete dell'organizzazione.

2. **Configurazione delle notifiche degli eventi nei dispositivi client**

   Istruzioni dettagliate:

   Configurare la notifica (tramite e-mail, SMS o avviando un file eseguibile) degli eventi nei dispositivi client

3. **Modifica della risposta della rete di sicurezza all'evento Epidemia di virus**

   È possibile modificare le specifiche soglie nelle proprietà di Administration Server. È inoltre possibile creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.

4. **Esecuzione delle azioni consigliate per le notifiche critiche e di avviso**

   Istruzioni dettagliate:

   Eseguire le azioni consigliate per la rete dell'organizzazione

5. **Analisi dello stato di sicurezza della rete dell'organizzazione**

   Istruzioni dettagliate:

   - Esaminare il widget Stato protezione
   - Generare ed esaminare il Rapporto sullo stato della protezione
   - Generare ed esaminare il Rapporto sugli errori

6. **Individuazione dei dispositivi client che non sono protetti**

   Istruzioni dettagliate:

   - Esaminare il widget Nuovi dispositivi
   - Generare ed esaminare il Rapporto sulla distribuzione della protezione

7. **Verifica della protezione dei dispositivi client**

   Istruzioni dettagliate:

   - Generare ed esaminare i rapporti delle categorie Stato protezione e Statistiche delle minacce
   - Avviare ed esaminare la selezione eventi Critico

8. **Valutazione e limitazione del carico di eventi nel database**

   Le informazioni sugli eventi che si verificano durante il funzionamento delle applicazioni gestite vengono trasferite da un dispositivo client e registrate nel database di Administration Server. Per ridurre il carico su Administration Server, valutare e limitare il numero massimo di eventi che possono essere archiviati nel database.

   Istruzioni dettagliate:

   - Calcolo dello spazio del database
   - Limitazione del numero massimo di eventi

9. **Analisi delle informazioni sulla licenza**

   Istruzioni dettagliate:

   - Aggiungere il widget Utilizzo chiavi di licenza al dashboard ed esaminarlo
   - Generare ed esaminare il Rapporto sull'utilizzo delle chiavi di licenza

Risultati

Al termine dello scenario, si dispone di informazioni sulla protezione della rete dell'organizzazione e quindi è possibile pianificare le azioni per il miglioramento della protezione.

Informazioni sui tipi di monitoraggio e generazione dei rapporti

Le informazioni sugli eventi di sicurezza nella rete di un'organizzazione sono archiviate nel database di Administration Server. In base agli eventi, Kaspersky Security Center Web Console fornisce i seguenti tipi di monitoraggio e generazione dei rapporti nella rete dell'organizzazione:

- Dashboard
- Rapporti
- Selezioni eventi
- Notifiche

Dashboard

Il dashboard consente di monitorare le tendenze relative alla sicurezza nella rete dell'organizzazione fornendo una visualizzazione grafica delle informazioni.

Rapporti

La funzionalità Rapporti consente di ottenere informazioni numeriche dettagliate sulla sicurezza della rete dell'organizzazione, nonché di salvare le informazioni in un file, inviarlo tramite e-mail e stamparlo.

Selezioni eventi

Le selezioni eventi consentono di visualizzare i set denominati degli eventi selezionati dal database di Administration Server. Questi set di eventi sono raggruppati in base alle seguenti categorie:

- In base al livello di importanza: **Eventi critici**, **Errori funzionali**, **Avvisi** e **Eventi informativi**
- In base al tempo: **Eventi recenti**
- In base al tipo: **Richieste utente** e **Eventi di controllo**

È possibile creare e visualizzare le selezioni eventi definite dall'utente in base alle impostazioni disponibili per la configurazione nell'interfaccia di Kaspersky Security Center Web Console.

Notifiche

Le notifiche segnalano gli eventi e consentono di velocizzare le risposte a tali eventi eseguendo le azioni consigliate o le azioni che si ritengono appropriate.

Dashboard e widget

Questa sezione contiene informazioni sul dashboard e sui widget forniti dal dashboard. La sezione include istruzioni su come gestire i widget e configurare le impostazioni dei widget.

Utilizzo del dashboard

Il dashboard consente di monitorare le tendenze relative alla sicurezza nella rete dell'organizzazione fornendo una visualizzazione grafica delle informazioni.

Il dashboard è disponibile in Kaspersky Security Center Web Console, nella sezione **Monitoraggio e generazione dei rapporti**, facendo clic su **Dashboard**.

Il dashboard fornisce widget che possono essere personalizzati. È possibile scegliere tra numerosi widget diversi, presentati come grafici a torta o grafici ad anello, tabelle, grafici, grafici a barre ed elenchi. Le informazioni visualizzate nei widget vengono aggiornate automaticamente, il periodo di aggiornamento è di uno o due minuti. L'intervallo tra gli aggiornamenti varia per i diversi widget. È possibile aggiornare manualmente i dati in un widget in qualsiasi momento tramite il menu delle impostazioni.

Per impostazione predefinita, i widget includono informazioni su tutti gli eventi archiviati nel database di Administration Server.

Kaspersky Security Center Web Console dispone di un set predefinito di widget per le seguenti categorie:

- **Stato protezione**
- **Distribuzione**
- **Aggiornamento**
- **Statistiche delle minacce**
- **Altro**

Alcuni widget contengono informazioni di testo con collegamenti. È possibile visualizzare informazioni dettagliate facendo clic su un collegamento.

Quando si configura il dashboard, è possibile aggiungere i widget desiderati, nascondere i widget non necessari, modificare le dimensioni o l'aspetto dei widget, spostare i widget e modificarne le impostazioni.

Aggiunta di widget al dashboard

Per aggiungere widget al dashboard:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sul pulsante **Aggiungi o ripristina widget Web**.
3. Nell'elenco dei widget disponibili selezionare i widget che si desidera aggiungere al dashboard.

   I widget sono raggruppati per categoria. Per visualizzare l'elenco dei widget inclusi in una categoria, fare clic sull'icona della freccia di espansione (>) accanto al nome della categoria.
4. Fare clic sul pulsante **Aggiungi**.

I widget selezionati verranno aggiunti alla fine del dashboard.

Ora è possibile modificare la rappresentazione e i parametri dei widget aggiunti.

Occultamento di un widget dal dashboard

Per nascondere un widget visualizzato dal dashboard:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera nascondere.
3. Selezionare **Nascondi widget Web**.
4. Nella finestra **Avviso** visualizzata fare clic su **OK**.

Il widget selezionato verrà nascosto. In seguito, è possibile aggiungere nuovamente il widget al dashboard.

Spostamento di un widget nel dashboard

Per spostare un widget nel dashboard:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera spostare.
3. Selezionare **Sposta**.
4. Fare clic sul punto in cui si desidera spostare il widget. È possibile selezionare solo un altro widget.

Le posizioni dei widget selezionati vengono scambiate.

Modifica delle dimensioni o dell'aspetto del widget

Per i widget che visualizzano un grafico, è possibile modificarne la rappresentazione: un grafico a barre o un grafico a linee. Per alcuni widget è possibile modificare le dimensioni: Compatto, Medio o Massimo.

Per modificare la rappresentazione del widget:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera modificare.
3. Eseguire una delle seguenti operazioni:
   - Per visualizzare il widget come grafico a barre, selezionare **Tipo di grafico: barre**.
   - Per visualizzare il widget come grafico a linee, selezionare **Tipo di grafico: linee**.
   - Per modificare l'area occupata dal widget, selezionare uno dei valori:
     - **Compatto**
     - **Compatto (solo barra)**
     - **Medio (grafico ad anello)**
     - **Medio (grafico a barre)**
     - **Massimo**

La rappresentazione del widget selezionato verrà modificata.

Modifica delle impostazioni del widget

Per modificare le impostazioni di un widget:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera modificare.
3. Selezionare **Mostra impostazioni**.
4. Nella finestra delle impostazioni del widget visualizzata modificare le impostazioni del widget come richiesto.
5. Fare clic su **Salva** per salvare le modifiche.

Le impostazioni del widget selezionato verranno modificate.

Il set di impostazioni dipende dallo specifico widget. Di seguito sono riportate alcune delle impostazioni comuni:

- **Ambito del widget Web** (il set di oggetti per cui il widget visualizza informazioni), ad esempio un gruppo di amministrazione o una selezione dispositivi.
- **Seleziona attività** (l'attività per cui il widget visualizza informazioni).
- **Intervallo** (l'intervallo di tempo per cui le informazioni vengono visualizzate nel widget): tra le due date specificate, dalla data specificata al giorno corrente o dal giorno corrente meno il numero di giorni specificato al giorno corrente.
- **Imposta su Critico se è specificato** e **Imposta su Avviso se è specificato** (le regole che determinano il colore di un indicatore a semaforo).

Dopo aver modificato le impostazioni del widget, è possibile aggiornare manualmente i dati nel widget.

Per aggiornare i dati su un widget:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
2. Fare clic sull'icona delle impostazioni (⚙) accanto al widget che si desidera spostare.
3. Selezionare **Aggiorna**.

I dati nel widget vengono aggiornati.

Informazioni sulla modalità Solo dashboard

È possibile configurare la modalità Solo dashboard per i dipendenti che non gestiscono la rete ma che desiderano visualizzare le statistiche di protezione della rete in Kaspersky Security Center (ad esempio un Top Manager). Con questa modalità abilitata, l'utente visualizza solo un dashboard con un set predefinito di widget. L'utente può quindi monitorare le statistiche specificate nei widget, ad esempio lo stato della protezione di tutti i dispositivi gestiti, il numero di minacce rilevate di recente o l'elenco delle minacce più frequenti nella rete.

Quando un utente usa la modalità Solo dashboard, vengono applicate le seguenti restrizioni:

- Il menu principale non viene mostrato all'utente, che non potrà quindi modificare le impostazioni di protezione della rete.
- L'utente non può eseguire alcuna azione con i widget, ad esempio aggiungerli o nasconderli. È pertanto necessario inserire tutti i widget necessari per l'utente nel dashboard e configurarli, ad esempio impostando la regola di conteggio degli oggetti o specificando l'intervallo di tempo.

Non è possibile assegnare a se stessi la modalità Solo dashboard. Se si desidera utilizzare questa modalità, contattare un amministratore di sistema, un MSP (Managed Service Provider) o un utente con il diritto **Modifica elenchi di controllo degli accessi agli oggetti** nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

Configurazione della modalità Solo dashboard

Prima di iniziare a configurare la modalità Solo dashboard, assicurarsi che vengano soddisfatti i seguenti prerequisiti:

- L'utente dispone del diritto **Modifica elenchi di controllo degli accessi agli oggetti** nell'area funzionale **Caratteristiche generali: Autorizzazioni utente**. Se non si dispone di questo diritto, la scheda per la configurazione della modalità non sarà presente.
- L'utente ha il diritto **Lettura** nell'area funzionale **Caratteristiche generali: Funzionalità di base**.

Se nella rete è organizzata una gerarchia di Administration Server, per configurare la modalità Solo dashboard passare al Server in cui è disponibile l'account utente nella sezione **Utenti** tab of the **Utenti e ruoli** → **Utenti e gruppi**. Può trattarsi di un server primario o di un server secondario fisico. Non è possibile regolare la modalità in un server virtuale.

Per configurare la modalità Solo dashboard:

1. Nel menu principale, passare a **Utenti e ruoli** → **Utenti e gruppi**, quindi selezionare la scheda **Utenti**.
2. Fare clic sul nome dell'account utente per il quale si desidera modificare il dashboard con i widget.
3. Nella finestra delle impostazioni dell'account visualizzata selezionare la scheda **Dashboard**.

   Nella scheda aperta viene visualizzato lo stesso dashboard dell'utente.
4. Se l'opzione **Visualizza la console in modalità Solo dashboard** è abilitata, spostare l'interruttore per disabilitarla.

   Quando questa opzione è abilitata, non è nemmeno possibile modificare il dashboard. Dopo aver disabilitato l'opzione, è possibile gestire i widget.
5. Configurare l'aspetto del dashboard. Il set di widget preparato nella scheda **Dashboard** è disponibile per l'utente con l'account personalizzabile. L'utente non può modificare in alcun modo le impostazioni o le dimensioni dei widget, né aggiungere o rimuovere widget dal dashboard. È pertanto opportuno modificarli per l'utente, in modo che possa visualizzare le statistiche sulla protezione della rete. A tale scopo, nella scheda **Dashboard** è possibile eseguire con i widget le stesse azioni della sezione **Monitoraggio e generazione dei rapporti** → **Dashboard**:
   - Aggiungere nuovi widget al dashboard.
   - Nascondere i widget di cui l'utente non ha bisogno.
   - Spostare i widget in un ordine specifico.
   - Modificare le dimensioni o l'aspetto dei widget.
   - Modificare le impostazioni dei widget.

6. Spostare l'interruttore per abilitare l'opzione **Visualizza la console in modalità Solo dashboard**.

   Successivamente, sarà disponibile solo il dashboard per l'utente. Quest'ultimo può monitorare le statistiche ma non può modificare le impostazioni di protezione della rete e l'aspetto del dashboard. Poiché viene visualizzato lo stesso dashboard che appare all'utente, non è possibile modificarlo.

   Se si mantiene l'opzione disabilitata, viene visualizzato il menu principale per l'utente, in modo che possa eseguire varie azioni in Kaspersky Security Center, inclusa la modifica delle impostazioni di protezione e dei widget.

7. Fare clic sul pulsante **Salva** al termine della configurazione della modalità Solo dashboard. Solo successivamente l'utente visualizzerà il dashboard preconfigurato.

8. Se l'utente desidera visualizzare le statistiche delle applicazioni Kaspersky supportate e ha bisogno dei diritti di accesso per farlo, configurare i diritti per l'utente. Successivamente, l'utente può visualizzare i dati delle applicazioni Kaspersky nei widget di queste applicazioni.

Adesso l'utente può accedere a Kaspersky Security Center con l'account personalizzato e monitorare le statistiche di protezione della rete in modalità Solo dashboard.

Rapporti

Questa sezione descrive come utilizzare i rapporti, gestire i modelli di rapporti personalizzati, utilizzare i modelli di rapporti per generarne di nuovi e creare attività di distribuzione dei rapporti.

Utilizzo dei rapporti

La funzionalità Rapporti consente di ottenere informazioni numeriche dettagliate sulla sicurezza della rete dell'organizzazione, nonché di salvare le informazioni in un file, inviarlo tramite e-mail e stamparlo.

I rapporti sono disponibili in Kaspersky Security Center Web Console, nella sezione **Monitoraggio e generazione dei rapporti**, facendo clic su **Rapporti**.

Per impostazione predefinita, i rapporti includono informazioni relative agli ultimi 30 giorni.

Kaspersky Security Center dispone di un set predefinito di rapporti per le seguenti categorie:

- **Stato protezione**
- **Distribuzione**
- **Aggiornamento**
- **Statistiche delle minacce**
- **Altro**

È possibile creare modelli di rapporto personalizzati, modificare i modelli di rapporto ed eliminarli.

È possibile creare rapporti basati su modelli esistenti, esportare i rapporti in file e creare attività per l'invio dei rapporti.

Creazione di un modello di rapporto

Per creare un modello di rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuovo modello di rapporto. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
3. Immettere il nome del rapporto e selezionare il tipo di rapporto.
4. Nel passaggio **Ambito** della procedura guidata selezionare il set di dispositivi client (gruppo di amministrazione, selezione dispositivi, dispositivi selezionati o tutti i dispositivi nella rete) per cui visualizzare i dati nei rapporti basati su questo modello di rapporto.
5. Nel passaggio **Periodo di generazione del rapporto** della procedura guidata specificare il periodo del rapporto. I valori disponibili sono i seguenti:

   - Tra le due date specificate
   - Dalla data specificata alla data di creazione del rapporto
   - Dalla data di creazione del rapporto meno il numero specificato di giorni alla data di creazione del rapporto

   Questa pagina potrebbe non essere visualizzata per alcuni rapporti.
6. Fare clic su **OK** per chiudere la procedura guidata.
7. Eseguire una delle seguenti operazioni:

   - Fare clic sul pulsante **Salva ed esegui** per salvare il nuovo modello di rapporto ed eseguire un rapporto basato su di esso.

     Il modello di rapporto verrà salvato. Il rapporto verrà generato.
   - Fare clic sul pulsante **Salva** per salvare il nuovo modello di rapporto.

     Il modello di rapporto verrà salvato.

È possibile utilizzare il nuovo modello per la creazione e la visualizzazione dei rapporti.

Visualizzazione e modifica delle proprietà dei modelli di rapporto

È possibile visualizzare e modificare le proprietà di base di un modello di rapporto, ad esempio il nome del modello di rapporto o i campi visualizzati nel rapporto.

Per visualizzare e modificare le proprietà di un modello di rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Selezionare la casella di controllo accanto al modello di rapporto per cui si desidera visualizzare e modificare le proprietà.

   In alternativa, è possibile generare il rapporto e quindi fare clic sul pulsante **Modifica**.
3. Fare clic sul pulsante **Apri proprietà del modello di rapporto**.

   Verrà visualizzata la finestra **Modifica del rapporto <Nome rapporto>** con la scheda **Generale** selezionata.

4. Modificare le proprietà del modello di rapporto:

- Scheda **Generale**:
  - Nome del modello di rapporto
  - Numero massimo di voci da visualizzare

    Se questa opzione è abilitata, il numero di voci visualizzate nella tabella con i dati dettagliati del rapporto non supera il valore specificato.

    Le voci nei rapporti vengono prima ordinate in base alle regole specificate nella sezione **Campi** → **Campi dettagli** delle proprietà del modello di rapporto, quindi vengono mantenute solo le prime voci risultanti. Il titolo della tabella con i dati dettagliati del rapporto mostra il numero di voci visualizzate e il numero totale di voci disponibili, corrispondenti alle altre impostazioni del modello di rapporto.

    Se questa opzione è disabilitata, la tabella con i dati dettagliati del rapporto conterrà tutte le voci disponibili. Non è consigliabile disabilitare questa opzione. La limitazione del numero di voci visualizzate nel rapporto consente di ridurre il carico sul sistema di gestione database (DBMS) e il tempo necessario per la creazione e l'esportazione del rapporto. Alcuni rapporti contengono un numero eccessivo di voci. In questi casi, potrebbe essere difficile leggerle e analizzarle tutte. Inoltre, nel dispositivo potrebbe verificarsi l'esaurimento della memoria durante la generazione di un rapporto e, in questo caso, non sarà possibile visualizzare il rapporto.

    Per impostazione predefinita, questa opzione è abilitata. Il valore predefinito è 1000.

  - **Gruppo**

    Fare clic sul pulsante **Impostazioni** per modificare il set di dispositivi client per cui viene creato il rapporto. Per alcuni tipi di rapporti, il pulsante potrebbe non essere disponibile. Le impostazioni effettive dipendono dalle impostazioni specificate durante la creazione del modello di rapporto.

  - **Intervallo**

    Fare clic sul pulsante **Impostazioni** per modificare il periodo del rapporto. Per alcuni tipi di rapporti, il pulsante potrebbe non essere disponibile. I valori disponibili sono i seguenti:

    - Tra le due date specificate
    - Dalla data specificata alla data di creazione del rapporto
    - Dalla data di creazione del rapporto meno il numero specificato di giorni alla data di creazione del rapporto

  - Includi i dati degli Administration Server secondari e virtuali

    Se questa opzione è abilitata, il rapporto include le informazioni ottenute dagli Administration Server secondari e virtuali subordinati all'Administration Server per cui viene creato il modello di rapporto.

    Disabilitare questa opzione per visualizzare solo i dati relativi all'Administration Server corrente.

    Per impostazione predefinita, questa opzione è abilitata.

  - Fino al livello di nidificazione

Il rapporto include i dati degli Administration Server secondari e virtuali posizionati al di sotto dell'Administration Server corrente a un livello di nidificazione minore o uguale al valore specificato.

Il valore predefinito è 1. È consigliabile modificare questo valore se è necessario recuperare informazioni da Administration Server secondari posizionati a livelli inferiori della struttura.

- **Intervallo di attesa dati (min.)**

  Prima della generazione del rapporto, l'Administration Server per cui viene creato il modello di rapporto attende i dati dagli Administration Server secondari per il numero di minuti specificato. Se non viene ricevuto alcun dato da un Administration Server secondario al termine di questo periodo, il rapporto viene eseguito comunque. Anziché i dati effettivi, il rapporto mostra i dati recuperati dalla cache (se è abilitata l'opzione **Salva nella cache i dati degli Administration Server secondari**) oppure **N/D** (non disponibile) in caso contrario.

  Il valore predefinito è 5 (minuti).

- **Salva nella cache i dati degli Administration Server secondari**

  Gli Administration Server secondari trasferiscono regolarmente i dati all'Administration Server per cui viene creato il modello di rapporto. I dati trasferiti vengono quindi archiviati nella cache.

  Se l'Administration Server corrente non riesce a ricevere i dati da un Administration Server secondario durante la generazione del rapporto, il rapporto mostra i dati recuperati dalla cache. Verrà anche visualizzata la data in cui i dati sono stati trasferiti nella cache.

  Se questa opzione è abilitata, è possibile visualizzare le informazioni dagli Administration Server secondari, anche se non è possibile recuperare i dati aggiornati. I dati visualizzati potrebbero tuttavia essere obsoleti.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Frequenza di aggiornamento cache (ore)**

  A intervalli regolari gli Administration Server secondari trasferiscono i dati all'Administration Server per cui viene creato il modello di rapporto. È possibile specificare questo periodo in ore. Se si specificano 0 ore, i dati vengono trasferiti solo al momento della generazione del rapporto.

  Il valore predefinito è 0.

- **Trasferisci informazioni dettagliate dagli Administration Server secondari**

  Nel rapporto generato, la tabella con i dati dettagliati del rapporto include i dati ottenuti dagli Administration Server secondari dell'Administration Server per cui viene creato il modello di rapporto.

  L'abilitazione di questa opzione rallenta la generazione dei rapporti e aumenta il traffico tra gli Administration Server. È tuttavia possibile visualizzare tutti i dati in un solo rapporto.

  Anziché attivare questa opzione, può essere preferibile analizzare i dati dettagliati del rapporto per identificare un Administration Server secondario che presenta problemi e quindi generare lo stesso rapporto solo per tale Administration Server.

  Per impostazione predefinita, questa opzione è disabilitata.

- Scheda **Campi**

Selezionare i campi che verranno visualizzati nel rapporto e utilizzare i pulsanti **Sposta su** e **Sposta giù** per modificare l'ordine dei campi. Utilizzare il pulsante **Aggiungi** o **Modifica** per specificare se le informazioni nel rapporto devono essere ordinate e filtrate in base a ciascuno dei campi.

Nella sezione **Filtri di Campi dettagli** è inoltre possibile fare clic sul pulsante **Converti filtri** per iniziare a utilizzare il formato di filtro esteso. Questo formato consente di combinare le condizioni di filtro specificate in vari campi utilizzando l'operatore logico OR. Dopo aver fatto clic sul pulsante, il pannello **Converti filtri** si aprirà a destra. Fare clic sul pulsante **Converti filtri** per confermare la conversione. Adesso è possibile definire un filtro convertito con condizioni dalla sezione **Campi dettagli** che vengono applicate utilizzando l'operatore logico OR.

> La conversione di un rapporto nel formato che supporta condizioni di filtro complesse renderà il rapporto incompatibile con le versioni precedenti di Kaspersky Security Center (11 e precedenti). Inoltre, il rapporto convertito non conterrà alcun dato degli Administration Server secondari che eseguono le versioni incompatibili.

5. Fare clic su **Salva** per salvare le modifiche.
6. Chiudere la finestra **Modifica del rapporto <nome rapporto>**.

Il modello di rapporto aggiornato verrà visualizzato nell'elenco dei modelli di rapporto.

Esportazione di un rapporto in un file

È possibile esportare un rapporto in un file XML, HTML o PDF.

Per esportare un rapporto in un file:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Selezionare la casella di controllo accanto al rapporto che si desidera esportare in un file.
3. Fare clic sul pulsante **Esporta rapporto**.
4. Nella finestra visualizzata modificare il nome del file del rapporto nel campo **Nome**. Per impostazione predefinita, il nome del file coincide con il nome del modello di rapporto selezionato.
5. Selezionare il tipo di file del rapporto: XML, HTML o PDF.
6. Fare clic sul pulsante **Esporta rapporto**.

   Il rapporto nel formato selezionato verrà scaricato nel dispositivo (nella cartella predefinita del dispositivo) o verrà visualizzata una finestra **Salva con nome** standard nel browser per consentire di salvare il file nella posizione desiderata.

Il rapporto verrà salvato nel file.

Generazione e visualizzazione di un rapporto

Per creare e visualizzare un rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Fare clic sul nome del modello di rapporto che si desidera utilizzare per creare un rapporto.

   Verrà generato e visualizzato un rapporto che utilizza il modello selezionato.

I dati del rapporto vengono visualizzati in base alla localizzazione impostata per Administration Server.

Il rapporto include i seguenti dati:

- Nella scheda **Riepilogo**:
  - Nome e tipo di rapporto, breve descrizione e periodo di generazione del rapporto, oltre che informazioni sul gruppo di dispositivi per cui è stato generato il rapporto.
  - Grafico con i dati più significativi del rapporto.
  - Tabella consolidata con indicatori del rapporto calcolati.
- Nella scheda **Dettagli** viene visualizzata una tabella con dati dettagliati sul rapporto.

Creazione di un'attività di invio dei rapporti

È possibile creare un'attività per l'invio dei rapporti selezionati.

Per creare un'attività di invio dei rapporti:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Rapporti**.
2. Selezionare le caselle di controllo accanto ai modelli di rapporto per cui si desidera creare un'attività di invio dei rapporti.
3. Fare clic sul pulsante **Crea attività di consegna**.

   Verrà avviata la Creazione guidata nuova attività. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.
4. Al passaggio **Impostazioni nuova attività** della procedura guidata immettere il nome dell'attività.

   Il nome predefinito è **Invia rapporti**. Se esiste già un'attività con questo nome, viene aggiunto un numero di sequenza (<N>) al nome dell'attività.

5. Al passaggio **Configurazione rapporto** della procedura guidata, specificare le seguenti impostazioni:

   a. Modelli di rapporti che devono essere inviati dall'attività.

   b. Formato del rapporto: HTML, XLS o PDF.

      Lo strumento wkhtmltopdf è necessario per convertire un rapporto in formato PDF. Quando si seleziona l'opzione PDF, Administration Server verifica se lo strumento wkhtmltopdf è installato nel dispositivo. Se lo strumento non è installato, l'applicazione mostra un messaggio in cui si richiede di installare lo strumento nel dispositivo Administration Server. Installare lo strumento manualmente, quindi continuare con il passaggio successivo.

   c. Se i rapporti devono essere inviati tramite e-mail, insieme alle impostazioni di notifica tramite e-mail.

      È possibile specificare fino a 20 indirizzi e-mail. Per separare gli indirizzi e-mail, premere **Invio**. È inoltre possibile incollare un elenco di indirizzi e-mail separati da virgole, quindi premere **Invio**.

   d. Se i rapporti devono essere salvati in una cartella, se i rapporti salvati precedentemente in questa cartella devono essere sovrascritti e se deve essere utilizzato un account specifico per accedere alla cartella (per una cartella condivisa).

6. Al passaggio **Configurare la pianificazione delle attività** della procedura guidata, selezionare la pianificazione dell'avvio dell'attività.

   Sono disponibili le seguenti opzioni di pianificazione delle attività:

   - **Manualmente**

     L'attività non viene eseguita automaticamente. È possibile avviarla solo manualmente.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Ogni N minuti**

     L'attività viene eseguita periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata nel giorno in cui viene creata l'attività.

     Per impostazione predefinita, l'attività viene eseguita ogni 30 minuti, a partire dall'ora di sistema corrente.

   - **Ogni N ore**

     L'attività viene eseguita periodicamente, con l'intervallo specificato in ore, a partire dalla data e dall'ora specificate.

     Per impostazione predefinita, l'attività viene eseguita ogni sei ore, a partire dalla data e dall'ora di sistema correnti.

   - **Ogni N giorni**

     L'attività viene eseguita periodicamente, con l'intervallo specificato in giorni. È inoltre possibile specificare data e ora della prima esecuzione dell'attività. Queste opzioni aggiuntive diventano disponibili se sono supportate dall'applicazione per cui viene creata l'attività.

     Per impostazione predefinita, l'attività viene eseguita ogni giorno, a partire dalla data e dall'ora di sistema correnti.

   - **Ogni N settimane**

     L'attività viene eseguita periodicamente, con l'intervallo specificato in settimane, nel giorno della settimana specificato e all'ora specificata.

     Per impostazione predefinita, l'attività viene eseguita ogni lunedì all'ora di sistema corrente.

   - **Mensile**

     L'attività viene eseguita periodicamente, nel giorno del mese specificato, all'ora specificata.

     Nei mesi che non comprendono il giorno specificato, l'attività viene eseguita l'ultimo giorno.

     Per impostazione predefinita, l'attività viene eseguita il primo giorno di ogni mese, all'ora di sistema corrente.

   - **Nei giorni specificati**

L'attività viene eseguita periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

Per impostazione predefinita, l'ora di inizio è le 18:00 e non viene selezionato alcun giorno del mese.

Si noti che non si seleziona né una data specifica nel mese, né il numero della settimana (prima, seconda settimana del mese) ma il numero progressivo del giorno della settimana in un mese. Se ad esempio si imposta il cursore nella cella **Ma** della riga **Prima**, significa che l'attività verrà eseguita ogni primo martedì di ogni nuovo mese.

È possibile selezionare più giorni della settimana.

- Durante un'epidemia di virus

L'attività viene eseguita dopo che si verifica un evento *Epidemia di virus*. Selezionare i tipi di applicazione da cui dovranno essere monitorate le epidemie di virus. Sono disponibili i seguenti tipi di applicazione:

- Anti-virus per workstation e file server
- Anti-virus per la difesa perimetrale
- Anti-virus per i sistemi di posta

Per impostazione predefinita, sono selezionati tutti i tipi di applicazione.

Può essere utile eseguire differenti attività a seconda del tipo di applicazione di protezione che segnala un'epidemia di virus. In questo caso, rimuovere la selezione dei tipi di applicazione non necessari.

- Al completamento di un'altra attività

L'attività corrente viene avviata dopo il completamento di un'altra attività. Questa opzione funziona solo se entrambe le attività sono assegnate agli stessi dispositivi. È ad esempio possibile eseguire l'attività *Gestisci dispositivi* con l'opzione **Accendi il dispositivo** e, al termine, eseguire l'attività *Scansione virus* come attività di attivazione.

È necessario selezionare l'attività di attivazione nella tabella e lo stato con cui questa attività deve essere completata (**Completato** o **Non riuscito**).

Se necessario, è possibile cercare, ordinare e filtrare le attività nella tabella come segue:

- Immettere il nome dell'attività nel campo di ricerca per cercare l'attività in base al nome.
- Fare clic sull'icona di ordinamento per ordinare le attività in base al nome.

  Per impostazione predefinita, le attività sono disposte in ordine alfabetico crescente.
- Fare clic sull'icona del filtro e, nella finestra visualizzata, filtrare le attività in base al gruppo, quindi fare clic sul pulsante **Applica**.

7. In questo passaggio della procedura guidata configurare altre impostazioni di pianificazione delle attività:

- Nella sezione **Pianificazione delle attività** controllare o riconfigurare la pianificazione selezionata in precedenza e impostare l'intervallo di tempo, i giorni del mese o della settimana, impostare la condizione di epidemia di virus o completare un'altra attività come trigger per l'avvio dell'attività. È inoltre possibile specificare un'ora di inizio in questa sezione se è stata selezionata una pianificazione applicabile.

- Nella sezione **Altre impostazioni** specificare le seguenti impostazioni:

  - **Esegui attività non effettuate**

    Questa opzione determina il comportamento di un'attività se un dispositivo client non è visibile nella rete al momento dell'avvio dell'attività.

    Se questa opzione è abilitata, il sistema tenta di avviare l'attività alla successiva esecuzione di un'applicazione Kaspersky in un dispositivo client. Se la pianificazione dell'attività è **Manualmente**, **Una sola volta** o **Immediatamente**, l'attività viene avviata non appena il dispositivo diventa visibile nella rete o subito dopo che il dispositivo viene incluso nell'ambito dell'attività.

    Se questa opzione è disabilitata, solo le attività pianificate vengono eseguite nei dispositivi client. Per i tipi di pianificazione **Manualmente**, **Una sola volta** e **Immediatamente**, le attività vengono eseguite solo nei dispositivi client visibili nella rete. È ad esempio possibile disabilitare questa opzione per un'attività con un notevole utilizzo di risorse che si desidera eseguire solo in orario non lavorativo.

    Per impostazione predefinita, questa opzione è disabilitata.

  - **Usa automaticamente il ritardo casuale per l'avvio delle attività**

    Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno di un intervallo di tempo specificato (*avvio distribuito dell'attività*). L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

    Il periodo di avvio distribuito viene calcolato automaticamente durante la creazione di un'attività, in base al numero di dispositivi client a cui è assegnata l'attività. Successivamente, l'attività viene sempre eseguita all'ora di inizio calcolata. Tuttavia, quando si modificano le impostazioni dell'attività o l'attività viene avviata manualmente, il valore calcolato dell'ora di inizio dell'attività cambia.

    Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

  - **Usa ritardo casuale automaticamente per l'avvio delle attività con un intervallo di**

    Se questa opzione è abilitata, l'attività viene avviata nei dispositivi client in modo casuale all'interno dell'intervallo di tempo specificato. L'avvio distribuito dell'attività consente di evitare che Administration Server riceva numerose richieste simultanee da parte dei dispositivi client durante l'esecuzione di un'attività pianificata.

    Se questa opzione è disabilitata, l'attività viene avviata nei dispositivi client in base alla pianificazione.

    Per impostazione predefinita, questa opzione è disabilitata. Il periodo di tempo predefinito è 1 minuto.

  - **Arresta se l'attività viene eseguita per più di**

Al termine del periodo di tempo specificato, l'attività viene arrestata automaticamente, che sia stata completata o meno.

Abilitare questa opzione se si desidera interrompere (o arrestare) le attività che richiedono troppo tempo per l'esecuzione.

Per impostazione predefinita, questa opzione è disabilitata. Il tempo predefinito per l'esecuzione dell'attività è 120 minuti.

8. Nel passaggio della procedura guidata **Selezione di un account per l'esecuzione dell'attività** specificare le credenziali dell'account utente utilizzato per l'esecuzione dell'attività.

9. Se si desidera modificare altre impostazioni dell'attività dopo averla creata, nel passaggio **Completare la creazione dell'attività** della procedura guidata abilitare l'opzione **Apri i dettagli dell'attività al termine della creazione** (per impostazioni predefinita, questa opzione è abilitata).

10. Fare clic sul pulsante **Fine** per creare l'attività e chiudere la procedura guidata.

    Verrà creata l'attività di invio dei rapporti. Se è stata abilitata l'opzione **Apri i dettagli dell'attività al termine della creazione**, verrà visualizzata la finestra delle impostazioni dell'attività.

Eliminazione di modelli di rapporto

Per eliminare uno o più modelli di rapporto:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Rapporti**.

2. Selezionare le caselle di controllo accanto ai modelli di rapporto che si desidera eliminare.

3. Fare clic sul pulsante **Elimina**.

4. Nella finestra visualizzata fare clic su **OK** per confermare la selezione.

I modelli di rapporto selezionati verranno eliminati. Se questi modelli di rapporto sono stati inclusi nelle attività di invio dei rapporti, verranno rimossi anche dalle attività.

Eventi e selezioni di eventi

Questa sezione fornisce informazioni sugli eventi e sulle selezioni di eventi, sui tipi di eventi che si verificano nei componenti di Kaspersky Security Center e sulla gestione del blocco degli eventi frequenti.

Informazioni sugli eventi di Kaspersky Security Center

Kaspersky Security Center consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Le informazioni sugli eventi vengono salvate nel database di Administration Server.

Tipi di evento

In Kaspersky Security Center sono disponibili i seguenti tipi di eventi:

- Eventi generici. Questi eventi si verificano in tutte le applicazioni Kaspersky gestite. Un esempio di evento generico è l'Epidemia di virus. Gli eventi generici hanno sintassi e semantica rigorosamente definite. Gli eventi generici vengono ad esempio utilizzati nei rapporti e nei dashboard.
- Eventi specifici delle applicazioni gestiti da Kaspersky. Ogni applicazione Kaspersky gestita dispone di uno specifico set di eventi.

Origini eventi

Gli eventi possono essere generati dalle seguenti applicazioni:

- Componenti di Kaspersky Security Center:
  - Administration Server
  - Network Agent
  - Server per dispositivi mobili MDM iOS
  - Server per dispositivi mobili Exchange
- Applicazioni Kaspersky gestite

  Per i dettagli sugli eventi generati dalle applicazioni gestite da Kaspersky, consultare la documentazione dell'applicazione corrispondente.

È possibile visualizzare l'elenco completo degli eventi che possono essere generati da un'applicazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare l'elenco degli eventi nelle proprietà dell'Administration Server.

Livello di importanza degli eventi

Ogni evento dispone di uno specifico livello di importanza. In base alle condizioni in cui si verifica, a un evento possono essere assegnati diversi livelli di importanza. Esistono quattro livelli di importanza degli eventi:

- Un *evento critico* è un evento che indica la presenza di un problema critico che può determinare una perdita dei dati, un malfunzionamento o un errore critico.
- Un *errore funzionale* è un evento che indica la presenza di un problema grave, un errore o un malfunzionamento che si è verificato durante l'esecuzione dell'applicazione o di una procedura.
- Un *avviso* è un evento che non è necessariamente grave, ma indica comunque un potenziale problema futuro. La maggior parte degli eventi viene designata come avviso se l'applicazione può essere ripristinata senza perdite di dati o funzionalità importanti dopo che si sono verificati tali eventi.
- Un *evento informativo* è un evento che si verifica allo scopo di segnalare il completamento di un'operazione, il corretto funzionamento dell'applicazione o il completamento di una procedura.

Ogni evento ha un periodo di archiviazione definito, durante il quale può essere visualizzato o modificato in Kaspersky Security Center. Alcuni eventi non vengono salvati nel database di Administration Server per impostazione predefinita, poiché il relativo periodo di archiviazione definito è pari a zero. Solo gli eventi che verranno memorizzati nel database di Administration Server per almeno un giorno possono essere esportati in sistemi esterni.

Utilizzo di selezioni eventi

Le selezioni eventi consentono di visualizzare i set denominati degli eventi selezionati dal database di Administration Server. Questi set di eventi sono raggruppati in base alle seguenti categorie:

- In base al livello di importanza: **Eventi critici**, **Errori funzionali**, **Avvisi** e **Eventi informativi**
- In base al tempo: **Eventi recenti**
- In base al tipo: **Richieste utente** e **Eventi di controllo**

È possibile creare e visualizzare le selezioni eventi definite dall'utente in base alle impostazioni disponibili per la configurazione nell'interfaccia di Kaspersky Security Center Web Console.

Le selezioni eventi sono disponibili in Kaspersky Security Center Web Console, nella sezione **Monitoraggio e generazione dei rapporti**, facendo clic su **Selezioni eventi**.

Per impostazione predefinita, le selezioni eventi includono informazioni relative agli ultimi sette giorni.

Kaspersky Security Center dispone di un set predefinito di selezioni eventi (preimpostate):

- Eventi con diversi livelli di importanza:
  - **Eventi critici**
  - **Errori funzionali**
  - **Avvisi**
  - **Eventi informativi**
- **Richieste utente** (eventi delle applicazioni gestite)
- **Eventi recenti** (nell'ultima settimana)
- **Eventi di controllo**.

È inoltre possibile creare e configurare ulteriori selezioni definite dall'utente. Nelle selezioni definite dall'utente è possibile filtrare gli eventi in base alle proprietà dei dispositivi da cui hanno avuto origine (nomi dei dispositivi, intervalli IP e gruppi di amministrazione), per tipi di eventi e livelli di criticità, per nome dell'applicazione e del componente e per intervallo di tempo. È anche possibile includere i risultati delle attività nell'ambito della ricerca. È inoltre disponibile un semplice campo di ricerca, in cui è possibile digitare una o più parole. Vengono visualizzati tutti gli eventi che contengono una delle parole digitate in qualsiasi punto dei relativi attributi (come nome dell'evento, descrizione o nome del componente).

Sia per le selezioni predefinite che per quelle definite dall'utente, è possibile limitare il numero di eventi visualizzati o il numero di record da cercare. Entrambe le opzioni influiscono sul tempo richiesto da Kaspersky Security Center per visualizzare gli eventi. Più grande è il database, più tempo può richiedere il processo.

È possibile procedere come segue:

- Modificare le proprietà delle selezioni eventi
- Generare selezioni eventi
- Visualizzare i dettagli delle selezioni eventi
- Eliminare le selezioni eventi
- Eliminare gli eventi dal database di Administration Server

Creazione di una selezione eventi

Per creare una selezione eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.
2. Fare clic su **Aggiungi**.
3. Nella finestra **Nuova selezione eventi** visualizzata specificare le impostazioni della nuova selezione eventi. Eseguire tale operazione in una o più sezioni della finestra.
4. Fare clic su **Salva** per salvare le modifiche.

   Verrà visualizzata la finestra di conferma.
5. Per visualizzare i risultati della selezione eventi, mantenere selezionata la casella di controllo **Vai al risultato della selezione**.
6. Fare clic su **Salva** per confermare la creazione della selezione eventi.

Se è stata mantenuta selezionata la casella di controllo **Vai al risultato della selezione**, verranno visualizzati i risultati della selezione eventi. In caso contrario, la nuova selezione eventi verrà visualizzata nell'elenco delle selezioni eventi.

Modifica di una selezione eventi

Per modificare una selezione eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.
2. Selezionare la casella di controllo accanto alla selezione eventi che si desidera modificare.
3. Fare clic sul pulsante **Proprietà**.

   Verrà visualizzata una finestra delle impostazioni della selezione eventi.

4. Modificare le proprietà della selezione eventi.

> Per le selezioni di eventi predefinite, è possibile modificare solo le proprietà nelle seguenti schede: **Generale** (tranne il nome della selezione), **Data/ora** e **Diritti di accesso**.

Per le selezioni definite dall'utente, è possibile modificare tutte le proprietà.

5. Fare clic su **Salva** per salvare le modifiche.

La selezione eventi modificata verrà visualizzata nell'elenco.

Visualizzazione di un elenco di una selezione eventi

Per visualizzare una selezione eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.
2. Selezionare la casella di controllo accanto alla selezione eventi che si desidera avviare.
3. Eseguire una delle seguenti operazioni:
   - Se si desidera configurare l'ordinamento dei risultati della selezione eventi, effettuare le seguenti operazioni:
     a. Fare clic sul pulsante **Riconfigura ordinamento e avvia**.
     b. Nella finestra **Riconfigurare l'ordinamento per la selezione eventi** visualizzata specificare le impostazioni di ordinamento.
     c. Fare clic sul nome della selezione.
   - In caso contrario, se si desidera visualizzare l'elenco degli eventi in base all'ordinamento in Administration Server, fare clic sul nome della selezione.

Verranno visualizzati i risultati della selezione eventi.

Esportazione di una selezione di eventi

Kaspersky Security Center consente di salvare una selezione di eventi e le relative impostazioni in un file KLO. È possibile utilizzare questo file KLO per importare la selezione di eventi salvata sia per Kaspersky Security Center Windows che per Kaspersky Security Center Linux.

> Si noti che è possibile esportare solo le selezioni di eventi definite dall'utente. Le selezioni di eventi dal set predefinito di Kaspersky Security Center (selezioni predefinite) non possono essere salvate in un file.

Per esportare una selezione di eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.
2. Selezionare la casella di controllo accanto alla selezione eventi che si desidera esportare.

   Non è possibile esportare più selezioni di eventi contemporaneamente. Se si selezionano più selezioni, il pulsante **Esporta** verrà disabilitato.
3. Fare clic sul pulsante **Esporta**.
4. Nella finestra **Salva con nome** aperta, specificare il nome e il percorso del file della selezione di eventi, quindi fare clic sul pulsante **Salva**.

   La finestra **Salva con nome** viene visualizzata solo se si utilizza Google Chrome, Microsoft Edge oppure Opera. Se si utilizza un altro browser, il file della selezione di eventi viene salvato automaticamente nella cartella **Download**.

Importazione di una selezione di eventi

Kaspersky Security Center consente di importare una selezione di eventi da un file KLO. Il file KLO contiene la selezione di eventi esportata e le sue impostazioni.

Per importare una selezione di eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Selezioni eventi**.
2. Fare clic sul pulsante **Importa**, quindi scegliere una selezione di eventi che si desidera importare.
3. Nella finestra visualizzata, specificare il percorso del file KLO, quindi fare clic sul pulsante **Apri**. Si noti che è possibile selezionare solo una selezione di eventi.

   Viene avviata l'elaborazione della selezione di eventi.

Viene visualizzata la notifica con i risultati dell'importazione. Se la selezione di eventi viene importata correttamente, è possibile fare clic sul collegamento **Visualizza dettagli importazione** per visualizzare le proprietà della selezione di eventi.

Dopo un'importazione riuscita, la selezione di eventi viene visualizzata nell'elenco delle selezioni. Vengono importate anche le impostazioni della selezione di eventi.

Se la selezione di eventi appena importata ha un nome identico a quello di una selezione di eventi esistente, il nome della selezione importata viene espanso con l'indice **(<numero progressivo successivo>)**, ad esempio: **(1)**, **(2)**.

Visualizzazione dei dettagli di un evento

Per visualizzare i dettagli di un evento:

1. Avviare una selezione eventi.
2. Fare clic sull'ora dell'evento desiderato.
   Verrà visualizzata la finestra **Proprietà evento**.
3. Nella finestra visualizzata è possibile eseguire le seguenti operazioni:
   - Visualizzare le informazioni sull'evento selezionato
   - Passare all'evento successivo e all'evento precedente nei risultati della selezione eventi
   - Passare al dispositivo in cui si è verificato l'evento
   - Passare al gruppo di amministrazione che include il dispositivo in cui si è verificato l'evento
   - Per un evento correlato a un'attività, passare alle proprietà dell'attività

Esportazione degli eventi in un file

Kaspersky Security Center consente di salvare gli eventi da una selezione di eventi in un file TXT.

Per esportare gli eventi in un file:

1. Avviare una selezione eventi.
2. Selezionare la casella di controllo accanto all'evento desiderato.
   È inoltre possibile selezionare più eventi o l'intera selezione di eventi.
3. Fare clic sul pulsante **Esporta in un file**.

L'evento selezionato verrà esportato in un file TXT.

Visualizzazione della cronologia di un oggetto da un evento

Da un evento di creazione o di modifica di un oggetto che supporta la gestione delle revisioni, è possibile passare alla cronologia delle revisioni dell'oggetto.

Per visualizzare la cronologia di un oggetto da un evento:

1. Avviare una selezione eventi.
2. Selezionare la casella di controllo accanto all'evento desiderato.
3. Fare clic sul pulsante **Cronologia revisioni**.

   Verrà aperta la cronologia delle revisioni dell'oggetto.

Eliminazione di eventi

Per eliminare uno o più eventi:

1. Avviare una selezione eventi.
2. Selezionare le caselle di controllo accanto agli eventi desiderati.
3. Fare clic sul pulsante **Elimina**.

   Gli eventi selezionati verranno eliminati e non potranno essere ripristinati.

Eliminazione di selezioni eventi

È possibile eliminare solo le selezioni eventi definite dall'utente. Le selezioni eventi predefinite non possono essere eliminate.

Per eliminare una o più selezioni eventi:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Selezioni eventi**.
2. Selezionare le caselle di controllo accanto alle selezioni eventi che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Nella finestra visualizzata fare clic su **OK**.

   La selezione eventi verrà eliminata.

Impostazione del periodo di archiviazione per un evento

Kaspersky Security Center consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Le informazioni sugli eventi vengono salvate nel database di Administration Server. Potrebbe essere necessario archiviare alcuni eventi per un periodo più o meno lungo di quanto specificato dai valori predefiniti. È possibile modificare le impostazioni predefinite del periodo di archiviazione per un evento.

Se non si è interessati all'archiviazione di alcuni eventi nel database di Administration Server, è possibile disabilitare l'impostazione appropriata nel criterio di Administration Server e nel criterio dell'applicazione Kaspersky o nelle proprietà di Administration Server (solo per gli eventi di Administration Server). Ciò consentirà di ridurre il numero dei tipi di eventi nel database.

Più lungo è il periodo di archiviazione per un evento, più velocemente il database raggiunge la capacità massima. Tuttavia, un periodo di archiviazione più lungo per un evento consente di eseguire le attività di monitoraggio e generazione dei rapporti per un periodo superiore.

Per impostare il periodo di archiviazione per un evento nel database di Administration Server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.
2. Fare clic sul nome del criterio desiderato.

   È possibile selezionare un criterio per un'applicazione Kaspersky gestita, Network Agent o Administration Server. Per Administration Server, è inoltre possibile configurare il periodo di archiviazione degli eventi facendo clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server desiderato.
3. Selezionare la scheda **Configurazione eventi**.

   Verrà visualizzato un elenco dei tipi di eventi correlati alla sezione **Critico**. Se necessario, è possibile passare alla sezione **Errore funzionale**, **Avviso** o **Informazioni**.
4. Nell'elenco dei tipi di eventi nel riquadro destro fare clic sul collegamento per l'evento di cui si desidera modificare il periodo di archiviazione.

   Nella sezione **Registrazione eventi** della finestra visualizzata l'interruttore **Archivia nel database di Administration Server per (giorni)** è abilitata.
5. Nella casella di modifica sotto questo interruttore inserire il numero di giorni per l'archiviazione dell'evento.
6. Se non si desidera archiviare un evento nel database di Administration Server, disabilitare l'opzione **Archivia nel database di Administration Server per (giorni)**.

   > Se si configurano gli eventi di Administration Server nella finestra delle proprietà di Administration Server e se le impostazioni degli eventi sono bloccate nel criterio di Kaspersky Security Center Administration Server, non è possibile ridefinire il valore del periodo di archiviazione per un evento.
7. Fare clic su **OK**, quindi, dopo aver chiuso il riquadro destro, fare clic sul pulsante **Salva**.

   La finestra delle proprietà del criterio verrà chiusa.

Da questo momento, quando Administration Server riceve e archivia gli eventi del tipo selezionato, questi avranno il periodo di archiviazione modificato. Administration Server non modifica il periodo di archiviazione degli eventi ricevuti in precedenza.

Eventi dei componenti di Kaspersky Security Center

Ogni componente Kaspersky Security Center dispone di uno specifico set di tipi di eventi. Questa sezione elenca i tipi di eventi che si verificano in Kaspersky Security Center Administration Server, Network Agent e iOS MDM Server. I tipi di eventi che si verificano nelle applicazioni Kaspersky non sono elencati in questa sezione.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Struttura dei dati della descrizione del tipo di evento

Per ogni tipo di evento, sono indicati il relativo nome visualizzato, l'identificatore (ID), il codice alfabetico, la descrizione e il periodo di archiviazione predefinito.

- **Nome visualizzato del tipo di evento**. Questo testo è visualizzato in Kaspersky Security Center durante la configurazione degli eventi e quando gli eventi si verificano.
- **ID del tipo di evento**. Questo codice numerico viene utilizzato durante l'elaborazione degli eventi tramite strumenti di terzi per l'analisi degli eventi.
- **Tipo di evento** (codice alfabetico). Questo codice viene utilizzato quando si esplorano e si elaborano gli eventi con le visualizzazione pubbliche disponibili nel database di Kaspersky Security Center e quando gli eventi vengono esportati in un sistema SIEM.
- **Descrizione**. Questo testo contiene le situazioni in cui si verifica un evento e come procedere in questo caso.
- **Periodo di archiviazione predefinito**. Rappresenta il numero di giorni per cui l'evento viene memorizzato nel database di Administration Server ed è visualizzato nell'elenco degli eventi in Administration Server. Al termine di questo periodo, l'evento viene eliminato. Se il valore per il periodo di archiviazione degli eventi è 0, gli eventi vengono rilevati ma non sono visualizzati nell'elenco degli eventi in Administration Server. Se è stato configurato il salvataggio di tali eventi nel registro eventi del sistema operativo, è possibile accedervi in tale posizione.

  È possibile modificare il periodo di archiviazione per gli eventi:

  - Administration Console: Impostazione del periodo di archiviazione per un evento
  - Kaspersky Security Center Web Console: Impostazione del periodo di archiviazione per un evento

Tra gli altri dati possono essere inclusi i seguenti campi:

- **event_id**: numero univoco dell'evento nel database, generato e assegnato automaticamente; da non confondere con l'**ID del tipo di evento**.
- **task_id**: l'ID dell'attività che ha causato l'evento (se presente)
- **criticità**: uno dei seguenti livelli di criticità (in ordine di criticità crescente):

  0) Livello di criticità non valido

  1) Informazioni

  2) Avviso

  3) Errore

  4) Critico

Eventi di Administration Server

Questa sezione contiene informazioni sugli eventi relativi ad Administration Server.

Eventi critici di Administration Server

La tabella seguente elenca i tipi di eventi di Kaspersky Security Center Administration Server con il livello di importanza **Critico**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Se è stata specificata la porta nella finestra delle proprietà di Administration Server in Administration Console, **Kaspersky Security Center pubblica le metriche** e gli eventi critici che devono essere ottenuti da Prometheus, un sistema per il monitoraggio e gli avvisi. Prometheus ottiene le metriche e gli eventi critici, quindi genera avvisi per ciascun evento.

// KL.KSC.Common—Kaspersky Security Center common counters

"xdr_klserver_errors", "counter", "klserver errors"

"xdr_klserver_api_calls_time", "counter", "klserver api calls time"

// KL.KSC.Transport—Transport counters set

"ksc_Transport__Number_of_all_connections", "counter", "number of all connections"

"ksc_Transport__Number_of_all_nagent_connection", "counter", "number of all Network Agent connection"

"ksc_Transport__Number_of_controlled_nagent_connections", "counter", "number of controlled Network Agent connections"

"ksc_Transport__Total_active_hosts_count", "gauge", "total active devices count"

"ksc_Transport__Number_of_pings_processed", "counter", "number of pings processed"

"ksc_Transport__Number_of_pings_rejected", "counter", "number of pings rejected"

"ksc_Transport__Number_of_ping_processing_errors", "counter", "number of ping processing errors"

"ksc_Transport__Number_of_TCP_connections_accepted", "counter", "number of TCP connections accepted"

"ksc_Transport__Number_of_failed_TCP_connections", "counter", "number of failed TCP connections"

"ksc_Transport__Bytes_sent_by_TCP", "counter", "bytes sent by TCP"

"ksc_Transport__Bytes_received_by_TCP", "counter", "bytes received by TCP"

"ksc_Transport__Number_of_GetNextFileChunk_requests", "counter", "number of GetNextFileChunk requests"

"ksc_Transport__Number_of_GetNextFileChunk_rejected", "counter", "number of GetNextFileChunk rejected"

"ksc_Transport__Bytes_transmitted_through_GetNextFileChunk", "counter", "bytes transmitted through GetNextFileChunk"

// KL.KSC.Events—Events delivery counters set

"ksc_Events__Number_of_event_bulks_processed", "counter", "number of event bulks processed"

"ksc_Events__Number_of_event_bulks_rejected", "counter", "number of event bulks rejected"

"ksc_Events__Number_of_event_bulks_processing_errors", "counter", "number of event bulks processing errors"

"ksc_Events__Number_of_event_bulks_processing_just_now", "gauge", "number of event bulks processing just now"

"ksc_Events__Number_of_events_processed", "counter", "number of events processed"

"ksc_Events__Number_of_events_rejected", "counter", "number of events rejected"

"ksc_Events__Number_of_events_processing_errors", "counter", "number of events processing errors"

"ksc_Events__Number_of_events_processing_just_now", "gauge", "number of events processing just now"

// KL.KSC.Resources—Kaspersky Security Center resources usage

"ksc_Resources__CPU_time_in_user_mode", "counter", "CPU time in user mode"

"ksc_Resources__CPU_time_in_kernel_mode", "counter", "CPU time in kernel mode"

"ksc_Resources__PID_of_klserver_process", "gauge", "process ID of klserver"

"ksc_Resources__PID_of_klnagent_process", "gauge", "process ID of klnagent"

"ksc_Resources__Available_disk_user_quota_for_server_data", "gauge", "available disk user quota for server data"

"ksc_Resources__Available_disk_user_quota_for_packages", "gauge", "available disk user quota for packages"

"ksc_Resources__Current_OpenAPI_threads_count", "counter", "current OpenAPI threads count"

"ksc_Resources__Maximum_OpenAPI_threads_count", "counter", "maximum OpenAPI threads count"

// KL.KSC.NLST

// KL.KSC.NLST.Trans.Common—List of server transactions

"ksc_NLST__Common__Current_transactions_count", "gauge", "current transactions count"

"ksc_NLST__Common__Transactions_queue_ful", "gauge", "transactions queue full"

"ksc_NLST__Common__Transactions_queue_near_to_ful", "gauge", "transactions queue near to full"

// KL.KSC.NLST.InvAppCtrlLink—Application Control link

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvSoft—Software Inventory

"ksc_NLST__Software_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Software_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Software_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Software_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Software_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Software_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Software_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Software_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Software_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.InvHard—Hardware Inventory

"ksc_NLST__Hardware_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Hardware_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Hardware_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Hardware_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Hardware_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Hardware_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Hardware_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Hardware_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Hardware_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DevCtrl—Device Control

"ksc_NLST__Device_control__items_changed", "gauge", "items changed"

"ksc_NLST__Device_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_control__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDM—Mobile Device Management

"ksc_NLST__Mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__Mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.MDMmails—Device management emails

"ksc_NLST__Device_management_emails__items_changed", "gauge", "items changed"

"ksc_NLST__Device_management_emails__items_deleted", "gauge", "items deleted"

"ksc_NLST__Device_management_emails__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Device_management_emails__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Device_management_emails__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Device_management_emails__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Device_management_emails__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Device_management_emails__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Device_management_emails__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AppCtrl—Application Control

"ksc_NLST__Application_control__items_changed", "gauge", "items changed"

"ksc_NLST__Application_control__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_control__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_control__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_control__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_control__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_control__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_control__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_control__transactions_in_queue", "gauge", "transactions in queue"

"ksc_NLST__Application_inventory__items_changed", "gauge", "items changed"

"ksc_NLST__Application_inventory__items_deleted", "gauge", "items deleted"

"ksc_NLST__Application_inventory__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Application_inventory__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Application_inventory__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Application_inventory__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Application_inventory__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Application_inventory__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Application_inventory__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.DPEErrors—Data protection errors

"ksc_NLST__Data_protection_errors__items_changed", "gauge", "items changed"

"ksc_NLST__Data_protection_errors__items_deleted", "gauge", "items deleted"

"ksc_NLST__Data_protection_errors__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Data_protection_errors__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Data_protection_errors__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Data_protection_errors__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Data_protection_errors__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Data_protection_errors__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Data_protection_errors__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.iOsMDM—iOS Mobile Device Management

"ksc_NLST__iOS_mobile_device_management__items_changed", "gauge", "items changed"

"ksc_NLST__iOS_mobile_device_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__iOS_mobile_device_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__iOS_mobile_device_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__iOS_mobile_device_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__iOS_mobile_device_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__iOS_mobile_device_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__iOS_mobile_device_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Vapm—Vulnerability assessment and patch management

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment_and_patch_management__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment_and_patch_management__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment_and_patch_management__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment_and_patch_management__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment_and_patch_management__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.Va—Vulnerability assessment

"ksc_NLST__Vulnerability_assesment__items_changed", "gauge", "items changed"

"ksc_NLST__Vulnerability_assesment__items_deleted", "gauge", "items deleted"

"ksc_NLST__Vulnerability_assesment__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Vulnerability_assesment__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Vulnerability_assesment__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Vulnerability_assesment__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Vulnerability_assesment__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Vulnerability_assesment__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Vulnerability_assesment__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.VM—Virtual machines

"ksc_NLST__Virtual_machines__items_changed", "gauge", "items changed"

"ksc_NLST__Virtual_machines__items_deleted", "gauge", "items deleted"

"ksc_NLST__Virtual_machines__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Virtual_machines__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Virtual_machines__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Virtual_machines__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Virtual_machines__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Virtual_machines__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Virtual_machines__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.WUS—Windows Update

"ksc_NLST__Windows_update__items_changed", "gauge", "items changed"

"ksc_NLST__Windows_update__items_deleted", "gauge", "items deleted"

"ksc_NLST__Windows_update__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Windows_update__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Windows_update__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Windows_update__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Windows_update__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Windows_update__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Windows_update__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.CIP_PLC—CIP PLC

"ksc_NLST__CIP_PLC__items_changed", "gauge", "items changed"

"ksc_NLST__CIP_PLC__items_deleted", "gauge", "items deleted"

"ksc_NLST__CIP_PLC__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__CIP_PLC__change_item_operations", "gauge", "change item operations"

"ksc_NLST__CIP_PLC__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__CIP_PLC__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__CIP_PLC__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__CIP_PLC__list_is_pending", "gauge", "list is pending"

"ksc_NLST__CIP_PLC__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.NagentNetScan—Network Agent Network Scan

"ksc_NLST__Network_scan__items_changed", "gauge", "items changed"

"ksc_NLST__Network_scan__items_deleted", "gauge", "items deleted"

"ksc_NLST__Network_scan__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Network_scan__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Network_scan__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Network_scan__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Network_scan__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Network_scan__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Network_scan__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.AS—Adaptive Security

"ksc_NLST__Adaptive_security__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.ASS—Adaptive Security State

"ksc_NLST__Adaptive_security_state__items_changed", "gauge", "items changed"

"ksc_NLST__Adaptive_security_state__items_deleted", "gauge", "items deleted"

"ksc_NLST__Adaptive_security_state__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Adaptive_security_state__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Adaptive_security_state__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Adaptive_security_state__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Adaptive_security_state__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Adaptive_security_state__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Adaptive_security_state__transactions_in_queue", "gauge", "transactions in queue"

// KL.KSC.NLST.KillChain—Kill Chain

"ksc_NLST__Kill_chain__items_changed", "gauge", "items changed"

"ksc_NLST__Kill_chain__items_deleted", "gauge", "items deleted"

"ksc_NLST__Kill_chain__DeleteAll_items", "gauge", "DeleteAll() items"

"ksc_NLST__Kill_chain__change_item_operations", "gauge", "change item operations"

"ksc_NLST__Kill_chain__list_is_disabled_due_to_oversize", "gauge", "list is disabled due to oversize"

"ksc_NLST__Kill_chain__transactions_queue_full", "gauge", "transactions queue full"

"ksc_NLST__Kill_chain__transactions_queue_near_to_full", "gauge", "transactions queue near to full"

"ksc_NLST__Kill_chain__list_is_pending", "gauge", "list is pending"

"ksc_NLST__Kill_chain__transactions_in_queue", "gauge", "transactions in queue"

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
È stato superato il limite di licenze	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Una volta al giorno Kaspersky Security Center verifica se è stato superato un limite di licenze. Gli eventi di questo tipo si verificano quando Administration Server rileva il superamento di alcune limitazioni di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client e se il numero delle unità di licensing attualmente utilizzate coperte da una singola licenza supera il 110% del numero totale di unità coperte dalla licenza. Anche quando si verifica questo evento, i dispositivi client sono protetti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare i dispositivi non in uso. • Fornire una licenza per più dispositivi (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). Kaspersky Security Center determina le regole per generare gli eventi quando viene superato un limite di licenze.	180 giorni
Epidemia di virus	26 (per Protezione minacce file)	GNRL_EV_VIRUS_OUTBREAK	Gli eventi di questo tipo si verificano quando il numero di oggetti dannosi rilevati in più dispositivi gestiti supera il limite in un periodo limitato. È possibile rispondere all'evento nei seguenti modi: • Configurare la soglia nelle proprietà di Administration Server. • Creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.	180 giorni
Epidemia di virus	27 (per Protezione minacce di posta)	GNRL_EV_VIRUS_OUTBREAK	Gli eventi di questo tipo si verificano quando il numero di oggetti dannosi rilevati in più dispositivi gestiti supera il limite in un periodo limitato. È possibile rispondere all'evento nei seguenti modi: • Configurare la soglia nelle proprietà di Administration Server. • Creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.	180 giorni
Epidemia di virus	28 (per firewall)	GNRL_EV_VIRUS_OUTBREAK	Gli eventi di questo tipo si verificano quando il numero di oggetti dannosi rilevati in più dispositivi gestiti supera il limite in un periodo limitato. È possibile rispondere all'evento nei seguenti modi: • Configurare la soglia nelle proprietà di Administration Server. • Creare un criterio più rigoroso da attivare o creare un'attività da eseguire quando si verifica l'evento.	180 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Il dispositivo è diventato non gestito	4111	KLSRV_HOST_OUT_CONTROL	Eventi di questo tipo si verificano se un dispositivo gestito è visibile nella rete ma non si connette ad Administration Server da un periodo specifico. Determinare il motivo che impedisce il corretto funzionamento di Network Agent nel dispositivo. Le cause possibili includono i problemi di rete e la rimozione di Network Agent dal dispositivo.	180 giorni
Lo stato del dispositivo è Critico	4113	KLSRV_HOST_STATUS_CRITICAL	Eventi di questo tipo si verificano quando a un dispositivo gestito viene assegnato lo stato *Critico*. È possibile configurare le condizioni in cui lo stato del dispositivo diventa *Critico*.	180 giorni
Il file chiave è stato aggiunto alla lista vietati	4124	KLSRV_LICENSE_BLACKLISTED	Eventi di questo tipo si verificano quando Kaspersky ha aggiunto il codice di attivazione o il file chiave in uso alla lista vietati. Contattare il Servizio di assistenza tecnica per ulteriori dettagli.	180 giorni
Modalità con funzionalità limitate	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Eventi di questo tipo si verificano quando Kaspersky Security Center viene avviato con funzionalità di base, senza le funzionalità Vulnerability e patch management e Mobile Device Management. Di seguito sono riportati i motivi dell'evento e le risposte appropriate: • Il periodo licenza è scaduto. Fornire una licenza per utilizzare la modalità con funzionalità complete di Kaspersky Security Center (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). • Administration Server gestisce più dispositivi rispetto a quanto previsto dalla limitazione licenza. Spostare i dispositivi dai gruppi di amministrazione di un Administration Server a quelli di un altro Administration Server (se la limitazione licenza dell'altro Administration Server lo consente).	180 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
La licenza sta per scadere	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Eventi di questo tipo si verificano quando si avvicina la data di scadenza della licenza commerciale. Una volta al giorno Kaspersky Security Center verifica se si è in prossimità della data di scadenza della licenza. Gli eventi di questo tipo vengono pubblicati 30 giorni, 15 giorni, 5 giorni e 1 giorno prima della data di scadenza della licenza. Non è possibile modificare il numero di giorni. Se Administration Server è disattivato nel giorno specificato prima della data di scadenza della licenza, l'evento non verrà pubblicato fino al giorno successivo. Alla scadenza della licenza commerciale, Kaspersky Security Center fornisce solo le funzionalità di base. È possibile rispondere all'evento nei seguenti modi: • Verificare di aver aggiunto una chiave di licenza di riserva ad Administration Server. • Se si utilizza un abbonamento, assicurarsi di rinnovarlo. L'abbonamento illimitato viene rinnovato automaticamente se il pagamento al provider di servizi è stato effettuato anticipatamente entro il termine.	180 giorni
Il certificato è scaduto	4132	KLSRV_CERTIFICATE_EXPIRED	Eventi di questo tipo si verificano quando il certificato client nei dispositivi con certificato mobile scade.	180 giorni
Il certificato di Administration Server è scaduto.	6129	ServerCertificateExpired	Eventi di questo tipo si verificano quando scadono i certificati di Administration Server per i dispositivi mobili e i dispositivi UEFI. È necessario aggiornare il certificato scaduto.	180 giorni
Gli aggiornamenti per i moduli dell'applicazione Kaspersky sono stati revocati	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Eventi di questo tipo si verificano se gli aggiornamenti immediati sono stati revocati (per questi aggiornamenti viene visualizzato lo stato *Revocato*) dagli esperti di Kaspersky perché, ad esempio, devono essere aggiornati a una versione più recente. L'evento riguarda le patch di Kaspersky Security Center e non riguarda i moduli delle applicazioni gestite di Kaspersky. L'evento indica come motivo che gli aggiornamenti immediati non sono installati.	180 giorni
Controllo: esportazione in SIEM non riuscita	5130	KLAUD_EV_SIEM_EXPORT_ERROR	Eventi di questo tipo si verificano quando l'esportazione degli eventi nel sistema SIEM non è riuscita a causa di un errore di connessione con il sistema SIEM.	180 giorni

Eventi di errore funzionale di Administration Server

La tabella seguente elenca i tipi di eventi di Kaspersky Security Center Administration Server con il livello di importanza **Errore funzionale**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di errore funzionale di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Errore di runtime	4125	KLSRV_RUNTIME_ERROR	Eventi di questo tipo si verificano a causa di problemi sconosciuti. La maggior parte delle volte si tratta di problemi DBMS, problemi di rete e altri problemi hardware e software. È possibile trovare i dettagli dell'evento nella descrizione dell'evento.	180 giorni
Limite di installazioni superato per uno dei gruppi di applicazioni concesse in licenza	4126	KLSRV_INVLICPROD_EXCEDED	Administration Server genera periodicamente eventi di questo tipo (ogni ora). Eventi di questo tipo si verificano se in Kaspersky Security Center si gestiscono chiavi di licenza di applicazioni di terze parti e se il numero di installazioni ha superato il limite impostato dalla chiave di licenza dell'applicazione di terze parti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare l'applicazione di terzi dai dispositivi in cui non è in uso l'applicazione. • Utilizzare una licenza di terzi per altri dispositivi. È possibile gestire le chiavi di licenza di applicazioni di terze parti utilizzando le funzionalità dei gruppi di applicazioni concesse in licenza. Un gruppo di applicazioni concesse in licenza include le applicazioni di terzi che soddisfano i criteri impostati dall'utente.	180 giorni
Impossibile eseguire il polling del segmento cloud	4143	KLSRV_KLCLOUD_SCAN_ERROR	Eventi di questo tipo si verificano quando Administration Server non riesce a eseguire il polling di un segmento di rete in un ambiente cloud. Leggere i dettagli nella descrizione dell'evento e rispondere di conseguenza.	Non archiviato
Impossibile copiare gli aggiornamenti nella cartella specificata	4123	KLSRV_UPD_REPL_FAIL	Eventi di questo tipo si verificano quando gli aggiornamenti software vengono copiati in una cartella condivisa aggiuntiva. È possibile rispondere all'evento nei seguenti modi: • Verificare che l'account utente utilizzato per ottenere l'accesso alla cartella disponga dell'autorizzazione di scrittura. • Verificare eventuali variazioni del nome utente e/o della password della cartella. • Verificare la connessione Internet poiché potrebbe essere la causa dell'evento. Seguire le istruzioni per l'aggiornamento dei database e dei moduli software.	180 giorni
Spazio su disco esaurito	4107	KLSRV_DISK_FULL	Eventi di questo tipo si verificano quando nel disco rigido del dispositivo in cui è installato Administration Server si esaurisce lo spazio disponibile. Liberare spazio su disco nel dispositivo.	180 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
La cartella condivisa non è disponibile	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Eventi di questo tipo si verificano se la cartella condivisa di Administration Server non è disponibile. È possibile rispondere all'evento nei seguenti modi: • Verificare che Administration Server (dove si trova la cartella condivisa) sia attivato e disponibile. • Verificare eventuali variazioni del nome utente e/o della password della cartella. • Verificare la connessione di rete.	180 giorni
Database di Administration Server non disponibile	4109	KLSRV_DATABASE_UNAVAILABLE	Eventi di questo tipo si verificano se il database di Administration Server diventa non disponibile. È possibile rispondere all'evento nei seguenti modi: • Verificare se è disponibile il server remoto in cui è installato SQL Server. • Visualizzare i log DBMS per scoprire il motivo della mancata disponibilità di Administration Server. A causa della manutenzione preventiva, un server remoto in cui è installato SQL Server potrebbe ad esempio non essere disponibile.	180 giorni
Spazio disponibile esaurito nel database di Administration Server	4110	KLSRV_DATABASE_FULL	Eventi di questo tipo si verificano quando non è disponibile spazio nel database di Administration Server. Administration Server non funziona quando il database ha raggiunto la capacità massima e non è possibile eseguire ulteriori registrazioni nel database. Di seguito sono riportate le cause di questo evento, a seconda del DBMS in uso, e le risposte appropriate all'evento: • Si utilizza il DBMS SQL Server Express Edition: Nella documentazione di SQL Server Express esaminare il limite relativo alle dimensioni del database per la versione utilizzata. È probabile che il database di Administration Server abbia superato il limite relativo alle dimensioni del database. Limitare il numero di eventi da archiviare nel database di Administration Server. Nel database di Administration Server sono presenti troppi eventi inviati dal componente Controllo Applicazioni. È possibile modificare le impostazioni del criterio di Kaspersky Endpoint Security for Windows relative all'archiviazione degli eventi di Controllo Applicazioni nel database di Administration Server. • Si utilizza un DBMS diverso da SQL Server Express Edition: Non limitare il numero di eventi da archiviare nel database di Administration Server. Ridurre l'elenco degli eventi da archiviare nel database di Administration Server. Rivedere le informazioni sulla selezione DBMS.	180 giorni

Eventi di avviso di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Administration Server con il livello di importanza **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
È stato rilevato un evento frequente		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Eventi di questo tipo si verificano quando Administration Server rileva un evento frequente in un dispositivo gestito. Per ulteriori dettagli, consultare la sezione seguente: Blocco degli eventi frequenti.	90 giorni
È stato superato il limite di licenze	4098	KLSRV_EV_LICENSE_CHECK_100_110	Una volta al giorno Kaspersky Security Center verifica se è stato superato un limite di licenze. Gli eventi di questo tipo si verificano quando Administration Server rileva il superamento di alcune limitazioni di licenza da parte delle applicazioni Kaspersky installate nei dispositivi client e se il numero delle unità di licensing attualmente utilizzate coperte da una singola licenza costituisce dal 100% al 110% del numero totale di unità coperte dalla licenza. Anche quando si verifica questo evento, i dispositivi client sono protetti. È possibile rispondere all'evento nei seguenti modi: • Esaminare l'elenco dei dispositivi gestiti. Eliminare i dispositivi non in uso. • Fornire una licenza per più dispositivi (aggiungere un codice di attivazione valido o un file chiave ad Administration Server). Kaspersky Security Center determina le regole per generare gli eventi quando viene superato un limite di licenze.	90 giorni
Il dispositivo è rimasto inattivo nella rete per molto tempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Eventi di questo tipo si verificano quando un dispositivo gestito risulta inattivo per un determinato periodo di tempo. Molto spesso ciò accade quando un dispositivo gestito viene disattivato. È possibile rispondere all'evento nei seguenti modi: • Rimuovere manualmente il dispositivo dall'elenco dei dispositivi gestiti. • Specificare l'intervallo di tempo dopo il quale viene creato l'evento **Il dispositivo è rimasto inattivo nella rete per molto tempo** utilizzando Administration Console o Kaspersky Security Center Web Console. • Specificare l'intervallo di tempo dopo il quale il dispositivo viene automaticamente rimosso dal gruppo utilizzando Administration Console o utilizzando Kaspersky Security Center Web Console.	90 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Conflitto dei nomi di dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Eventi di questo tipo si verificano quando Administration Server considera due o più dispositivi gestiti come un unico dispositivo. Molto spesso questo accade quando un disco rigido clonato è stato utilizzato per la distribuzione del software nei dispositivi gestiti e senza eseguire il passaggio di Network Agent alla modalità di clonazione del disco dedicata in un dispositivo di riferimento. Per evitare questo problema, eseguire il passaggio di Network Agent alla modalità di clonazione del disco in un dispositivo di riferimento prima di clonare il disco rigido di questo dispositivo.	90 giorni
Lo stato del dispositivo è Avviso	4114	KLSRV_HOST_STATUS_WARNING	Eventi di questo tipo si verificano quando a un dispositivo gestito viene assegnato lo stato *Avviso*. È possibile configurare le condizioni in cui lo stato del dispositivo diventa *Avviso*.	90 giorni
Il limite di installazioni sta per essere superato per uno dei gruppi di applicazioni concesse in licenza	4127	KLSRV_INVLICPROD_FILLED	Eventi di questo tipo si verificano quando il numero di installazioni per applicazioni di terze parti incluse in un gruppo di applicazioni concesse in licenza raggiunge il 90% del valore massimo consentito specificato nelle proprietà della chiave di licenza. È possibile rispondere all'evento nei seguenti modi: • Se l'applicazione di terzi non è in uso in alcuni dei dispositivi gestiti, eliminare l'applicazione da questi dispositivi. • Se si prevede che il numero di installazioni per l'applicazione di terzi supererà il valore massimo consentito nell'immediato futuro, valutare la possibilità di ottenere in anticipo una licenza di terzi per un numero superiore di dispositivi. È possibile gestire le chiavi di licenza di applicazioni di terze parti utilizzando le funzionalità dei gruppi di applicazioni concesse in licenza.	90 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Il certificato è stato richiesto	4133	KLSRV_CERTIFICATE_REQUESTED	Eventi di questo tipo si verificano quando un certificato per Mobile Device Management non viene riemesso automaticamente. Di seguito sono elencate le possibili cause e le risposte appropriate all'evento: • È stata avviata la riemissione automatica per un certificato per il quale l'opzione **Riemetti automaticamente il certificato se possibile** è disabilitata. Ciò potrebbe essere dovuto a un errore che si è verificato durante la creazione del certificato. Potrebbe essere necessaria la riemissione manuale del certificato. • Se si utilizza un'integrazione con un'infrastruttura a chiave pubblica, la causa potrebbe essere un attributo SAM-Account-Name mancante dell'account utilizzato per l'integrazione con PKI e per l'emissione del certificato. Esaminare le proprietà dell'account.	90 giorni
Il certificato è stato rimosso	4134	KLSRV_CERTIFICATE_REMOVED	Eventi di questo tipo si verificano quando un amministratore rimuove qualsiasi tipo di certificato (generale, posta, VPN) per Mobile Device Management. Dopo aver rimosso un certificato, i dispositivi mobili connessi tramite questo certificato non riusciranno a connettersi ad Administration Server. Questo evento potrebbe essere utile quando si esaminano malfunzionamenti associati alla gestione dei dispositivi mobili.	90 giorni
Il certificato sta per scadere	6128	ServerCertificateExpiresSoon	Eventi di questo tipo si verificano quando scadono i certificati di Administration Server per i dispositivi mobili e i dispositivi UEFI. È necessario aggiornare il certificato scaduto.	90 giorni
Il certificato APNs è scaduto	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Eventi di questo tipo si verificano allo scadere di un certificato APNs. È necessario rinnovare manualmente il certificato APNs e installarlo in un server per dispositivi mobili MDM iOS.	Non archiviato
Il certificato APNs sta per scadere	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Eventi di questo tipo si verificano quando mancano meno di 14 giorni allo scadere del certificato APNs. Allo scadere del certificato APNs, è necessario rinnovare manualmente il certificato APNs e installarlo in un server per dispositivi mobili MDM iOS. È consigliabile pianificare il rinnovo del certificato APNs prima della data di scadenza.	Non archiviato

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Impossibile inviare il messaggio FCM al dispositivo mobile	4138	KLSRV_GCM_DEVICE_ERROR	Eventi di questo tipo si verificano quando Mobile Device Management è configurato per l'utilizzo di Firebase Cloud Messaging (FCM) per la connessione a dispositivi mobili gestiti con un sistema operativo Android e FCM Server non riesce a gestire alcune delle richieste ricevute da Administration Server. Questo vuol dire che alcuni dei dispositivi mobili gestiti non riceveranno una notifica push. Leggere il codice HTTP nei dettagli della descrizione dell'evento e rispondere di conseguenza. Per ulteriori informazioni sui codici HTTP ricevuti da FCM Server e sugli errori correlati, fare riferimento alla documentazione del servizio Firebase (vedere il capitolo "Codici di risposta dell'errore dei messaggi downstream").	90 giorni
Errore HTTP durante l'invio del messaggio FCM al server FCM	4139	KLSRV_GCM_HTTP_ERROR	Eventi di questo tipo si verificano quando Mobile Device Management è configurato per l'utilizzo di Firebase Cloud Messaging (FCM) per la connessione dei dispositivi mobili gestiti con il sistema operativo Android e FCM Server ripristina in Administration Server una richiesta con un codice HTTP diverso da 200 (OK). Di seguito sono elencate le possibili cause e le risposte appropriate all'evento: • Problemi sul lato server FCM. Leggere il codice HTTP nei dettagli della descrizione dell'evento e rispondere di conseguenza. Per ulteriori informazioni sui codici HTTP ricevuti da FCM Server e sugli errori correlati, fare riferimento alla documentazione del servizio Firebase (vedere il capitolo "Codici di risposta dell'errore dei messaggi downstream"). • Problemi sul lato server proxy (se si utilizza un server proxy). Leggere il codice HTTP nei dettagli della descrizione dell'evento e rispondere di conseguenza.	90 giorni
Impossibile inviare il messaggio FCM al server FCM	4140	KLSRV_GCM_GENERAL_ERROR	Eventi di questo tipo si verificano a causa di errori imprevisti sul lato Administration Server quando si utilizza il protocollo HTTP di Firebase Cloud Messaging. Leggere i dettagli nella descrizione dell'evento e rispondere di conseguenza. Se non si riesce a trovare autonomamente la soluzione a un problema, è consigliabile contattare il Servizio di assistenza tecnica Kaspersky.	90 giorni
Poco spazio libero nel disco rigido	4105	KLSRV_NO_SPACE_ON_VOLUMES	Eventi di questo tipo si verificano quando nel disco rigido del dispositivo in cui è installato Administration Server si esaurisce quasi totalmente lo spazio disponibile. Liberare spazio su disco nel dispositivo.	90 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Spazio libero insufficiente nel database di Administration Server	4106	KLSRV_NO_SPACE_IN_DATABASE	Eventi di questo tipo si verificano se lo spazio in Administration Server è troppo limitato. Se non si ovvierà alla situazione, il database di Administration Server raggiungerà in breve tempo la capacità massima e Administration Server non funzionerà. Di seguito sono riportate le cause di questo evento, a seconda del DBMS in uso, e le risposte appropriate all'evento. Si utilizza il DBMS SQL Server Express Edition: • Nella documentazione di SQL Server Express esaminare il limite relativo alle dimensioni del database per la versione utilizzata. È probabile che il database di Administration Server stia per raggiungere il limite relativo alle dimensioni del database. • Limitare il numero di eventi da archiviare nel database di Administration Server. • Nel database di Administration Server sono presenti troppi eventi inviati dal componente Controllo Applicazioni. È possibile modificare le impostazioni del criterio di Kaspersky Endpoint Security for Windows relative all'archiviazione degli eventi di Controllo Applicazioni nel database di Administration Server. Si utilizza un DBMS diverso da SQL Server Express Edition: • Non limitare il numero di eventi da archiviare nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server Rivedere le informazioni sulla selezione DBMS.	90 giorni
La connessione all'Administration Server secondario è stata interrotta	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Eventi di questo tipo si verificano quando una connessione all'Administration Server secondario viene interrotta. Leggere il registro eventi Kaspersky nel dispositivo in cui è installato l'Administration Server secondario e rispondere di conseguenza.	90 giorni
La connessione all'Administration Server primario è stata interrotta	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Eventi di questo tipo si verificano quando una connessione all'Administration Server primario viene interrotta. Leggere il registro eventi Kaspersky nel dispositivo in cui è installato l'Administration Server primario e rispondere di conseguenza.	90 giorni
Sono stati registrati nuovi aggiornamenti per i moduli dell'applicazione Kaspersky	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Eventi di questo tipo si verificano quando Administration Server registra nuovi aggiornamenti per il software Kaspersky installato nei dispositivi gestiti la cui installazione richiede l'approvazione. Approvare o rifiutare gli aggiornamenti utilizzando Administration Console o Kaspersky Security Center Web Console.	90 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Poiché è stato superato il limite relativo al numero di eventi nel database, è stata avviata l'eliminazione degli eventi	4145	KLSRV_EVP_DB_TRUNCATING	Eventi di questo tipo si verificano quando viene avviata l'eliminazione degli eventi precedenti dal database di Administration Server dopo il raggiungimento della capacità massima del database di Administration Server. È possibile rispondere all'evento nei seguenti modi: • Cambiare il numero massimo di eventi archiviati nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server	Non archiviato
Poiché è stato superato il limite relativo al numero di eventi nel database, gli eventi sono stati eliminati	4146	KLSRV_EVP_DB_TRUNCATED	Eventi di questo tipo si verificano dopo l'eliminazione degli eventi precedenti dal database di Administration Server in seguito al raggiungimento della capacità massima del database di Administration Server. È possibile rispondere all'evento nei seguenti modi: • Cambiare il numero massimo consentito di eventi archiviati nel database di Administration Server • Ridurre l'elenco degli eventi da archiviare nel database di Administration Server	Non archiviato
Controllo (test della connessione al server SIEM non riuscito)	5120	KLAUD_EV_SIEM_TEST_FAILED	Eventi di questo tipo si verificano quando una connessione di test al server SIEM non riesce.	30 giorni
Impossibile emettere il certificato automaticamente		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Questo evento si verifica in caso di errore durante la creazione di un certificato client per un dispositivo mobile (un dispositivo eseguito con un protocollo mobile).	90 giorni

Eventi informativi di Administration Server

La tabella seguente elenca gli eventi di Kaspersky Security Center Administration Server con il livello di importanza **Informazioni**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare e configurare l'elenco degli eventi nelle proprietà dell'Administration Server. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi informativi di Administration Server

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito	Osservazioni
Utilizzo della chiave di licenza superiore al 90%	4097	KLSRV_EV_LICENSE_CHECK_90	30 giorni	
Nuovo dispositivo rilevato	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 giorni	
Il dispositivo è stato aggiunto automaticamente al gruppo	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 giorni	

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito	Osservazioni
Il dispositivo è stato spostato automaticamente in base a una regola	1074	KLSRV_HOST_MOVED_WITH_RULE_EX	30 giorni	
Il dispositivo è stato rimosso dal gruppo poiché inattivo nella rete per molto tempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 giorni	
Sta per essere superato il limite di installazioni (è stato utilizzato più del 95%) per uno dei gruppi di applicazioni concesse in licenza	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 giorni	
Sono disponibili alcuni file da inviare a Kaspersky per l'analisi	4131	KLSRV_APS_FILE_APPEARED	30 giorni	
L'ID istanza FCM è stato modificato in questo dispositivo mobile	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 giorni	
Aggiornamenti copiati nella cartella specificata	4122	KLSRV_UPD_REPL_OK	30 giorni	
La connessione all'Administration Server secondario è stata stabilita	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 giorni	
La connessione all'Administration Server primario è stata stabilita	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 giorni	
I database sono stati aggiornati	4144	KLSRV_UPD_BASES_UPDATED	30 giorni	
Controllo: la connessione ad Administration Server è stata stabilita	4147	KLAUD_EV_SERVERCONNECT	30 giorni	Eventi di questo tipo si verificano quando un utente si connette ad Administration Server tramite Administration Console o Kaspersky Security Center Web Console. Questi eventi includono informazioni sull'indirizzo IP del dispositivo in cui è installata l'Administration Console basata su MMC o Kaspersky Security Center Web Console Server.
Controllo: l'oggetto è stato modificato	4148	KLAUD_EV_OBJECTMODIFY	30 giorni	Questo evento monitora le modifiche nei seguenti oggetti: • Gruppo di amministrazione • Gruppo di protezione • Utente • Pacchetto • Attività • Criterio • Server • Server virtuale
Controllo: lo stato dell'oggetto è stato modificato	4150	KLAUD_EV_TASK_STATE_CHANGED	30 giorni	Ad esempio, questo evento si verifica quando un'attività non è riuscita con un errore.

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito	Osservazioni
Controllo: le impostazioni del gruppo sono state modificate	4149	KLAUD_EV_ADMGROUP_CHANGED	30 giorni	
Controllo: la connessione ad Administration Server è stata terminata	4151	KLAUD_EV_SERVERDISCONNECT	30 giorni	
Controllo: le proprietà dell'oggetto sono state modificate	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 giorni	Questo evento monitora le modifiche nelle seguenti proprietà: • Utente • Licenza • Server • Server virtuale
Controllo: le autorizzazioni dell'utente sono state modificate	4153	KLAUD_EV_OBJECTACLMODIFIED	30 giorni	
Controllo: le chiavi di criptaggio sono state importate o esportate da Administration Server	5100	KLAUD_EV_DPEKEYSEXPORT	30 giorni	
Controllo: test della connessione al server SIEM riuscito	5110	KLAUD_EV_SIEM_TEST_SUCCESS	30 giorni	Questo evento si verifica quando una connessione di test al server SIEM riesce.
Certificato di riserva creato		ServerReserveCertificateCreated	30 giorni	Questo evento si verifica quando è stato creato un certificato di Administration Server.
Certificato in rinnovo		ServerCertificateRenewed	30 giorni	Questo evento si verifica quando il certificato di Administration Server è stato rinnovato.

Gli eventi **Certificato di riserva creato** e **Certificato in rinnovo** vengono pubblicati automaticamente da Administration Server e visualizzati in Administration Console solo quando le operazioni corrispondenti a questi eventi vengono eseguite per i certificati di Administration Server per i dispositivi mobili e i dispositivi UEFI.

Eventi di Network Agent

Questa sezione contiene informazioni sugli eventi relativi a Network Agent.

Eventi di errore funzionale di Network Agent

La tabella seguente elenca i tipi di eventi di Kaspersky Security Center Network Agent con il livello di criticità **Errore funzionale**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di errore funzionale di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Descrizione	Periodo di archiviazione predefinito
Errore durante l'installazione dell'aggiornamento	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Gli eventi di questo tipo si verificano se l'installazione automatica di aggiornamenti e patch per i componenti Kaspersky Security Center non è andata a buon fine. L'evento non riguarda gli aggiornamenti delle applicazioni gestite Kaspersky. Leggere la descrizione dell'evento. Un problema di Windows in Administration Server potrebbe essere la causa dell'evento. Se nella descrizione vengono menzionati problemi relativi alla configurazione di Windows, risolvere il problema.	30 giorni
Impossibile installare l'aggiornamento software di terze parti	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Gli eventi di questo tipo si verificano se sono in uso le funzionalità Vulnerability e patch management e Mobile Device Management e se l'aggiornamento del software di terze parti non è andato a buon fine. Verificare che il collegamento al software di terze parti sia valido. Leggere la descrizione dell'evento.	30 giorni
Impossibile installare gli aggiornamenti di Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Gli eventi di questo tipo si verificano se gli aggiornamenti di Windows non sono andati a buon fine. Configurare gli aggiornamenti di Windows in un criterio di Network Agent. Leggere la descrizione dell'evento. Cercare l'errore nella Microsoft Knowledge Base. Contattare il supporto tecnico Microsoft se non si riesce a risolvere autonomamente il problema.	30 giorni
Gestione degli utenti: errori	7723	KLNAG_EV_USR_MNG_ERR	Evento di avviso generale.	30 giorni
Impossibile ripristinare il valore di riferimento del file Sudoers	7726	KLNAG_EV_SUDOER_RESTORED_ERR	L'evento contiene la descrizione dell'errore di sostituzione del file sudoers.	30 giorni
Impossibile installare i certificati radice	7728	KLNAG_EV_ROOT_CERT_INSTALL_ERR	L'evento contiene la descrizione dell'errore di installazione dei certificati.	30 giorni
Impossibile rimuovere i certificati radice	7730	KLNAG_EV_ROOT_CERT_REMOVE_ERR	L'evento contiene la descrizione dell'errore di rimozione dei certificati.	30 giorni

Eventi di avviso di Network Agent

La tabella seguente elenca gli eventi di Kaspersky Security Center Network Agent con il livello di gravità **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
È stato restituito un avviso durante l'installazione dell'aggiornamento dei moduli software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 giorni
Installazione dell'aggiornamento software di terze parti completata con un avviso	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 giorni
Installazione dell'aggiornamento software di terze parti rimandata	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 giorni

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Si è verificato un problema di sicurezza	549	GNRL_EV_APP_INCIDENT_OCCURED	30 giorni
Proxy KSN avviato. Impossibile verificare la disponibilità di KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 giorni
Gestione degli utenti: avvisi	7722	KLNAG_EV_USR_MNG_WRN	30 giorni
Trovato file Sudoers che non corrisponde al valore di riferimento	7724	KLNAG_EV_SUDOER_DIFFERENT	30 giorni

Eventi informativi di Network Agent

La tabella seguente elenca gli eventi di Kaspersky Security Center Network Agent con il livello di gravità **Informazioni**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi informativi di Network Agent

Nome visualizzato del tipo di evento	ID del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Installazione dell'aggiornamento per i moduli software completata	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 giorni
Installazione dell'aggiornamento dei moduli software avviata	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 giorni
Applicazione installata	7703	KLNAG_EV_INV_APP_INSTALLED	30 giorni
Applicazione rimossa	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 giorni
Applicazione monitorata installata	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 giorni
Applicazione monitorata rimossa	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 giorni
Applicazione di terze parti installata	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 giorni
Nuovo dispositivo aggiunto	7708	KLNAG_EV_DEVICE_ARRIVAL	30 giorni
Dispositivo rimosso	7709	KLNAG_EV_DEVICE_REMOVE	30 giorni
Nuovo dispositivo rilevato	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 giorni
Dispositivo autorizzato	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 giorni
Condivisione desktop Windows: file letto	7712	KLUSRLOG_EV_FILE_READ	30 giorni
Condivisione desktop Windows: file modificato	7713	KLUSRLOG_EV_FILE_MODIFIED	30 giorni
Condivisione desktop Windows: applicazione avviata	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 giorni
Condivisione desktop Windows: avviata	7715	KLUSRLOG_EV_WDS_BEGIN	30 giorni
Condivisione desktop Windows: arrestata	7716	KLUSRLOG_EV_WDS_END	30 giorni
Installazione dell'aggiornamento software di terze parti completata	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 giorni
Installazione dell'aggiornamento software di terze parti avviata	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 giorni
Proxy KSN avviato. La verifica della disponibilità di KSN è stata completata	7719	KSNPROXY_STARTED_CON_CHK_OK	30 giorni
Proxy KSN arrestato	7720	KSNPROXY_STOPPED	30 giorni

Eventi di Server per dispositivi mobili MDM iOS

Questa sezione contiene informazioni sugli eventi relativi al server MDM iOS.

Eventi di errore funzionale di Server per dispositivi mobili MDM iOS

La tabella seguente elenca gli eventi del server per dispositivi mobili MDM iOS di Kaspersky Security Center con il livello di criticità **Errore funzionale**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di errore funzionale di Server per dispositivi mobili MDM iOS

Nome visualizzato del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Impossibile richiedere l'elenco dei profili	PROFILELIST_COMMAND_FAILED	30 giorni
Impossibile installare il profilo	INSTALLPROFILE_COMMAND_FAILED	30 giorni
Impossibile rimuovere il profilo	REMOVEPROFILE_COMMAND_FAILED	30 giorni
Impossibile richiedere l'elenco dei profili di provisioning	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 giorni
Impossibile installare il profilo di provisioning	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 giorni
Impossibile eliminare il profilo di provisioning	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 giorni
Impossibile richiedere l'elenco dei certificati digitali	CERTIFICATELIST_COMMAND_FAILED	30 giorni
Impossibile richiedere l'elenco di applicazioni installate	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 giorni
Impossibile richiedere le informazioni generali sul dispositivo mobile	DEVICEINFORMATION_COMMAND_FAILED	30 giorni
Impossibile richiedere le informazioni di protezione	SECURITYINFO_COMMAND_FAILED	30 giorni
Impossibile bloccare il dispositivo mobile	DEVICELOCK_COMMAND_FAILED	30 giorni
Impossibile reimpostare la password	CLEARPASSCODE_COMMAND_FAILED	30 giorni
Impossibile cancellare i dati dal dispositivo mobile	ERASEDEVICE_COMMAND_FAILED	30 giorni
Impossibile installare l'app	INSTALLAPPLICATION_COMMAND_FAILED	30 giorni
Impossibile impostare il codice di riscatto per l'app	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 giorni
Impossibile richiedere l'elenco delle app gestite	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 giorni
Impossibile rimuovere l'app gestita	REMOVEAPPLICATION_COMMAND_FAILED	30 giorni
Impostazioni roaming rifiutate	SETROAMINGSETTINGS_COMMAND_FAILED	30 giorni
Si è verificato un errore durante l'esecuzione dell'app	PRODUCT_FAILURE	30 giorni
Il risultato del comando contiene dati non validi	MALFORMED_COMMAND	30 giorni
Impossibile inviare la notifica push	SEND_PUSH_NOTIFICATION_FAILED	30 giorni
Impossibile inviare il comando	SEND_COMMAND_FAILED	30 giorni
Dispositivo non trovato	DEVICE_NOT_FOUND	30 giorni

Eventi di avviso di Server per dispositivi mobili MDM iOS

La tabella seguente elenca gli eventi di Server per dispositivi mobili MDM iOS di Kaspersky Security Center con il livello di gravità **Avviso**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi di avviso di Server per dispositivi mobili MDM iOS

Nome visualizzato del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
È stato rilevato un tentativo di connessione di un dispositivo mobile	INACTICE_DEVICE_TRY_CONNECTED	30 giorni
Il profilo è stato rimosso	MDM_PROFILE_WAS_REMOVED	30 giorni
Tentativo di utilizzare un certificato client già in uso	CLIENT_CERT_ALREADY_IN_USE	30 giorni
È stato rilevato un dispositivo inattivo	FOUND_INACTIVE_DEVICE	30 giorni
È necessario il codice di riscatto	NEED_REDEMPTION_CODE	30 giorni
Profilo incluso in un criterio rimosso dal dispositivo	UMDM_PROFILE_WAS_REMOVED	30 giorni

Eventi informativi di Server per dispositivi mobili MDM iOS

La tabella seguente elenca gli eventi di Server per dispositivi mobili MDM iOS di Kaspersky Security Center con il livello di gravità **Informazioni**.

Per ogni evento che può essere generato da un'applicazione, è possibile specificare le impostazioni di notifica e le impostazioni di archiviazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Se si desidera configurare le impostazioni di notifica per tutti gli eventi contemporaneamente, configurare le impostazioni di notifica generali nelle proprietà di Administration Server.

Eventi informativi di Server per dispositivi mobili MDM iOS

Nome visualizzato del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Un nuovo dispositivo mobile è stato connesso	NEW_DEVICE_CONNECTED	30 giorni
L'elenco dei profili è stato richiesto	PROFILELIST_COMMAND_SUCCESSFULL	30 giorni
Il profilo è stato installato	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 giorni
Il profilo è stato rimosso	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 giorni
L'elenco dei profili di provisioning è stato richiesto	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 giorni
L'installazione del profilo di provisioning è stata completata	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 giorni
La rimozione del profilo di provisioning è stata completata	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 giorni
L'elenco dei certificati digitali è stato richiesto	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 giorni
L'elenco delle applicazioni installate è stato richiesto	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 giorni
Informazioni generali sul dispositivo mobile richieste	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 giorni
Le informazioni di protezione sono state richieste	SECURITYINFO_COMMAND_SUCCESSFULL	30 giorni
Il dispositivo mobile è stato bloccato	DEVICELOCK_COMMAND_SUCCESSFULL	30 giorni
La password è stata reimpostata	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 giorni
I dati sono stati cancellati dal dispositivo mobile	ERASEDEVICE_COMMAND_SUCCESSFULL	30 giorni
L'applicazione è stata installata	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 giorni

Nome visualizzato del tipo di evento	Tipo di evento	Periodo di archiviazione predefinito
Il codice di riscatto è stato impostato per l'app	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 giorni
L'elenco delle app gestite è stato richiesto	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 giorni
L'app gestita è stata rimossa	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 giorni
Impostazioni roaming applicate	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 giorni

Blocco degli eventi frequenti

Questa sezione fornisce informazioni sulla gestione del blocco degli eventi frequenti e sulla rimozione del blocco degli eventi frequenti.

Informazioni sul blocco degli eventi frequenti

Un'applicazione gestita, ad esempio Kaspersky Endpoint Security for Windows, installata in uno o più dispositivi gestiti può inviare molti eventi dello stesso tipo ad Administration Server. La ricezione di eventi frequenti può sovraccaricare il database di Administration Server e sovrascrivere altri eventi. Administration Server inizia a bloccare gli eventi più frequenti quando il numero di tutti gli eventi ricevuti supera il limite specificato per il database.

Administration Server blocca la ricezione automatica degli eventi frequenti. Non è possibile bloccare autonomamente gli eventi frequenti o scegliere quali eventi bloccare.

Se si desidera scoprire se un evento è bloccato, è possibile visualizzare l'elenco delle notifiche o controllare se questo evento è presente nella sezione **Blocco degli eventi frequenti** delle proprietà di Administration Server. Se l'evento è bloccato, è possibile eseguire le seguenti operazioni:

- Se si desidera impedire la sovrascrittura del database, è possibile continuare a bloccare la ricezione di questo tipo di eventi.
- Se ad esempio si desidera individuare il motivo dell'invio degli eventi frequenti ad Administration Server, è possibile sbloccare gli eventi frequenti e continuare a ricevere comunque gli eventi di questo tipo.
- Se si desidera continuare a ricevere gli eventi frequenti finché non vengono nuovamente bloccati, è possibile rimuovere dal blocco gli eventi frequenti.

Gestione del blocco degli eventi frequenti

Administration Server blocca la ricezione automatica degli eventi frequenti, ma è possibile sbloccare e continuare a ricevere gli eventi frequenti. È inoltre possibile bloccare la ricezione degli eventi frequenti sbloccati in precedenza.

Per gestire il blocco degli eventi frequenti:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Blocco degli eventi frequenti**.

3. Nella sezione **Blocco degli eventi frequenti**:

   - Se si desidera sbloccare la ricezione degli eventi frequenti:

     a. Selezionare gli eventi frequenti che si desidera sbloccare e fare clic sul pulsante **Escludi**.

     b. Fare clic sul pulsante **Salva**.

   - Se si desidera bloccare la ricezione degli eventi frequenti:

     a. Selezionare gli eventi frequenti che si desidera bloccare e fare clic sul pulsante **Blocca**.

     b. Fare clic sul pulsante **Salva**.

Administration Server riceve gli eventi frequenti sbloccati e non riceve gli eventi frequenti bloccati.

Rimozione del blocco degli eventi frequenti

È possibile rimuovere il blocco per gli eventi frequenti e iniziare a riceverli fino a quando Administration Server bloccherà nuovamente questi eventi frequenti.

Per rimuovere il blocco per gli eventi frequenti:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Blocco degli eventi frequenti**.

3. Nella sezione **Blocco degli eventi frequenti** selezionare i tipi di eventi frequenti per i quali si desidera rimuovere il blocco.

4. Fare clic sul pulsante **Rimuovi dal blocco**.

L'evento frequente viene rimosso dall'elenco degli eventi frequenti. Administration Server riceverà gli eventi di questo tipo.

Ricezione di eventi da Kaspersky Security for Microsoft Exchange Servers

Le informazioni relative agli eventi durante il funzionamento delle applicazioni gestite, come Kaspersky Endpoint Security for Windows, vengono trasferite dai dispositivi gestiti e registrate nel database di Administration Server. Per impostazione predefinita, gli eventi di Kaspersky Security for Microsoft Exchange Servers versione 9.0 MR6 e precedenti non vengono registrati nel database di Administration Server. Se Kaspersky Security for Microsoft Exchange Servers versione 9.0 MR6 e precedenti è installato nei dispositivi gestiti dell'organizzazione e si desidera ricevere gli eventi da questa applicazione, abilitare la registrazione degli eventi per questa applicazione utilizzando l'utilità klscflag.

Per abilitare la registrazione degli eventi per Kaspersky Security for Microsoft Exchange Servers:

1. Nel dispositivo Administration Server eseguire il prompt dei comandi di Windows con un account che disponga dei diritti di amministratore.

2. Sostituire la directory corrente con la cartella di installazione di Kaspersky Security Center (in genere, C:\Programmi (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Eseguire uno dei seguenti comandi:

   - Per l'Administration Server installato in un cluster di failover di Windows Server

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Per l'Administration Server installato in un nodo del cluster di failover Kaspersky Security Center:

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Per l'Administration Server che non funziona su un cluster:

     ```
     klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
     -v 0
     ```

   La registrazione degli eventi per Kaspersky Security for Microsoft Exchange Servers è abilitata:

Per Kaspersky Security for Microsoft Exchange Servers non è possibile impostare il periodo di archiviazione per gli eventi o selezionare gli eventi da salvare nell'archivio dell'Administration Server. È possibile impostare il numero massimo di eventi che possono essere salvati nell'archivio. Questa impostazione viene applicata agli eventi ricevuti da tutte le applicazioni Kaspersky.

Notifiche e stati del dispositivo

Questa sezione contiene informazioni su come visualizzare le notifiche, configurare il recapito delle notifiche, utilizzare gli stati dei dispositivi e abilitare la modifica degli stati dei dispositivi.

Utilizzo delle notifiche

Le notifiche segnalano gli eventi e consentono di velocizzare le risposte a tali eventi eseguendo le azioni consigliate o le azioni che si ritengono appropriate.

A seconda del metodo di notifica scelto, sono disponibili i seguenti tipi di notifiche:

- Notifiche sullo schermo
- Notifiche tramite SMS
- Notifiche tramite e-mail
- Notifiche tramite file eseguibile o script

Notifiche sullo schermo

Le notifiche sullo schermo segnalano gli eventi raggruppati per livelli di importanza (*Critico*, *Avviso* e *Informativo*).

Una notifica sullo schermo può avere due stati:

- *Rivista*. Indica che è stata eseguita l'azione consigliata per la notifica o che è stato assegnato manualmente questo stato per la notifica.
- *Non rivista*. Indica che non è stata eseguita l'azione consigliata per la notifica o che non è stato assegnato manualmente questo stato per la notifica.

Per impostazione predefinita, l'elenco delle notifiche include le notifiche con lo stato *Non rivista*.

È possibile monitorare la rete dell'organizzazione visualizzando le notifiche sullo schermo e rispondendo in tempo reale a tali notifiche.

Notifiche tramite e-mail, SMS e file eseguibile o script

Kaspersky Security Center offre la possibilità di monitorare la rete dell'organizzazione inviando notifiche su qualsiasi evento che si ritiene importante. Per ogni evento è possibile configurare notifiche tramite e-mail, tramite SMS o avviando un file eseguibile o uno script.

Dopo aver ricevuto notifiche tramite e-mail o SMS, è possibile decidere la risposta a un evento. Questa risposta dovrebbe essere la più appropriata per la rete dell'organizzazione. Avviando un file eseguibile o uno script, si specifica una risposta predefinita a un evento. L'avvio di un file eseguibile o di uno script può anche essere considerato la risposta primaria a un evento. Dopo l'avvio del file eseguibile, è possibile eseguire altri passaggi per rispondere all'evento.

Visualizzazione delle notifiche sullo schermo

È possibile visualizzare le notifiche sullo schermo in tre modi:

- Nella sezione **Monitoraggio e generazione dei rapporti** → **Notifiche**. Qui è possibile visualizzare le notifiche relative alle categorie predefinite.
- In una finestra distinta che può essere aperta indipendentemente dalla sezione in uso. In questo caso, è possibile contrassegnare le notifiche come riviste.
- Nel widget **Notifiche in base al livello di criticità selezionato** nella sezione **Monitoraggio e generazione dei rapporti** → **Dashboard**. Nel widget è possibile visualizzare solo le notifiche degli eventi con i livelli di importanza *Critico* e *Avviso*.

È possibile eseguire azioni, ad esempio è possibile rispondere a un evento.

Per visualizzare le notifiche delle categorie predefinite:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Notifiche**.

   La categoria **Tutte le notifiche** è selezionata nel riquadro sinistro e nel riquadro destro sono visualizzate tutte le notifiche.

2. Nel riquadro sinistro selezionare una delle categorie:

   - **Distribuzione**
   - **Dispositivi**
   - **Protezione**
   - **Aggiornamenti** (sono incluse le notifiche relative alle applicazioni Kaspersky disponibili per il download e le notifiche relative agli aggiornamenti dei database anti-virus scaricati)
   - **Prevenzione Exploit**
   - **Administration Server** (sono inclusi gli eventi relativi solo ad Administration Server)
   - **Collegamenti utili** (sono inclusi collegamenti a risorse Kaspersky, ad esempio il Servizio di assistenza tecnica Kaspersky, il forum Kaspersky, la pagina di rinnovo della licenza o Kaspersky IT Encyclopedia)

Viene visualizzato un elenco di notifiche della categoria selezionata. L'elenco contiene i seguenti elementi:

- Icona relativa all'argomento della notifica: distribuzione (), protezione (), aggiornamenti (), gestione dispositivi (), Prevenzione Exploit (), Administration Server ().
- Livello di importanza della notifica. Vengono visualizzate le notifiche con i seguenti livelli di importanza: **Notifiche critiche** (), **Notifiche di avviso** (), **Notifiche informative**. Le notifiche nell'elenco sono raggruppate in base ai livelli di importanza.
- **Notifica**. Contiene una descrizione della notifica.

- **Azione**. Contiene un collegamento a un'azione rapida che è consigliabile eseguire. Ad esempio, facendo clic su questo collegamento, è possibile passare all'archivio e installare le applicazioni di protezione nei dispositivi oppure visualizzare un elenco di dispositivi o un elenco di eventi. Dopo aver eseguito l'azione consigliata per la notifica, alla notifica viene assegnato lo stato *Rivista*.

- **Stato registrato**. Contiene il numero di giorni o ore trascorsi dal momento in cui la notifica è stata registrata in Administration Server.

Per visualizzare le notifiche sullo schermo in una finestra distinta in base al livello di importanza:

1. Nell'angolo superiore destro di Kaspersky Security Center Web Console, fare clic sull'icona a forma di bandiera ( ).

   Se l'icona a forma di bandiera contiene un punto rosso, sono presenti notifiche che non sono state riviste.

   Verrà visualizzata una finestra che elenca le notifiche. Per impostazione predefinita, la scheda **Tutte le notifiche** è selezionata e le notifiche sono raggruppate per livello di importanza: *Critico*, *Avviso* e *Informazioni*.

2. Selezionare la scheda **Sistema**.

   Verrà visualizzato l'elenco delle notifiche con i livelli di importanza *Critico* ( ) e *Avviso* ( ). L'elenco delle notifiche include i seguenti elementi:

   - Contrassegno del colore. Le notifiche critiche sono contrassegnate in rosso. Le notifiche di avviso sono contrassegnate in giallo.
   - Icona che indica l'argomento della notifica: distribuzione ( ), protezione ( ), aggiornamenti ( ), gestione dispositivi ( ), Prevenzione Exploit ( ), Administration Server ( ).
   - Descrizione della notifica.
   - Icona a forma di bandiera. L'icona a forma di bandiera è grigia se alle notifiche è stato assegnato lo stato *Non rivista*. Quando si seleziona l'icona a forma di bandiera di colore grigio e si assegna lo stato *Rivista* a una notifica, il colore dell'icona diventa bianco.
   - Collegamento all'azione consigliata. Quando si esegue l'azione consigliata dopo aver fatto clic sul collegamento, alla notifica viene assegnato lo stato *Rivista*.
   - Numero di giorni trascorsi dalla data in cui la notifica è stata registrata in Administration Server.

3. Selezionare la scheda **Altro**.

   Verrà visualizzato l'elenco delle notifiche con il livello di importanza *Informazioni*.

   L'organizzazione dell'elenco è la stessa dell'elenco nella scheda **Sistema** (vedere la descrizione precedente). L'unica differenza è l'assenza di un contrassegno del colore.

È possibile filtrare le notifiche in base all'intervallo di date in cui sono state registrate in Administration Server. Utilizzare la casella di controllo **Mostra filtro** per gestire il filtro.

Per visualizzare le notifiche sullo schermo nel widget:

1. Nella sezione **Dashboard** selezionare **Aggiungi o ripristina widget Web**.

2. Nella finestra visualizzata fare clic sulla categoria **Altro**, selezionare il widget **Notifiche in base al livello di criticità selezionato** e fare clic su Aggiungi.

   Il widget verrà visualizzato nella scheda **Dashboard**. Per impostazione predefinita, nel widget vengono visualizzate le notifiche con il livello di importanza *Critico*.

   È possibile fare clic sul pulsante **Impostazioni** nel widget e modificare le impostazioni del widget per visualizzare le notifiche con il livello di importanza *Avviso*. In alternativa, è possibile aggiungere un altro widget: **Notifiche in base al livello di criticità selezionato**, con un livello di importanza *Avviso*.

   L'elenco delle notifiche nel widget è limitato dalle dimensioni e include due notifiche. Queste due notifiche si riferiscono agli ultimi eventi.

L'elenco delle notifiche nel widget include i seguenti elementi:

- Icona relativa all'argomento della notifica: distribuzione (), protezione (), aggiornamenti (), gestione dispositivi (), Prevenzione Exploit (), Administration Server ().
- Descrizione della notifica con un collegamento all'azione consigliata. Quando si esegue un'azione consigliata dopo aver fatto clic sul collegamento, alla notifica viene assegnato lo stato *Rivista*.
- Numero di giorni o numero di ore trascorsi dalla data in cui la notifica è stata registrata in Administration Server.
- Collegamento ad altre notifiche. Facendo clic su questo collegamento, è possibile passare alla visualizzazione delle notifiche nella sezione **Notifiche** della sezione **Monitoraggio e generazione dei rapporti**.

Informazioni sugli stati dei dispositivi

Kaspersky Security Center assegna uno stato a ciascun dispositivo gestito. Lo stato specifico dipende dal rispetto delle condizioni definite dall'utente. In alcuni casi, durante l'assegnazione di uno stato a un dispositivo, Kaspersky Security Center prende in considerazione il flag di visibilità del dispositivo nella rete (vedere la tabella seguente). Ad esempio, se a un dispositivo gestito è stato assegnato lo stato *Critico* perché è stata soddisfatta la condizione *I database non sono aggiornati* e successivamente è stato impostato il flag di visibilità per il dispositivo, al dispositivo viene assegnato lo stato *OK*. Se Kaspersky Security Center non rileva un dispositivo nella rete entro due ore, il flag di visibilità del dispositivo è impostato su *Non visibile*.

Gli stati sono i seguenti:

- *Critico* o *Critico / Visibile*
- *Avviso* o *Avviso / Visibile*
- *OK* o *OK / Visibile*

La tabella seguente elenca le condizioni predefinite da soddisfare per assegnare a un dispositivo lo stato *Critico* o *Avviso*, con tutti i possibili valori.

Condizioni per l'assegnazione di uno stato a un dispositivo

Condizione	Descrizione della condizione	Valori disponibili
Applicazione di protezione non installata	Network Agent è installato nel dispositivo, ma un'applicazione di protezione non è installata.	• L'interruttore è attivato. • L'interruttore è disattivato.
Troppi virus rilevati	Nel dispositivo sono stati rilevati alcuni virus da parte di un'attività per il rilevamento dei virus, ad esempio l'attività *Scansione malware*, e il numero di virus trovati supera il valore specificato.	Più di 0.
Livello protezione in tempo reale diverso da quello impostato dall'amministratore	Il dispositivo è visibile nella rete, ma il livello della protezione in tempo reale è diverso dal livello impostato (nella condizione) dall'amministratore per lo stato del dispositivo.	• Arrestata. • Sospesa. • In esecuzione.
Scansione malware non eseguita da molto tempo	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma né l'attività *Scansione malware* né un'attività di scansione locale sono state eseguite nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server 7 giorni o più di 7 giorni prima.	Più di 1 giorno.
I database non sono aggiornati	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma i database anti-virus non vengono aggiornati nel dispositivo nell'intervallo di tempo specificato. La condizione è applicabile solo ai dispositivi che sono stati aggiunti al database di Administration Server un giorno o più di un giorno prima.	Più di 1 giorno.
Connessione non eseguita da molto tempo	Network Agent è installato nel dispositivo, ma il dispositivo non viene connesso a un Administration Server nell'intervallo di tempo specificato, perché il dispositivo era spento.	Più di 1 giorno.
Rilevate minacce attive	Il numero di oggetti non elaborati nella cartella **Minacce attive** è superiore al valore specificato.	Più di 0 elementi.
È necessario il riavvio	Il dispositivo è visibile nella rete, ma un'applicazione richiede il riavvio del dispositivo da un periodo superiore all'intervallo di tempo specificato e per uno dei motivi selezionati.	Più di 0 minuti.
Applicazioni incompatibili installate	Il dispositivo è visibile nella rete, ma l'inventario software eseguito tramite Network Agent ha rilevato applicazioni incompatibili installate nel dispositivo.	• L'interruttore è disattivato. • L'interruttore è attivato.
Rilevate vulnerabilità del software	Il dispositivo è visibile nella rete e Network Agent è installato nel dispositivo, ma l'attività *Trova vulnerabilità e aggiornamenti richiesti* ha rilevato vulnerabilità con il livello di criticità specificato nelle applicazioni installate nel dispositivo.	• Critico. • Alto. • Medio. • Ignora se non è possibile correggere il tipo di vulnerabilità. • Ignora se un aggiornamento è assegnato per l'installazione.
La licenza è scaduta	Il dispositivo è visibile nella rete, ma la licenza è scaduta.	• L'interruttore è disattivato. • L'interruttore è attivato.
La licenza sta per scadere	Il dispositivo è visibile nella rete, ma la licenza nel dispositivo scadrà tra un numero di giorni inferiore rispetto a quello specificato.	Meno di 0 giorni.
Verifica disponibilità aggiornamenti di Windows Update non eseguita da molto tempo	Il dispositivo è visibile nella rete, ma l'attività *Esegui sincronizzazione di Windows Update* non viene eseguita nell'intervallo di tempo specificato.	Più di 1 giorno.

Condizione	Descrizione della condizione	Valori disponibili
Stato criptaggio non valido	Network Agent è installato nel dispositivo, ma il risultato del criptaggio dispositivo è uguale al valore specificato.	• Non è conforme al criterio a causa di un rifiuto dell'utente (solo per i dispositivi esterni). • Non è conforme al criterio a causa di un errore. • È richiesto il riavvio per l'applicazione del criterio. • Non è specificato alcun criterio di criptaggio. • Non supportato. • Quando viene applicato il criterio.
Impostazioni dispositivo mobile non conformi al criterio	Le impostazioni del dispositivo mobile sono diverse dalle impostazioni specificate nel criterio di Kaspersky Endpoint Security for Android durante il controllo delle regole di conformità.	• L'interruttore è disattivato. • L'interruttore è attivato.
Problemi di sicurezza non elaborati rilevati	Sono stati rilevati nel dispositivo alcuni problemi di sicurezza non elaborati. I problemi di sicurezza possono essere creati automaticamente, tramite le applicazioni gestite Kaspersky installate nel dispositivo client, o manualmente, dall'amministratore.	• L'interruttore è disattivato. • L'interruttore è attivato.
Stato dispositivo definito dall'applicazione	Lo stato del dispositivo è definito dall'applicazione gestita. I dispositivi gestiti possono avere uno stato definito dallr applicazioni gestite indipendentemente dalle impostazioni di Kaspersky Security Center. Dopo che questo stato restituisce uno degli stati definiti da Kaspersky Security Center, Administration Server assegna a un dispositivo gestito lo stato più critico tra quelli restituiti dall'applicazione gestita e assegnati da Administration Server. Gli stati definiti dalle applicazioni gestite hanno descrizioni trasferite dalle applicazioni gestite. È possibile visualizzare le descrizioni nell'elenco dei dispositivi gestiti, colonna **Descrizione stato**.	• L'interruttore è disattivato. • L'interruttore è attivato.
Spazio su disco esaurito nel dispositivo	Lo spazio disponibile sul disco nel dispositivo è inferiore al valore specificato o il dispositivo non può essere sincronizzato con Administration Server. Lo stato *Critico* o *Avviso* diventa *OK* quando il dispositivo viene sincronizzato con Administration Server e lo spazio disponibile nel dispositivo è maggiore o uguale al valore specificato.	Più di 0 MB.
Il dispositivo è diventato non gestito	Durante la device discovery, il dispositivo è stato riconosciuto come visibile nella rete, ma più di tre tentativi di sincronizzazione con Administration Server hanno avuto esito negativo.	• L'interruttore è disattivato. • L'interruttore è attivato.
Protezione disattivata	Il dispositivo è visibile nella rete, ma l'applicazione di protezione nel dispositivo è stata disabilitata per un periodo superiore all'intervallo di tempo specificato. In questo caso, lo stato dell'applicazione di protezione è *interrotto* o *non riuscito* e differisce dai seguenti: *avvio*, *esecuzione* o *sospensione*.	Più di 0 minuti.
Applicazione di protezione non in esecuzione	Il dispositivo è visibile nella rete e un'applicazione di protezione è installata nel dispositivo, ma non è in esecuzione.	• L'interruttore è disattivato. • L'interruttore è attivato.

Kaspersky Security Center consente di configurare la selezione automatica dello stato di un dispositivo in un gruppo di amministrazione quando vengono soddisfatte le condizioni specificate. Quando vengono soddisfatte le condizioni specificate, al dispositivo client viene assegnato uno dei seguenti stati: *Critico* o *Avviso*. Quando le condizioni specificate non vengono soddisfatte, al dispositivo client viene assegnato lo stato *OK*.

Diversi stati possono corrispondere ai diversi valori di una condizione. Ad esempio, per impostazione predefinita, se alla condizione **I database non sono aggiornati** è associato il valore **Più di 3 giorni**, al dispositivo client sarà assegnato lo stato *Avviso*; se il valore è **Più di 7 giorni**, verrà assegnato lo stato *Critico*.

Se si esegue l'upgrade di Kaspersky Security Center dalla versione precedente, i valori della condizione **I database non sono aggiornati** per l'assegnazione dello stato *Critico* o *Avviso* restano invariati.

Configurazione del passaggio degli stati del dispositivo

È possibile modificare le condizioni per assegnare lo stato *Critico* o *Avviso* a un dispositivo.

Per abilitare la modifica dello stato del dispositivo in Critico:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.
4. Nel riquadro sinistro selezionare **Critico**.
5. Nel riquadro destro, nella sezione **Imposta su Critico se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Critico*.

   > È possibile modificare solo le impostazioni che non sono bloccate nel criterio principale.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.
7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.
8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.
9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Critico*.

Per abilitare la modifica dello stato del dispositivo in Avviso:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Gerarchia dei gruppi**.
2. Nell'elenco dei gruppi visualizzato fare clic sul collegamento con il nome di un gruppo per cui si desidera modificare lo stato del dispositivo.
3. Nella finestra delle proprietà visualizzata selezionare la scheda **Stato dispositivo**.

4. Nel riquadro sinistro selezionare **Avviso**.
5. Nel riquadro destro, nella sezione **Imposta su Avviso se è specificato**, abilitare la condizione per il passaggio di un dispositivo allo stato *Avviso*.

   È possibile modificare solo le impostazioni che non sono bloccate nel criterio principale.

6. Selezionare il pulsante di opzione accanto alla condizione nell'elenco.
7. Nell'angolo superiore sinistro dell'elenco fare clic sul pulsante **Modifica**.
8. Impostare il valore richiesto per la condizione selezionata.

   I valori non possono essere impostati per tutte le condizioni.

9. Fare clic su **OK**.

Quando le condizioni specificate vengono soddisfatte, al dispositivo gestito viene assegnato lo stato *Avviso*.

Configurazione dell'invio delle notifiche

È possibile configurare notifiche per gli eventi che si verificano in Kaspersky Security Center. A seconda del metodo di notifica scelto, sono disponibili i seguenti tipi di notifiche:

- E-mail: quando si verifica un evento, Kaspersky Security Center invia una notifica agli indirizzi e-mail specificati.
- SMS: quando si verifica un evento, Kaspersky Security Center invia una notifica ai numeri di telefono specificati.
- File eseguibile: quando si verifica un evento, viene eseguito il file eseguibile in Administration Server.

Per configurare l'invio delle notifiche per gli eventi che si verificano in Kaspersky Security Center:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server, con la scheda **Generale** selezionata.

2. Fare clic sulla sezione **Notifica** e nel riquadro destro selezionare la scheda per il metodo di notifica desiderato:

   - E-mail

La scheda **E-mail** consente di configurare la notifica degli eventi tramite e-mail.

Nel campo **Destinatari (indirizzi e-mail)** specificare gli indirizzi e-mail a cui l'applicazione invierà le notifiche. È possibile specificare più indirizzi in questo campo, separandoli con punto e virgola.

Nel campo **Server SMTP** specificare gli indirizzi dei server di posta, separandoli con punto e virgola. È possibile utilizzare i seguenti valori:

- Indirizzo IPv4 o IPv6
- Nome di rete Windows (nome NetBIOS) del dispositivo
- Nome DNS del server SMTP

Nel campo **Porta server SMTP** specificare il numero di una porta di comunicazione del server SMTP. Il numero di porta predefinito è 25.

Se si abilita l'opzione **Usa ricerca DNS MX**, è possibile utilizzare più record MX degli indirizzi IP per lo stesso nome DNS del server SMTP. Lo stesso nome DNS può avere diversi record MX con valori di priorità differenti di ricezione dei messaggi e-mail. Administration Server tenta di inviare notifiche e-mail al server SMTP in ordine crescente di priorità dei record MX.

Se si abilita l'opzione **Usa ricerca DNS MX** e non si abilita l'utilizzo delle impostazioni TLS, è consigliabile utilizzare le impostazioni DNSSEC nel dispositivo server come misura di protezione aggiuntiva per l'invio di notifiche e-mail.

Se si abilita l'opzione **Usa autenticazione ESMTP**, è possibile specificare le impostazioni di autenticazione ESMTP nei campi **Nome utente** e **Password**. Per impostazione predefinita, l'opzione è disabilitata e le impostazioni per l'autenticazione ESMTP non sono disponibili.

È possibile specificare le impostazioni di connessione TLS con un server SMTP:

- **Non utilizzare TLS**

È possibile selezionare questa opzione se si desidera disabilitare il criptaggio dei messaggi e-mail.

- **Usa TLS se supportato dal server SMTP**

È possibile selezionare questa opzione se si desidera utilizzare una connessione TLS in un server SMTP. Se il server SMTP non supporta TLS, Administration Server si connette al server SMTP senza utilizzare TLS.

- **Usa sempre TLS, controlla la validità del certificato del server**

È possibile selezionare questa opzione se si desidera utilizzare le impostazioni di autenticazione TLS. Se il server SMTP non supporta TLS, Administration Server non può connettersi al server SMTP.

È consigliabile utilizzare questa opzione per una protezione più efficace della connessione con un server SMTP. Se si seleziona questa opzione, è possibile configurare le impostazioni di autenticazione per una connessione TLS.

Se si seleziona il valore **Usa sempre TLS, controlla la validità del certificato del server**, è possibile specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. È inoltre possibile specificare un certificato per l'autenticazione del client nel server SMTP.

È possibile specificare i certificati per una connessione TLS facendo clic sul collegamento **Specifica certificati**:

- Cercare un file di certificato del server SMTP:

È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Administration Server. Kaspersky Security Center verifica se anche il certificato di un server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center non può connettersi a un server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

- Cercare un file di certificato del client:

È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. È necessario specificare il certificato e la relativa chiave privata utilizzando uno dei seguenti tipi di certificato:

- Certificato X-509:

È necessario specificare un file con il certificato e un file con la chiave privata. Entrambi i file non dipendono l'uno dall'altro e l'ordine di caricamento dei file non è significativo. Quando entrambi i file vengono caricati, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

- Contenitore pkcs12:

È necessario caricare un singolo file che contenga il certificato e la relativa chiave privata. Quando il file viene caricato, è necessario specificare la password per la decodifica della chiave privata. La password può avere un valore vuoto se la chiave privata non è codificata.

Nel campo **Oggetto** specificare l'oggetto del messaggio e-mail. È possibile lasciare vuoto questo campo.

Nell'elenco a discesa **Modello oggetto** selezionare il modello per l'oggetto. Una variabile determinata dal modello selezionato viene automaticamente inserita nel campo **Oggetto**. È possibile creare un oggetto e-mail selezionando diversi modelli di oggetto.

Nel campo **Indirizzo e-mail del mittente** specificare l'indirizzo del mittente del messaggio e-mail. Se si lascia vuoto questo campo, per impostazione predefinita viene utilizzato l'indirizzo del destinatario. Non è consigliabile utilizzare indirizzi e-mail fittizi.

Il campo **Messaggio di notifica** contiene testo standard con le informazioni sull'evento inviate dall'applicazione quando si verifica un evento. Il testo include parametri sostitutivi, ad esempio il nome dell'evento, il nome del dispositivo e il nome di dominio. È possibile modificare il testo del messaggio aggiungendo altri parametri sostitutivi con dettagli più pertinenti sull'evento.

> Se il testo di notifica contiene un segno percentuale (%), è necessario digitarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

Il collegamento **Configura un limite numerico per le notifiche** consente di specificare il numero massimo di notifiche che l'applicazione può inviare nell'intervallo di tempo specificato.

Il pulsante **Invia messaggio di test** consente di verificare se le notifiche sono state configurate correttamente: l'applicazione invia una notifica di prova all'indirizzo e-mail specificato.

- SMS

La scheda **SMS** consente di configurare la trasmissione delle notifiche SMS di diversi eventi a un cellulare. I messaggi SMS vengono inviati tramite un gateway di posta.

Nel campo **Server SMTP** specificare gli indirizzi dei server di posta, separandoli con punto e virgola. È possibile utilizzare i seguenti valori:

- Indirizzo IPv4 o IPv6
- Nome di rete Windows (nome NetBIOS) del dispositivo
- Nome DNS del server SMTP

Nel campo **Porta server SMTP** specificare il numero di una porta di comunicazione del server SMTP. Il numero di porta predefinito è 25.

Se l'opzione **Usa autenticazione ESMTP** è abilitata, è possibile specificare le impostazioni di autenticazione ESMTP nei campi **Nome utente** e **Password**. Per impostazione predefinita, l'opzione è disabilitata e le impostazioni per l'autenticazione ESMTP non sono disponibili.

È possibile specificare le impostazioni di connessione TLS con un server SMTP:

- **Non utilizzare TLS**

È possibile selezionare questa opzione se si desidera disabilitare il criptaggio dei messaggi e-mail.

- **Usa TLS se supportato dal server SMTP**

È possibile selezionare questa opzione se si desidera utilizzare una connessione TLS in un server SMTP. Se il server SMTP non supporta TLS, Administration Server si connette al server SMTP senza utilizzare TLS.

- **Usa sempre TLS, controlla la validità del certificato del server**

È possibile selezionare questa opzione se si desidera utilizzare le impostazioni di autenticazione TLS. Se il server SMTP non supporta TLS, Administration Server non può connettersi al server SMTP.

È consigliabile utilizzare questa opzione per una protezione più efficace della connessione con un server SMTP. Se si seleziona questa opzione, è possibile configurare le impostazioni di autenticazione per una connessione TLS.

Se si seleziona il valore **Usa sempre TLS, controlla la validità del certificato del server**, è possibile specificare un certificato per l'autenticazione del server SMTP e scegliere se si desidera abilitare la comunicazione tramite qualsiasi versione di TLS o solo tramite TLS 1.2 o versioni successive. È inoltre possibile specificare un certificato per l'autenticazione del client nel server SMTP.

È possibile specificare il file del certificato del server SMTP facendo clic sul collegamento **Specifica certificati**:

È possibile ricevere un file con l'elenco dei certificati da un'autorità di certificazione attendibile e caricare il file in Administration Server. Kaspersky Security Center verifica se anche il certificato di un server SMTP è firmato da un'autorità di certificazione attendibile. Kaspersky Security Center non può connettersi a un server SMTP se il certificato del server SMTP non viene ricevuto da un'autorità di certificazione attendibile.

Nel campo **Destinatari (indirizzi e-mail)** specificare gli indirizzi e-mail a cui l'applicazione invierà le notifiche. È possibile specificare più indirizzi in questo campo, separandoli con punto e virgola. Le notifiche verranno inviate ai numeri di telefono associati agli indirizzi e-mail specificati.

Nel campo **Oggetto** specificare l'oggetto del messaggio e-mail.

Nell'elenco a discesa **Modello oggetto** selezionare il modello per l'oggetto. Una variabile basata sul modello selezionato viene inserita nel campo **Oggetto**. È possibile creare un oggetto e-mail selezionando diversi modelli di oggetto.

Nel campo **Indirizzo e-mail del mittente: se questa impostazione non è specificata, verrà utilizzato l'indirizzo del destinatario. Avviso: è consigliabile non utilizzare un indirizzo e-mail fittizio** specificare l'indirizzo del mittente del messaggio e-mail. Se si lascia vuoto questo campo, per impostazione predefinita viene utilizzato l'indirizzo del destinatario. Non è consigliabile utilizzare indirizzi e-mail fittizi.

Nel campo **Numeri di telefono dei destinatari dei messaggi SMS** specificare i numeri di cellulare dei destinatari delle notifiche SMS.

Nel campo **Messaggio di notifica** specificare un testo standard con le informazioni sull'evento inviate dall'applicazione quando si verifica un evento. Il testo può includere parametri sostitutivi, ad esempio il nome dell'evento, il nome del dispositivo e il nome di dominio.

Se il testo di notifica contiene un segno percentuale (%), è necessario digitarlo due volte di seguito per consentire l'invio del messaggio. Ad esempio, "Il carico della CPU è 100%%".

Fare clic sul collegamento **Configura un limite numerico per le notifiche** per specificare il numero massimo di notifiche che l'applicazione può inviare durante l'intervallo di tempo specificato.

Fare clic su **Invia messaggio di test** per verificare se le notifiche sono state configurate correttamente: l'applicazione invia una notifica di prova al destinatario specificato.

- File eseguibile da avviare

Se è selezionato questo metodo di notifica, nel campo di immissione è possibile specificare l'applicazione che verrà avviata quando si verifica un evento.

Nel campo **File eseguibile da avviare in Administration Server al verificarsi di un evento** specificare la cartella e il nome del file da eseguire. Prima di specificare il file, preparare il file e specificare i segnaposto che definiscono i dettagli dell'evento da inviare nel messaggio di notifica. La cartella e il file specificati devono trovarsi in Administration Server.

Il collegamento **Configura un limite numerico per le notifiche** consente di specificare il numero massimo di notifiche che l'applicazione può inviare nell'intervallo di tempo specificato.

3. Nella scheda definire le impostazioni di notifica.
4. Fare clic sul pulsante **OK** per chiudere la finestra delle proprietà di Administration Server.

Le impostazioni di invio delle notifiche salvate vengono applicate a tutti gli eventi che si verificano in Kaspersky Security Center.

È possibile sostituire le impostazioni di invio delle notifiche per determinati eventi nella sezione **Configurazione eventi** delle impostazioni di Administration Server, delle impostazioni di un criterio o delle impostazioni di un'applicazione.

Notifiche degli eventi visualizzate dall'esecuzione di un file eseguibile

Kaspersky Security Center consente di inviare all'amministratore notifiche degli eventi nei dispositivi client visualizzate dall'esecuzione di un file eseguibile. Il file eseguibile deve contenere un altro file eseguibile con segnaposto dell'evento da inviare all'amministratore (vedere la tabella seguente).

Segnaposto per la descrizione di un evento

Segnaposto	Descrizione del segnaposto
%SEVERITY%	Livello di criticità di un evento. Valori possibili: • **Informazioni** • **Avviso** • **Errore** • **Critico**
%COMPUTER%	Nome del dispositivo in cui si è verificato l'evento. La lunghezza massima del nome del dispositivo è di 256 caratteri.
%DOMAIN%	Nome di dominio del dispositivo in cui si è verificato l'evento
%EVENT%	Nome del tipo di evento. La lunghezza massima del nome del tipo di evento è 50 caratteri.
%DESCR%	Descrizione dell'evento. La lunghezza massima della descrizione è di 1000 caratteri.
%RISE_TIME%	Ora di creazione dell'evento.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nome dell'attività. La lunghezza massima del nome dell'attività è di 100 caratteri.
%KL_PRODUCT%	Nome applicazione.
%KL_VERSION%	Numero di versione dell'applicazione.
%KLCSAK_EVENT_SEVERITY_NUM%	Numero del livello di criticità dell'evento. Valori possibili: • 1—**Informazioni** • 2—**Avviso** • 3—**Errore** • 4—**Critico**
%HOST_IP%	Indirizzo IP del dispositivo in cui si è verificato l'evento.
%HOST_CONN_IP%	Indirizzo IP della connessione del dispositivo in cui si è verificato l'evento.

Esempio:
Le notifiche degli eventi sono inviate tramite un file eseguibile (come script1.bat) all'interno del quale viene avviato un altro file eseguibile (come script2.bat) con il segnaposto %COMPUTER%. Quando si verifica un evento, il file script1.bat viene eseguito nel dispositivo dell'amministratore, eseguendo a sua volta il file script2.bat con il segnaposto %COMPUTER%. L'amministratore riceverà il nome del dispositivo in cui si è verificato l'evento.

Annunci Kaspersky

Questa sezione descrive come utilizzare, configurare e disabilitare gli annunci di Kaspersky.

Informazioni sugli annunci di Kaspersky

La sezione Annunci Kaspersky (**Monitoraggio e generazione dei rapporti → Annunci Kaspersky**) consente di rimanere informati fornendo informazioni relative alla versione in uso di Kaspersky Security Center e alle applicazioni gestite installate nei dispositivi gestiti. Kaspersky Security Center aggiorna periodicamente le informazioni nella sezione rimuovendo gli annunci obsoleti e aggiungendo nuove informazioni.

Kaspersky Security Center mostra solo gli annunci di Kaspersky relativi all'Administration Server attualmente connesso e alle applicazioni Kaspersky installate nei dispositivi gestiti di questo Administration Server. Gli annunci vengono visualizzati singolarmente per qualsiasi tipo di Administration Server: primario, secondario o virtuale.

L'Administration Server deve disporre di una connessione Internet per ricevere gli annunci Kaspersky.

Gli annunci includono informazioni dei seguenti tipi:

- Annunci relativi alla sicurezza

  Gli annunci relativi alla sicurezza hanno lo scopo di mantenere aggiornate e completamente funzionanti le applicazioni Kaspersky installate nella rete. Gli annunci possono includere informazioni sugli aggiornamenti critici per le applicazioni Kaspersky, correzioni per le vulnerabilità rilevate e modalità di risoluzione di altri problemi nelle applicazioni Kaspersky. Gli annunci relativi alla sicurezza sono abilitati per impostazione predefinita. Se non si desidera ricevere gli annunci, è possibile disabilitare questa funzionalità.

  Per mostrare le informazioni corrispondenti alla configurazione della protezione di rete, Kaspersky Security Center invia i dati ai server cloud Kaspersky e riceve solo gli annunci relativi alle applicazioni Kaspersky installate nella rete. Il set di dati che può essere inviato ai server è descritto nel Contratto di licenza con l'utente finale che l'utente accetta durante l'installazione di Kaspersky Security Center Administration Server.

- Annunci di marketing

  Gli annunci di marketing includono informazioni su offerte speciali per le applicazioni Kaspersky, pubblicità e notizie provenienti da Kaspersky. Gli annunci di marketing sono disabilitati per impostazione predefinita. Questo tipo di annunci viene ricevuto solo se è stato abilitato Kaspersky Security Network (KSN). È possibile disabilitare gli annunci di marketing disabilitando KSN.

  Al fine di mostrare solo le informazioni attinenti che potrebbero essere utili per la protezione dei dispositivi di rete e nelle attività quotidiane, Kaspersky Security Center invia i dati ai server cloud Kaspersky e riceve gli annunci appropriati. Il set di dati che può essere inviato ai server è descritto nella sezione Dati elaborati dell' Informativa KSN.

Le nuove informazioni sono suddivise nelle seguenti categorie, in base al livello di importanza:

1. Informazioni critiche
2. Novità importanti
3. Avviso
4. Informazioni

Quando vengono visualizzate nuove informazioni nella sezione Annunci Kaspersky, Kaspersky Security Center Web Console visualizza un'etichetta di notifica che corrisponde al livello di importanza degli annunci. È possibile fare clic sull'etichetta per visualizzare l'annuncio nella sezione Annunci Kaspersky.

È possibile specificare le impostazioni degli annunci Kaspersky, comprese le categorie di annunci che si desidera visualizzare e dove visualizzare l'etichetta di notifica.

Configurazione delle impostazioni per gli annunci di Kaspersky

Nella sezione Annunci Kaspersky è possibile specificare le impostazioni degli annunci Kaspersky, comprese le categorie di annunci che si desidera visualizzare e dove visualizzare l'etichetta di notifica.

Per configurare gli annunci Kaspersky:

1. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti → Annunci Kaspersky**.
2. Fare clic sul collegamento **Impostazioni**.

   Verrà visualizzata la finestra delle impostazioni degli annunci di Kaspersky.
3. Specificare le seguenti impostazioni:

   - Selezionare il livello di importanza degli annunci che si desidera visualizzare. Gli annunci di altre categorie non verranno visualizzati.
   - Selezionare dove si desidera visualizzare l'etichetta di notifica. L'etichetta può essere visualizzata in tutte le sezioni della console o nella sezione **Monitoraggio e generazione dei rapporti** e nelle relative sottosezioni.
4. Fare clic sul pulsante **OK**.

   Le impostazioni degli annunci Kaspersky sono state specificate.

Disabilitazione degli annunci di Kaspersky

La sezione Annunci Kaspersky (**Monitoraggio e generazione dei rapporti → Annunci Kaspersky**) consente di rimanere informati fornendo informazioni relative alla versione in uso di Kaspersky Security Center e alle applicazioni gestite installate nei dispositivi gestiti. Se non si desidera ricevere gli annunci di Kaspersky, è possibile disabilitare questa funzionalità.

Gli annunci Kaspersky includono due tipi di informazioni: annunci relativi alla sicurezza e annunci di marketing. È possibile disabilitare separatamente gli annunci di ciascun tipo.

Per disabilitare gli annunci relativi alla sicurezza:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Generale** selezionare la sezione **Annunci Kaspersky**.
3. Spostare l'interruttore sulla posizione **Annunci relativi alla sicurezza Disabilitati**.
4. Fare clic sul pulsante **Salva**.

   Gli annunci di Kaspersky vengono disabilitati.

Gli annunci di marketing sono disabilitati per impostazione predefinita. Gli annunci di marketing vengono ricevuti solo se è stato abilitato Kaspersky Security Network (KSN). È possibile disabilitare questo tipo di annunci disabilitando KSN.

Per disabilitare gli annunci di marketing:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.
2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN**.

3. Disabilitare l'opzione **Usa Kaspersky Security Network Abilitato**.

4. Fare clic sul pulsante **Salva**.

   Gli annunci di marketing vengono disabilitati.

Visualizzazione delle informazioni sui rilevamenti delle minacce

È possibile abilitare o disabilitare la visualizzazione delle informazioni relative agli avvisi.

*Per abilitare o disabilitare la visualizzazione della sezione **Avvisi** nel menu principale:*

1. Nel menu principale, passare alle impostazioni dell'account, quindi selezionare **Opzioni di interfaccia**.

2. Nella finestra **Opzioni di interfaccia** visualizzata abilitare o disabilitare l'opzione **Mostra avvisi EDR**.

3. Fare clic su **Salva**.

La console visualizza la sottosezione **Avvisi** nella sezione **Monitoraggio e generazione dei rapporti** del menu principale. Nella sottosezione **Avvisi** è possibile visualizzare informazioni sui rilevamenti delle minacce nei dispositivi endpoint. Se si aggiunge una chiave di licenza per EDR Optimum, Kaspersky Security Center Web Console visualizza automaticamente la sottosezione **Avvisi** nella sezione **Monitoraggio e generazione dei rapporti** del menu principale. È inoltre possibile aggiungere un widget che visualizza informazioni sugli avvisi.

> La sottosezione **Avvisi** viene visualizzata automaticamente solo se è stata aggiunta la chiave di licenza per EDR Optimum prima di abilitare l'opzione **Mostra avvisi EDR**. Se la chiave di licenza è stata aggiunta dopo aver abilitato l'opzione **Mostra avvisi EDR**, la sottosezione **Avvisi** verrà visualizzata solo dopo aver riabilitato questa opzione.

Per visualizzare correttamente le informazioni dettagliate sulle minacce rilevate nella scheda di avviso, è necessario installare il plug-in Kaspersky Endpoint Agent e la versione compatibile del plug-in Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux 12.1 o versione successiva, Kaspersky Endpoint Security for Mac 12.1 o versione successiva oppure Kaspersky Endpoint Security for Windows 12.6 o versione successiva).

Usare il menu **Filtro** per filtrare gli avvisi in base alla data e ai valori di campo.

Il campo **Tipo di oggetto** contiene i seguenti valori:

- Sconosciuto
- Collegamento di phishing
- Virus
- Trojan
- Strumento dannoso
- Backdoor
- Worm
- Altra applicazione

- Adware
- Pornware
- Programma compresso pericoloso
- Comportamento pericoloso

Il campo **Risposta automatica** contiene i seguenti valori:

- Rilevato oggetto dannoso
- Oggetto eliminato
- Oggetto disinfettato
- L'oggetto non è stato disinfettato
- Oggetto spostato in Quarantena
- Rilevato archivio protetto da password
- Rilevato virus

Cloud Discovery

Kaspersky Security Center consente di monitorare l'utilizzo dei servizi cloud nei dispositivi gestiti che eseguono Windows e di bloccare l'accesso ai servizi cloud considerati indesiderati. Cloud Discovery monitora i tentativi da parte degli utenti di ottenere l'accesso a questi servizi tramite i browser e le applicazioni desktop. Inoltre, tiene traccia dei tentativi da parte degli utenti di ottenere l'accesso ai servizi cloud tramite connessioni non criptate (ad esempio utilizzando il protocollo HTTP). Questa funzionalità consente di rilevare e bloccare l'utilizzo dei servizi cloud tramite shadow IT.

La funzionalità di blocco è disponibile solo se Kaspersky Security Center è stato attivato con una licenza Kaspersky Next EDR Optimum o Kaspersky Next XDR Expert.

La funzionalità di blocco è disponibile solo se si utilizza Kaspersky Endpoint Security 11.2 for Windows o versioni successive. Le versioni precedenti dell'applicazione di protezione consentono solo di monitorare l'utilizzo dei servizi cloud.

È possibile abilitare la funzionalità Cloud Discovery e selezionare i profili di protezione per i quali si desidera abilitare la funzionalità. È anche possibile abilitare o disabilitare la funzionalità separatamente in ciascun criterio o profilo di protezione. È possibile bloccare l'accesso ai servizi cloud a cui si desidera che gli utenti non accedano.

Per poter bloccare l'accesso ai servizi cloud indesiderati, assicurarsi che siano soddisfatti i seguenti prerequisiti:

- Si utilizza Kaspersky Endpoint Security 11.2 for Windows o versioni successive. Le versioni precedenti dell'applicazione di protezione consentono solo di monitorare l'utilizzo dei servizi cloud.
- È stato acquistato un livello di licenza Kaspersky Next che include la possibilità di bloccare l'accesso ai servizi cloud indesiderati. Per i dettagli, fare riferimento alla Guida di Kaspersky Next.

Il widget Cloud Discovery e i rapporti Cloud Discovery consentono di visualizzare le informazioni sui tentativi riusciti e bloccati di ottenere l'accesso ai servizi cloud. Il widget mostra inoltre il livello di rischio di ciascun servizio cloud. Kaspersky Security Center ottiene le informazioni sull'utilizzo dei servizi cloud da tutti i dispositivi gestiti protetti solo dai criteri o dai profili di protezione con la funzionalità abilitata.

Abilitazione di Cloud Discovery utilizzando il widget

La funzionalità Cloud Discovery consente di ottenere informazioni sull'utilizzo dei servizi cloud da tutti i dispositivi gestiti protetti solo dai criteri di protezione con la funzionalità abilitata. È possibile abilitare o disabilitare Cloud Discovery solo per il criterio di Kaspersky Endpoint Security for Windows.

Esistono due modi per abilitare la funzionalità Cloud Discovery:

- Utilizzando il widget Cloud Discovery:
- Nelle proprietà del criterio di Kaspersky Endpoint Security for Windows.

  Per informazioni dettagliate su come abilitare la funzionalità Cloud Discovery nelle proprietà del criterio di Kaspersky Endpoint Security for Windows, fare riferimento alla sezione Cloud Discovery della Guida di Kaspersky Endpoint Security for Windows.

Si noti che è possibile disabilitare la funzionalità Cloud Discovery solo nei parametri del criterio di Kaspersky Endpoint Security for Windows.

Per abilitare Cloud Discovery, è necessario disporre del diritto di **Scrittura** nell'area funzionale **Funzionalità generali: Funzionalità di base**.

Per abilitare la funzionalità Cloud Discovery utilizzando il widget Cloud Discovery:

1. Passare a Kaspersky Security Center.
2. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
3. Nel widget **Cloud Discovery**, fare clic sul pulsante **Abilita**.

   Se è installato Kaspersky Endpoint Security for Windows versione 12.4, abilitare la funzionalità Cloud Discovery nelle proprietà del criterio di Kaspersky Endpoint Security for Windows. Per i dettagli, fare riferimento alla sezione Cloud Discovery della Guida di Kaspersky Endpoint Security for Windows.

   Se si dispone di una versione di Kaspersky Endpoint Security for Windows precedente alla 12.4, aggiornare il plug-in di Kaspersky Endpoint Security for Windows alla versione 12.5.

4. Nella finestra **Abilita Cloud Discovery** visualizzata, selezionare i criteri di sicurezza per cui si desidera abilitare la funzionalità, quindi fare clic sul pulsante **Abilita**.

   Le seguenti impostazioni dei criteri verranno abilitate automaticamente: **Inocula script nel traffico Web per interagire con le pagine Web**, **Monitoraggio sessione Web** e **Scansione connessioni criptate**.

La funzionalità Cloud Discovery è abilitata e il widget viene aggiunto al dashboard.

Aggiunta del widget Cloud Discovery al dashboard

È possibile aggiungere il widget **Cloud Discovery** al dashboard per monitorare l'utilizzo dei servizi cloud nei dispositivi gestiti.

Per aggiungere il widget Cloud Discovery al dashboard, è necessario disporre del diritto di **Scrittura** nell'area **Funzionalità generali: Funzionalità di base**.

Per aggiungere il widget Cloud Discovery al dashboard:

1. Passare a Kaspersky Security Center.
2. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.
3. Fare clic sul pulsante **Aggiungi o ripristina widget Web**.
4. Nell'elenco dei widget disponibili, fare clic sull'icona della freccia di espansione (>) accanto alla categoria **Altro**.
5. Selezionare il widget **Cloud Discovery**, quindi fare clic sul pulsante **Aggiungi**.

   Se la funzionalità Cloud Discovery è disabilitata, seguire le istruzioni nella sezione Abilitazione di Cloud Discovery utilizzando il widget.

Il widget selezionato verrà aggiunto alla fine del dashboard.

Visualizzazione delle informazioni sull'utilizzo dei servizi cloud

È possibile visualizzare il widget **Cloud Discovery** che mostra informazioni sui tentativi di accesso ai servizi cloud. Il widget mostra inoltre il livello di rischio di ciascun servizio cloud. Kaspersky Security Center ottiene le informazioni sull'utilizzo dei servizi cloud da tutti i dispositivi gestiti protetti solo dai profili di protezione con la funzionalità abilitata.

Prima di visualizzare, assicurarsi che:

- Il widget Cloud Discovery sia aggiunto al dashboard.
- La funzionalità Cloud Discovery sia abilitata.
- di disporre del diritto **Lettura** nell'area funzionale **Caratteristiche generali: Funzionalità di base**.

Per visualizzare il widget Cloud Discovery:

1. Passare a Kaspersky Security Center.
2. Nel menu principale accedere a **Monitoraggio e generazione dei rapporti** → **Dashboard**.

   Il widget **Cloud Discovery** viene visualizzato nel dashboard.

3. Nella parte sinistra del widget **Cloud Discovery**, selezionare una categoria di servizi cloud.

   La tabella nella parte destra del widget mostra fino a cinque servizi, della categoria selezionata, a cui gli utenti tentano più spesso di accedere. Vengono calcolati sia i tentativi andati a buon fine che quelli bloccati.

4. Nella parte destra del widget selezionare un servizio specifico.

   La tabella seguente mostra fino a dieci dispositivi che tentano più spesso di ottenere l'accesso al servizio. In questa tabella, è possibile generare due tipi di rapporti: rapporto sui tentativi di accesso riusciti e rapporto sui tentativi di accesso bloccati.

   In questa tabella, è inoltre possibile bloccare l'accesso al servizio cloud per un dispositivo specifico.

Il widget visualizza le informazioni richieste.

Dal widget visualizzato è possibile effettuare le seguenti operazioni:

- Passare alla sezione **Monitoraggio e generazione dei rapporti** → **Rapporti** per visualizzare i rapporti di Cloud Discovery.
- Bloccare o consentire l'accesso al servizio cloud selezionato.

La funzionalità di blocco è disponibile solo se Kaspersky Security Center è stato attivato con una licenza Kaspersky Next EDR Optimum o Kaspersky Next XDR Expert.

La funzionalità di blocco è disponibile solo se si utilizza Kaspersky Endpoint Security 11.2 for Windows o versioni successive. Le versioni precedenti dell'applicazione di protezione consentono solo di monitorare l'utilizzo dei servizi cloud.

Livello di rischio di un servizio cloud

Per ogni servizio cloud, Cloud Discovery fornisce un livello di rischio. Il livello di rischio consente di determinare i servizi che non soddisfano i requisiti di protezione dell'organizzazione. Ad esempio, è possibile tenere conto del livello di rischio quando si decide se bloccare l'accesso a un determinato servizio.

Il livello di rischio è un indice stimato e non fornisce indicazioni sulla qualità di un servizio cloud o sul produttore del servizio. Il livello di rischio è semplicemente una raccomandazione degli esperti di Kaspersky.

I livelli di rischio dei servizi cloud vengono visualizzati nel widget Cloud Discovery e nell'elenco di tutti i servizi cloud monitorati.

Blocco dell'accesso ai servizi cloud indesiderati

È possibile bloccare l'accesso ai servizi cloud a cui si desidera che gli utenti non accedano. È inoltre possibile consentire l'accesso ai servizi cloud precedentemente bloccati.

Tra le altre considerazioni, è consigliabile tenere conto del livello di rischio quando si decide se bloccare l'accesso a un determinato servizio.

È possibile bloccare o consentire l'accesso ai servizi cloud per un criterio o un profilo di sicurezza.

Esistono due modi per bloccare l'accesso ai servizi cloud indesiderati:

- Utilizzando il widget Cloud Discovery:

  In questo caso, è possibile bloccare uno per uno l'accesso ai servizi.

- Nelle proprietà del criterio di Kaspersky Endpoint Security for Windows.

  In questo caso, è possibile bloccare l'accesso ai servizi uno per uno o bloccare un'intera categoria contemporaneamente.

  Per informazioni dettagliate su come abilitare la funzionalità Cloud Discovery nelle proprietà del criterio di Kaspersky Endpoint Security for Windows, fare riferimento alla sezione Cloud Discovery della Guida di Kaspersky Endpoint Security for Windows.

Per bloccare o consentire l'accesso a un servizio cloud utilizzando il widget:

1. Aprire il widget Cloud Discovery, quindi selezionare il servizio cloud richiesto.
2. Nel riquadro **I 10 dispositivi principali che utilizzano il servizio**, individuare il criterio o il profilo di sicurezza per cui si desidera bloccare o consentire il servizio.
3. Nella colonna **Stato di accesso nel criterio o nel profilo** della riga desiderata eseguire una delle seguenti operazioni:
   - Per bloccare il servizio, selezionare **Bloccato** nell'elenco a discesa.
   - Per consentire il servizio, selezionare **Consentito** nell'elenco a discesa.
4. Fare clic sul pulsante **Salva**.

L'accesso al servizio selezionato è bloccato o consentito per il criterio o il profilo di protezione.

Registrazione delle attività di Kaspersky Security Center Web Console

La registrazione delle attività di Kaspersky Security Center Web Console agevola l'individuazione delle cause di un malfunzionamento del software. Quando si contatta l'Assistenza tecnica Kaspersky per un malfunzionamento di Kaspersky Security Center Web Console, gli specialisti dell'Assistenza tecnica Kaspersky possono richiedere di inviare i file di log di Kaspersky Security Center Web Console. I file di log di Kaspersky Security Center Web Console sono archiviati nella cartella <cartella di installazione di Kaspersky Security Center Web Console>/logs per tutto il tempo per cui si utilizza l'applicazione. I file di log non vengono inviati automaticamente agli specialisti dell'Assistenza tecnica Kaspersky.

Per abilitare la registrazione delle attività di Kaspersky Security Center Web Console:

Selezionare la casella di controllo **Abilitare la registrazione delle attività di Kaspersky Security Center Web Console** nella finestra **Impostazioni di connessione di Kaspersky Security Center Web Console** dell'Installazione guidata di Kaspersky Security Center Web Console.

I file di log sono in formato di testo.

I nomi dei file di log sono nel formato logs-<nome componente>.<nome dispositivo>-<numero di revisione del file>.AAAA-MM-GG, dove:

- <nome componente> è il nome del componente di Kaspersky Security Center o il nome del plug-in di gestione di Kaspersky Security Center Web Console.
- <nome dispositivo> è il nome del dispositivo in cui è in esecuzione <nome componente>.
- <numero di revisione del file> è il numero del file di log creato per <nome componente> in esecuzione in <nome dispositivo>. In uno stesso giorno, possono essere creati diversi file di log per gli stessi <nome componente> e <nome dispositivo>. La dimensione massima di un file di log è di 50 megabyte (MB). Quando viene raggiunta la dimensione massima del file, viene creato un nuovo file di log. Un nuovo file di log <numero di revisione del file> viene incrementato di 1.
- AAAA, MM e GG sono l'anno, il mese e il giorno in cui è stato creato per la prima volta il log. All'inizio di un nuovo giorno viene creato un nuovo file di log.

Integrazione tra Kaspersky Security Center e altre soluzioni

Questa sezione descrive come configurare l'accesso da Kaspersky Security Center Web Console a un'altra applicazione Kaspersky, ad esempio Kaspersky Managed Detection and Response. Questa sezione descrive inoltre come configurare l'esportazione nei sistemi SIEM.

Stabilire una connessione in background

Per consentire a Kaspersky Security Center Web Console di eseguire le relative attività in background, è necessario stabilire una connessione in background tra Kaspersky Security Center Web Console e Administration Server. È possibile stabilire questa connessione solo se il proprio account dispone del diritto **Modifica elenchi di controllo degli accessi agli oggetti** dell'area funzionale **Caratteristiche generali: Autorizzazioni utente**.

Se si installa il plug-in di Kaspersky Endpoint Security for Windows 12.6 o se si aggiorna il plug-in di Kaspersky Endpoint Security for Windows da una versione precedente alla 11.7 e non è ancora stata stabilita una connessione in background, viene visualizzata una notifica per informare che è necessario stabilire una connessione in background. Sarà inoltre necessario concedere all'account di servizio i diritti dell'area funzionale **Caratteristiche generali**: **Operazioni in Administration Server**.

Per stabilire una connessione in background:

1. Nel menu principale, passare a **Impostazioni** → **Integrazione**.
2. Nella sezione **Integrazione**, spostare l'interruttore per stabilire una connessione in background nella posizione: **Connessione in background per l'integrazione Abilitato**.
3. Nella sezione **Abilita una connessione in background** aperta fare clic sul pulsante **OK**.

Viene stabilita la connessione in background tra Kaspersky Security Center Web Console e Administration Server. Administration Server crea un account per la connessione in background e questo account viene utilizzato come account di servizio per mantenere l'interazione tra Kaspersky Security Center e un'altra applicazione o soluzione Kaspersky. Il nome di questo account di servizio contiene il prefisso NWCSvcUser.

Administration Server cambia automaticamente la password dell'account di servizio ogni 30 giorni, per motivi di sicurezza. Non è possibile eliminare l'account di servizio manualmente. Administration Server elimina automaticamente questo account quando si disabilita una connessione tra servizi. Administration Server crea un singolo account di servizio per ogni Administration Console e assegna tutti gli account di servizio al gruppo di protezione con il nome ServiceNwcGroup. Administration Server crea automaticamente questo gruppo di protezione durante il processo di installazione di Kaspersky Security Center. Non è possibile eliminare questo gruppo di protezione manualmente.

Esportazione di eventi nei sistemi SIEM

Questa sezione descrive come configurare l'esportazione degli eventi nei sistemi SIEM.

Configurazione dell'esportazione di eventi nei sistemi SIEM

Kaspersky Security Center consente la configurazione con uno dei seguenti metodi: esportazione in qualsiasi sistema SIEM che utilizza il formato Syslog, esportazione in sistemi QRadar, Splunk, ArcSight SIEM che utilizzano i formati LEEF e CEF o esportazione di eventi in sistemi SIEM direttamente dal database di Kaspersky Security Center. Al termine di questo scenario, Administration Server invia automaticamente gli eventi al sistema SIEM.

Prerequisiti

Prima di avviare la configurazione dell'esportazione degli eventi in Kaspersky Security Center:

- Ulteriori informazioni sui metodi di esportazione degli eventi.
- Assicurarsi di disporre dei valori delle impostazioni di sistema.

> È possibile eseguire i passaggi di questo scenario in qualsiasi ordine.

Il processo di esportazione degli eventi nel sistema SIEM prevede i seguenti passaggi:

- **Configurazione del sistema SIEM per la ricezione di eventi da Kaspersky Security Center**

  Istruzioni dettagliate: Configurazione dell'esportazione di eventi in un sistema SIEM

- **Selezione degli eventi che si desidera esportare nel sistema SIEM:**

  Istruzioni dettagliate:

  - Administration Console: Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog, Contrassegno di eventi generici per l'esportazione nel formato Syslog
  - Kaspersky Security Center Web Console: Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog, Contrassegno di eventi generali per l'esportazione nel formato Syslog

- **Configurazione dell'esportazione degli eventi nel sistema SIEM utilizzando uno dei seguenti metodi:**

  - Utilizzo dei protocolli TCP, UDP o TLS su TCP.

    Istruzioni dettagliate:

- Administration Console: Configurazione dell'esportazione di eventi nei sistemi SIEM
- Kaspersky Security Center Web Console: Configurazione dell'esportazione di eventi nei sistemi SIEM

- Utilizzo dell'esportazione di eventi direttamente dal database di Kaspersky Security Center. È disponibile un set di visualizzazioni pubbliche nel database di Kaspersky Security Center. È possibile trovare la descrizione di queste visualizzazioni pubbliche nel documento klakdb.chm.

Risultati

Dopo aver configurato l'esportazione degli eventi nel sistema SIEM, è possibile visualizzare i risultati dell'esportazione se sono stati selezionati gli eventi da esportare.

Prima di iniziare

Durante la configurazione dell'esportazione automatica degli eventi in Kaspersky Security Center, è necessario specificare alcune impostazioni del sistema SIEM. È consigliabile verificare preventivamente queste impostazioni per la preparazione della configurazione di Kaspersky Security Center.

Per configurare l'invio automatico degli eventi in un sistema SIEM, è necessario conoscere le seguenti impostazioni:

- **Indirizzo server del sistema SIEM**

  L'indirizzo IP del server in cui è installato il sistema SIEM utilizzato attualmente. Verificare questo valore nelle impostazioni del sistema SIEM.

- **Porta server del sistema SIEM**

  Numero della porta utilizzato per stabilire la connessione tra Kaspersky Security Center e il server del sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center e nelle impostazioni del destinatario del sistema SIEM.

- **Protocollo**

  Protocollo utilizzato per il trasferimento dei messaggi da Kaspersky Security Center al sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center e nelle impostazioni del destinatario del sistema SIEM.

Informazioni sugli eventi in Kaspersky Security Center

Kaspersky Security Center consente di ricevere informazioni sugli eventi che si verificano durante l'esecuzione di Administration Server e delle applicazioni Kaspersky installate nei dispositivi gestiti. Le informazioni sugli eventi vengono salvate nel database di Administration Server. È possibile esportare queste informazioni in sistemi SIEM esterni. L'esportazione delle informazioni sugli eventi nei sistemi SIEM esterni consente agli amministratori dei sistemi SIEM di rispondere tempestivamente agli eventi del sistema di protezione che si verificano nei gruppi di amministrazione o dispositivi gestiti.

Tipi di evento

In Kaspersky Security Center sono disponibili i seguenti tipi di eventi:

- Eventi generici. Questi eventi si verificano in tutte le applicazioni Kaspersky gestite. Un esempio di evento generico è l'Epidemia di virus. Gli eventi generici hanno sintassi e semantica rigorosamente definite. Gli eventi generici vengono ad esempio utilizzati nei rapporti e nei dashboard.
- Eventi specifici delle applicazioni gestiti da Kaspersky. Ogni applicazione Kaspersky gestita dispone di uno specifico set di eventi.

Origini eventi

Gli eventi possono essere generati dalle seguenti applicazioni:

- Componenti di Kaspersky Security Center:
  - Administration Server
  - Network Agent
  - Server per dispositivi mobili MDM iOS
- Applicazioni Kaspersky gestite

  Per i dettagli sugli eventi generati dalle applicazioni gestite da Kaspersky, consultare la documentazione dell'applicazione corrispondente.

È possibile visualizzare l'elenco completo degli eventi che possono essere generati da un'applicazione nella scheda **Configurazione eventi** nel criterio dell'applicazione. Per l'Administration Server, è inoltre possibile visualizzare l'elenco degli eventi nelle proprietà dell'Administration Server.

Livello di importanza degli eventi

Ogni evento dispone di uno specifico livello di importanza. In base alle condizioni in cui si verifica, a un evento possono essere assegnati diversi livelli di importanza. Esistono quattro livelli di importanza degli eventi:

- Un *evento critico* è un evento che indica la presenza di un problema critico che può determinare una perdita dei dati, un malfunzionamento o un errore critico.
- Un *errore funzionale* è un evento che indica la presenza di un problema grave, un errore o un malfunzionamento che si è verificato durante l'esecuzione dell'applicazione o di una procedura.
- Un *avviso* è un evento che non è necessariamente grave, ma indica comunque un potenziale problema futuro. La maggior parte degli eventi viene designata come avviso se l'applicazione può essere ripristinata senza perdite di dati o funzionalità importanti dopo che si sono verificati tali eventi.
- Un *evento informativo* è un evento che si verifica allo scopo di segnalare il completamento di un'operazione, il corretto funzionamento dell'applicazione o il completamento di una procedura.

Ogni evento ha un periodo di archiviazione definito, durante il quale può essere visualizzato o modificato in Kaspersky Security Center. Alcuni eventi non vengono salvati nel database di Administration Server per impostazione predefinita, poiché il relativo periodo di archiviazione definito è pari a zero. Solo gli eventi che verranno memorizzati nel database di Administration Server per almeno un giorno possono essere esportati in sistemi esterni.

Informazioni sull'esportazione degli eventi

È possibile utilizzare l'esportazione degli eventi in sistemi centralizzati che gestiscono i problemi di protezione a livello tecnico e organizzativo, garantiscono servizi di monitoraggio della sicurezza e consolidano informazioni da diverse soluzioni. Si tratta di sistemi SIEM, che offrono analisi in tempo reale degli avvisi e degli eventi di protezione generati da applicazioni e hardware di rete o SOC (Security Operation Center).

Questi sistemi ricevono i dati da numerose origini, tra cui reti, sicurezza, server, database e applicazioni. I sistemi SIEM forniscono anche funzionalità per consolidare i dati monitorati ed evitare la perdita di eventi critici. Inoltre, questi sistemi eseguono analisi automatizzate di avvisi ed eventi correlati per inviare immediatamente agli amministratori una notifica dei problemi di protezione. Gli avvisi possono essere implementati tramite un dashboard o inviati tramite canali di terzi, ad esempio via e-mail.

Il processo di esportazione degli eventi da Kaspersky Security Center ai sistemi SIEM esterni coinvolge due parti: un mittente degli eventi (Kaspersky Security Center) e il destinatario di un evento (il sistema SIEM). Per eseguire l'esportazione degli eventi, è necessario configurare questa funzionalità nel sistema SIEM e in Kaspersky Security Center. Non è importante quale lato viene configurato per primo. È possibile configurare la trasmissione degli eventi in Kaspersky Security Center, quindi configurare la ricezione degli eventi dal sistema SIEM o viceversa.

Metodi per l'invio degli eventi da Kaspersky Security Center

Esistono tre metodi per l'invio degli eventi da Kaspersky Security Center ai sistemi esterni:

- Invio degli eventi tramite il protocollo Syslog a qualsiasi sistema SIEM

  Utilizzando il protocollo Syslog è possibile inviare gli eventi che si verificano in Kaspersky Security Center Administration Server e nelle applicazioni Kaspersky installate nei dispositivi gestiti. Il protocollo Syslog è un protocollo standard per la registrazione dei messaggi. Può essere utilizzato per esportare gli eventi in qualsiasi sistema SIEM.

  A tale scopo, è necessario contrassegnare gli eventi che si desidera inoltrare al sistema SIEM. È possibile contrassegnare gli eventi in Administration Console o Kaspersky Security Center Web Console. Solo gli eventi contrassegnati verranno inoltrati al sistema SIEM. Se non è stato contrassegnato nulla, nessun evento verrà inoltrato.

- Invio degli eventi tramite i protocolli CEF e LEEF ai sistemi QRadar, Splunk e ArcSight

  È possibile utilizzare i protocolli CEF e LEEF per esportare eventi generali. Durante l'esportazione degli eventi tramite i protocolli CEF e LEEF, non si ha la possibilità di selezionare gli eventi specifici da esportare. Al contrario, vengono esportati tutti gli eventi generali. Per convertire gli eventi Kaspersky Security Center in eventi nei formati CEF e LEEF, è necessario utilizzare il file siem_conversion_rules.xml. Questo file contiene l'elenco degli attributi degli eventi Kaspersky Security Center e gli attributi corrispondenti degli eventi nei formati CEF e LEEF. Inoltre, il file siem_conversion_rules.xml contiene le regole per generare messaggi corrispondenti agli eventi. Questo file è incluso nel kit di distribuzione di Kaspersky Security Center.

  A differenza del protocollo Syslog, i protocolli CEF e LEEF non sono universali. I protocolli CEF e LEEF sono destinati ai sistemi SIEM appropriati (QRadar, Splunk e ArcSight). Di conseguenza, quando si sceglie di esportare gli eventi in uno di questi protocolli, utilizzare il parser richiesto per il sistema SIEM.

- Direttamente dal database di Kaspersky Security Center in qualsiasi sistema SIEM

  Questo metodo di esportazione degli eventi può essere utilizzato per ricevere gli eventi direttamente da visualizzazioni pubbliche del database tramite query SQL. I risultati di una query vengono salvati in un file XML che può essere utilizzato come input dei dati per un sistema esterno. Solo gli eventi disponibili nelle visualizzazioni pubbliche possono essere esportati direttamente dal database.

Ricezione degli eventi da parte del sistema SIEM

Il sistema SIEM deve ricevere e analizzare correttamente gli eventi ricevuti da Kaspersky Security Center. A tale scopo, è necessario configurare correttamente il sistema SIEM. La configurazione dipende dallo specifico sistema SIEM in uso. Sono comunque previsti diversi passaggi generali per la configurazione di tutti i sistemi SIEM, ad esempio la configurazione del ricevitore e del parser.

Informazioni sulla configurazione dell'esportazione di eventi in un sistema SIEM

Il processo di esportazione degli eventi da Kaspersky Security Center ai sistemi SIEM esterni coinvolge due parti: un mittente degli eventi (Kaspersky Security Center) e il destinatario di un evento (il sistema SIEM). È necessario configurare l'esportazione degli eventi nel sistema SIEM e in Kaspersky Security Center.

Le impostazioni specificate nel sistema SIEM dipendono dal particolare sistema in uso. In genere, per tutti i sistemi SIEM è necessario impostare un ricevitore ed eventualmente un parser dei messaggi per l'analisi degli eventi ricevuti.

Configurazione del ricevitore

Per la ricezione degli eventi inviati da Kaspersky Security Center, è necessario impostare il ricevitore nel sistema SIEM. In generale, le seguenti impostazioni devono essere specificate nel sistema SIEM:

- **Protocollo di esportazione o tipo di input**

  È il protocollo di trasferimento dei messaggi, ad esempio UDP. Il protocollo deve corrispondere al protocollo specificato in Kaspersky Security Center.

- **Porta**

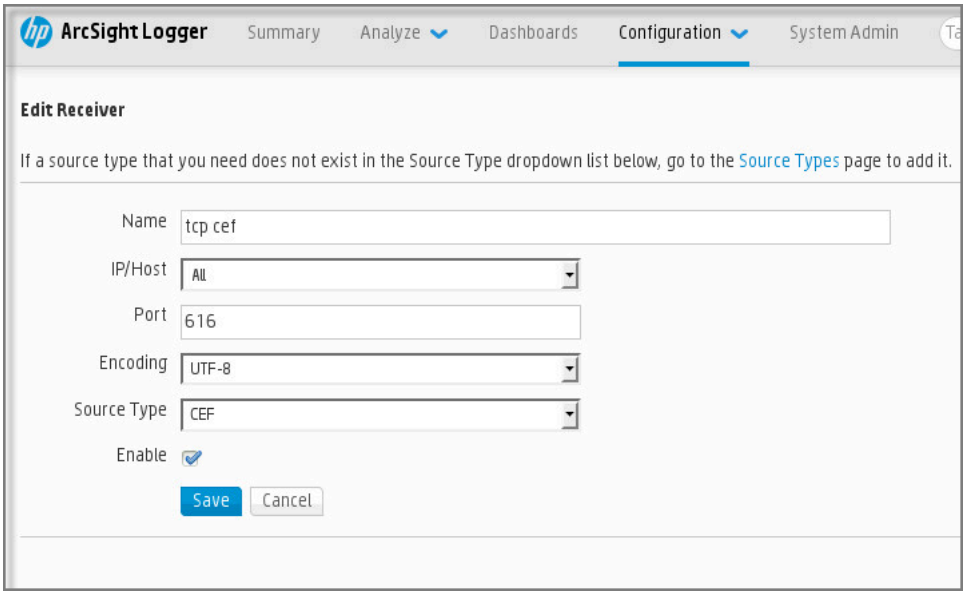
  Numero di porta per la connessione a Kaspersky Security Center. Questa porta deve corrispondere alla porta specificata in Kaspersky Security Center.

- **Protocollo dei messaggi o tipo di origine**

  Protocollo utilizzato per esportare gli eventi nel sistema SIEM. Può essere uno dei protocolli standard: Syslog, CEF o LEEF. Il sistema SIEM seleziona il parser dei messaggi in base al protocollo specificato.

A seconda del sistema SIEM in uso, potrebbe essere necessario specificare alcune impostazioni aggiuntive del ricevitore.

La figura seguente mostra la schermata di configurazione del ricevitore in ArcSight.



Configurazione del ricevitore in ArcSight

Parser dei messaggi

Gli eventi esportati vengono inviati ai sistemi SIEM come messaggi. Questi messaggi devono essere analizzati correttamente per consentire l'utilizzo delle informazioni sugli eventi nel sistema SIEM. I parser dei messaggi fanno parte del sistema SIEM: vengono utilizzati per suddividere il contenuto del messaggio nei campi appropriati, ad esempio l'ID degli eventi, il livello di criticità, la descrizione, i parametri. Questo consente al sistema SIEM di elaborare gli eventi ricevuti da Kaspersky Security Center in modo che possano essere memorizzati nel database del sistema SIEM.

Contrassegno degli eventi per l'esportazione nei sistemi SIEM in formato Syslog

Dopo aver abilitato l'esportazione automatica degli eventi, è necessario selezionare gli eventi da esportare nel sistema SIEM esterno.

È possibile configurare l'esportazione degli eventi in formato Syslog in un sistema esterno in base alle seguenti condizioni:

- Contrassegno di eventi generali. Se si contrassegnano gli eventi da esportare in un criterio, nelle impostazioni di un evento o nelle impostazioni di Administration Server, il sistema SIEM riceverà gli eventi contrassegnati che si sono verificati in tutte le applicazioni gestite dal criterio specifico. Se sono stati selezionati eventi esportati nel criterio, non sarà possibile ridefinirli per una singola applicazione gestita da questo criterio.

- Contrassegno degli eventi per un'applicazione gestita. Se si contrassegnano gli eventi da esportare per un'applicazione gestita installata in un dispositivo gestito, il sistema SIEM riceverà solo gli eventi che si sono verificati nell'applicazione.

Informazioni sul contrassegno degli eventi per l'esportazione nel sistema SIEM in formato Syslog

Dopo aver abilitato l'esportazione automatica degli eventi, è necessario selezionare gli eventi da esportare nel sistema SIEM esterno.

È possibile configurare l'esportazione degli eventi in formato Syslog in un sistema esterno in base alle seguenti condizioni:

- Contrassegno di eventi generali. Se si contrassegnano gli eventi da esportare in un criterio, nelle impostazioni di un evento o nelle impostazioni di Administration Server, il sistema SIEM riceverà gli eventi contrassegnati che si sono verificati in tutte le applicazioni gestite dal criterio specifico. Se sono stati selezionati eventi esportati nel criterio, non sarà possibile ridefinirli per una singola applicazione gestita da questo criterio.

- Contrassegno degli eventi per un'applicazione gestita. Se si contrassegnano gli eventi da esportare per un'applicazione gestita installata in un dispositivo gestito, il sistema SIEM riceverà solo gli eventi che si sono verificati nell'applicazione.

Contrassegno degli eventi di un'applicazione Kaspersky per l'esportazione nel formato Syslog

Se si desidera esportare gli eventi che si sono verificati in un'applicazione gestita specifica installata nei dispositivi gestiti, contrassegnare gli eventi per l'esportazione nel criterio dell'applicazione. In questo caso, gli eventi contrassegnati vengono esportati da tutti i dispositivi inclusi nell'ambito del criterio.

Per contrassegnare gli eventi per l'esportazione per una singola applicazione gestita:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Criteri e profili**.

2. Fare clic sul criterio dell'applicazione per cui si desidera contrassegnare gli eventi.

   Verrà visualizzata la finestra delle impostazioni del criterio.

3. Accedere alla sezione **Configurazione eventi**.
4. Selezionare le caselle di controllo accanto agli eventi che si desidera esportare in un sistema SIEM.
5. Fare clic sul pulsante **Contrassegna per l'esportazione nel sistema SIEM utilizzando Syslog**.

   È inoltre possibile contrassegnare un evento per l'esportazione nel sistema SIEM nella sezione **Registrazione eventi** visualizzata facendo clic sul collegamento dell'evento.

6. Un segno di spunta (✓) viene visualizzato nella colonna **Syslog** dell'evento o degli eventi contrassegnati per l'esportazione nel sistema SIEM.
7. Fare clic sul pulsante **Salva**.

Gli eventi contrassegnati dell'applicazione gestita sono pronti per l'esportazione in un sistema SIEM.

È possibile contrassegnare quali eventi esportare in un sistema SIEM per un dispositivo gestito specifico. Se sono stati contrassegnati eventi esportati in precedenza in un criterio dell'applicazione, non sarà possibile ridefinire gli eventi contrassegnati per un singolo dispositivo gestito.

Per contrassegnare gli eventi per l'esportazione per un dispositivo gestito:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   Verrà visualizzato l'elenco dei dispositivi gestiti.
2. Fare clic sul collegamento con il nome del dispositivo desiderato nell'elenco dei dispositivi gestiti.

   Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.
3. Accedere alla sezione **Applicazioni**.
4. Fare clic sul collegamento con il nome dell'applicazione desiderata nell'elenco delle applicazioni.
5. Accedere alla sezione **Configurazione eventi**.
6. Selezionare le caselle di controllo accanto agli eventi che si desidera esportare in SIEM.
7. Fare clic sul pulsante **Contrassegna per l'esportazione nel sistema SIEM utilizzando Syslog**.

   È inoltre possibile contrassegnare un evento per l'esportazione nel sistema SIEM nella sezione **Registrazione eventi** visualizzata facendo clic sul collegamento dell'evento.

8. Un segno di spunta (✓) viene visualizzato nella colonna **Syslog** dell'evento o degli eventi contrassegnati per l'esportazione nel sistema SIEM.

D'ora in poi, Administration Server invia gli eventi contrassegnati al sistema SIEM se è configurata l'esportazione nel sistema SIEM.

Contrassegno di eventi generici per l'esportazione nel formato Syslog

È possibile contrassegnare gli eventi generici che Administration Server esporterà nei sistemi SIEM utilizzando il formato Syslog.

Per contrassegnare eventi generici per l'esportazione in un sistema SIEM:

1. Eseguire una delle seguenti operazioni:

   - Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   - Nel menu principale, passare a **Risorse (dispositivi)** → **Criteri e profili**, quindi fare clic sul collegamento di un criterio.

2. Nella finestra visualizzata accedere alla scheda **Configurazione eventi**.

3. Fare clic su **Contrassegna per l'esportazione nel sistema SIEM utilizzando Syslog**.

   È inoltre possibile contrassegnare un evento per l'esportazione nel sistema SIEM nella sezione **Registrazione eventi** visualizzata facendo clic sul collegamento dell'evento.

4. Un segno di spunta ( ) viene visualizzato nella colonna **Syslog** dell'evento o degli eventi contrassegnati per l'esportazione nel sistema SIEM.

D'ora in poi, Administration Server invia gli eventi contrassegnati al sistema SIEM se è configurata l'esportazione nel sistema SIEM.

Informazioni sull'esportazione degli eventi tramite i formati CEF e LEEF

È possibile utilizzare i formati CEF e LEEF per esportare nei sistemi SIEM gli eventi generali, nonché gli eventi trasferiti dalle applicazioni Kaspersky ad Administration Server. Il set di eventi per l'esportazione è predefinito e non è possibile selezionare gli eventi da esportare. Prima di inviare eventi al sistema SIEM (QRadar, ArcSight o Splunk), è necessario interpretare gli eventi Kaspersky Security Center in eventi in formato CEF e LEEF utilizzando le regole specificate nel file siem_conversion_rules.xml.

Selezionare il formato di esportazione in base al sistema SIEM in uso. Nella tabella seguente sono elencati i sistemi SIEM e i formati di esportazione corrispondenti.

Formati di esportazione degli eventi in un sistema SIEM

Sistema SIEM	Formato di esportazione
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Log Event Extended Format) - un formato di eventi personalizzato per IBM Security QRadar SIEM. QRadar può integrare, identificare ed elaborare gli eventi LEEF. Gli eventi LEEF devono utilizzare la codifica dei caratteri UTF-8. Informazioni dettagliate sul protocollo LEEF sono disponibili in IBM Knowledge Center.

- CEF (Common Event Format) è uno standard aperto per la gestione dei registri che migliora l'interoperabilità delle informazioni relative alla sicurezza ottenute da diversi dispositivi e applicazioni di rete e di protezione. CEF consente di utilizzare un formato comune per il registro eventi, permettendo di integrare e aggregare facilmente i dati per l'analisi da un sistema di gestione aziendale. Gli eventi CEF devono utilizzare la codifica dei caratteri UTF-8.

L'esportazione automatica significa che Kaspersky Security Center invii gli eventi generali al sistema SIEM. L'esportazione automatica degli eventi viene avviata subito dopo essere stata abilitata. In questa sezione viene descritto in dettaglio come abilitare l'esportazione automatica degli eventi.

Conversione degli eventi nel formato CEF o LEEF

Prima di inviare eventi al sistema SIEM (QRadar, ArcSight o Splunk), è necessario interpretare gli eventi Kaspersky Security Center in eventi in formato CEF e LEEF utilizzando le regole specificate nel file siem_conversion_rules.xml. Questo file è incluso nel kit di distribuzione di Kaspersky Security Center.

Il file siem_conversion_rules.xml contiene le regole di interpretazione predefinite per convertire gli eventi nei formati CEF e LEEF. Se si desidera utilizzare ulteriori regole di interpretazione degli eventi, è possibile aggiungerle manualmente al file.

Il file siem_conversion_rules.xml include le sezioni `<product name="SP_QRADAR" vendor="IBM">` e `<product name="SP_QRADAR" vendor="IBM">`. La sezione `<product name="SP_QRADAR" vendor="IBM">` contiene regole per la generazione degli eventi nel formato LEEF, che possono essere esportate nel sistema QRadar SIEM. La sezione `<product name="SP_ARCSIGHT" vendor="HP">` contiene regole per la generazione degli eventi nel formato CEF, che può essere esportato nel sistema ArcSight o Splunk SIEM.

Ogni sezione dispone della sottosezione `<common>` in cui si trovano gli attributi degli eventi Kaspersky Security Center e gli attributi corrispondenti degli eventi nel formato LEEF. Questi attributi comuni vengono utilizzati per tutti i tipi di eventi che possono essere esportati.

Inoltre, ogni sezione dispone delle sottosezioni `<event>`. Ogni sottosezione `<event>` contiene attributi aggiuntivi aggiunti a questi elenchi nella sezione `<common>`.

È possibile aggiungere manualmente una nuova regola di generazione eventi al file siem_conversion_rules.xml.

Per aggiungere una nuova regola di generazione degli eventi:

1. Aggiungere una nuova sottosezione `<event>` alla sezione `<product name="SP_QRADAR" vendor="IBM">` o `<product name="SP_QRADAR" vendor="IBM">`, quindi specificare gli attributi degli eventi aggiuntivi, se necessario.

2. Se un evento è costituito solo da attributi comuni, la sottosezione `<event>` sarà vuota.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Attributi degli eventi comuni Kaspersky Security Center e attributi degli eventi LEEF
corrispondenti -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="EVC_EV_DISP_HOST_NAME" type="AT_STRING" limit="255"/>
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND"> <!-- Regola di generazione per l'evento GNRL_EV_VIRUS_FOUND con attributi
aggiuntivi -->
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="EVC_EV_SHA256" type="AT_STRING" limit="255"/>
            </param>
            ...
        </event>
...
</product>
    <product name="SP_ARCSIGHT" vendor="HP">
        <common> <!-- Attributi degli eventi comuni Kaspersky Security Center e attributi degli eventi LEEF
corrispondenti -->
            <param name="KLSPLG_HOST_DISP_NAME" type="STRING_T">
                <attr name="dhost" type="AT_STRING" limit="1023"/>
```

```
            </param>
            ...
        </common>
        <event id="GNRL_EV_VIRUS_FOUND">
            <param name="GNRL_EA_PARAM_1" type="STRING_T">
                <attr name="cs4" type="AT_STRING" limit="255"/>
                <attr name="cs4Label" type="AT_STRING" val="SHA256"/>
            </param>
            ...
</product>
</conversion_rules>
```

Informazioni sull'esportazione degli eventi utilizzando il formato Syslog

È possibile utilizzare il formato Syslog per esportare nei sistemi SIEM gli eventi che si verificano in Administration Server e in altre applicazioni Kaspersky installate nei dispositivi gestiti.

Syslog è un protocollo standard per la registrazione dei messaggi. Consente una separazione tra il software che genera i messaggi, il sistema che li archivia e il software che li segnala e li analizza. Ogni messaggio dispone di un codice che indica il tipo di software che ha generato il messaggio e di un livello di criticità.

Il formato Syslog è definito dai documenti RFC (Request for Comments) pubblicati da Internet Engineering Task Force (standard Internet). Per l'esportazione degli eventi da Kaspersky Security Center nei sistemi esterni viene utilizzato lo standard RFC 5424.

In Kaspersky Security Center è possibile configurare l'esportazione degli eventi per i sistemi esterni tramite il formato Syslog.

Il processo di esportazione comprende due passaggi:

1. Abilitazione dell'esportazione automatica degli eventi. In questo passaggio Kaspersky Security Center viene configurato in modo da inviare gli eventi al sistema SIEM. Kaspersky Security Center inizia a inviare gli eventi subito dopo l'abilitazione dell'esportazione automatica.

2. Selezione degli eventi da esportare nel sistema esterno. In questo passaggio è possibile selezionare gli eventi da esportare nel sistema SIEM.

Configurazione di Kaspersky Security Center per l'esportazione degli eventi nel sistema SIEM

Per esportare gli eventi nel sistema SIEM, è necessario configurare il processo di esportazione in Kaspersky Security Center Web Console.

Prima di inviare eventi al sistema SIEM (QRadar, ArcSight o Splunk), è necessario interpretare gli eventi Kaspersky Security Center in eventi in formato CEF e LEEF utilizzando le regole specificate nel file siem_conversion_rules.xml.

Per configurare l'esportazione nei sistemi SIEM in Kaspersky Security Center Web Console:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale**, selezionare la sezione **Esporta in SIEM**.

3. Fare clic sul collegamento **Impostazioni**.

   Si aprirà la sezione **Esporta impostazioni**.

4. Specificare le impostazioni nella sezione **Esporta impostazioni**:

- **Indirizzo server del sistema SIEM**

  L'indirizzo IP del server in cui è installato il sistema SIEM utilizzato attualmente. Verificare questo valore nelle impostazioni del sistema SIEM.

- **Porta del sistema SIEM**

  Numero della porta utilizzato per stabilire la connessione tra Kaspersky Security Center e il server del sistema SIEM. Questo valore viene specificato nelle impostazioni di Kaspersky Security Center e nelle impostazioni del destinatario del sistema SIEM.

- **Protocollo**

Selezionare il protocollo da utilizzare per il trasferimento dei messaggi al sistema SIEM. È possibile selezionare il protocollo TCP, UDP o TLS su TCP.

Specificare le seguenti impostazioni TLS se si seleziona il protocollo TLS su TCP:

- **Autenticazione server**

  Nel campo **Autenticazione server**, è possibile selezionare i valori **Certificati affidabili** o **Impronte digitali SHA**:

  - **Certificati affidabili**. È possibile ricevere una catena di certificati completa (incluso il certificato root) da un'autorità di certificazione (CA) attendibile e caricare il file in Kaspersky Security Center. Kaspersky Security Center verifica se anche la catena di certificati del server di sistema SIEM è firmata da un'autorità di certificazione attendibile o meno.

    Per aggiungere un certificato attendibile, fare clic sul pulsante **Cerca il file dei certificati CA**, quindi caricare il certificato.

  - **Impronte digitali SHA**. È possibile specificare le identificazioni personali SHA1 dell'intera catena di certificati del sistema SIEM (incluso il certificato root) in Kaspersky Security Center. Per aggiungere un'identificazione personale SHA1, immetterla nel campo **Identificazioni personali**, quindi fare clic sul pulsante **Aggiungi**.

  Utilizzando l'impostazione **Aggiungi autenticazione client**, è possibile generare un certificato per autenticare Kaspersky Security Center. Pertanto, verrà utilizzato un certificato autofirmato emesso da Kaspersky Security Center. In questo caso, è possibile utilizzare sia un certificato attendibile che un'impronta digitale SHA per autenticare il server di sistema SIEM.

- **Aggiungi nome soggetto/nome alternativo soggetto**

  Il nome del soggetto è un nome di dominio per il quale viene ricevuto il certificato. Kaspersky Security Center non può connettersi al server di sistema SIEM se il nome di dominio del server di sistema SIEM non corrisponde al nome del soggetto del certificato del server di sistema SIEM. Tuttavia, il server di sistema SIEM può modificare il proprio nome di dominio se il nome è stato modificato nel certificato. In questo caso, è possibile specificare i nomi dei soggetti nel campo **Aggiungi nome soggetto/nome alternativo soggetto**. Se uno dei nomi dei soggetti specificati corrisponde al nome del soggetto del certificato di sistema SIEM, Kaspersky Security Center convalida il certificato del server di sistema SIEM.

- **Aggiungi autenticazione client**

  Per l'autenticazione del client, è possibile inserire il certificato o generarlo in Kaspersky Security Center.

  - **Inserire il certificato**. È possibile utilizzare un certificato ricevuto da qualsiasi origine, ad esempio da qualsiasi autorità di certificazione attendibile. È necessario specificare il certificato e la relativa chiave privata utilizzando uno dei seguenti tipi di certificato:

    - **Certificato X.509 PEM**. Caricare un file con un certificato nel campo **File con certificato** e un file con una chiave privata nel campo **File con la chiave**. Entrambi i file non dipendono l'uno dall'altro e l'ordine di caricamento dei file non è significativo. Quando entrambi i file sono stati caricati, specificare la password per la decodifica della chiave privata nel campo **Verifica password o certificato**. La password può avere un valore vuoto se la chiave privata non è codificata.

    - **Certificato X.509 PKCS12**. Caricare un singolo file che contenga un certificato e la relativa chiave privata nel campo **File con certificato**. Quando il file viene caricato, specificare la password per la decodifica della chiave privata nel campo **Verifica password o certificato**. La password può avere un valore vuoto se la chiave privata non è codificata.

- **Genera chiave**. È possibile generare un certificato autofirmato in Kaspersky Security Center. Di conseguenza, Kaspersky Security Center archivia il certificato autofirmato generato ed è possibile passare la parte pubblica del certificato o l'impronta digitale SHA1 al sistema SIEM.

- Formato dei dati

  È possibile selezionare i formati del registro di sistema, CEF o LEEF, a seconda dei requisiti del sistema SIEM.

  Se si seleziona il formato dati del registro di sistema, è necessario specificare:

- Dimensioni massime messaggi, in byte

  Specificare la dimensione massima (in byte) di un messaggio inviato al sistema SIEM. Ciascun evento viene inviato in un messaggio. Se la durata effettiva di un messaggio è superiore al valore specificato, il messaggio viene troncato e può verificarsi una perdita di dati. Le dimensioni predefinite sono 2048 byte. Questo campo è disponibile solo se è stato selezionato il formato del registro di sistema nel campo **Protocollo**.

5. Facoltativamente è possibile esportare gli eventi archiviati dal database di Administration Server e impostare la data di inizio da cui si desidera avviare l'esportazione degli eventi archiviati:

   a. Fare clic sul collegamento **Impostare la data di inizio dell'esportazione**.

   b. Nella sezione visualizzata, specificare la data di inizio nel campo **Data di inizio dell'esportazione degli eventi di sistema**.

   c. Fare clic sul pulsante **OK**.

6. Spostare l'opzione sulla posizione **Esporta automaticamente gli eventi nel database del sistema SIEM Abilitato**.

7. Per verificare che la connessione al sistema SIEM sia configurata correttamente, fare clic sul pulsante **Verifica connessione**.

   Viene stabilita la connessione con il server del sistema SIEM e viene inviato un evento di prova. Verrà visualizzato lo stato della connessione.

   Il controllo viene eseguito solo per i protocolli TCP e TLS su TCP.

8. Fare clic sul pulsante **Salva**.

L'esportazione nel sistema SIEM è configurata.

Esportazione degli eventi direttamente dal database

È possibile recuperare gli eventi direttamente dal database di Kaspersky Security Center senza dover utilizzare l'interfaccia di Kaspersky Security Center. È possibile eseguire direttamente le query sulle visualizzazioni pubbliche e recuperare i dati degli eventi o creare le proprie visualizzazioni sulla base delle visualizzazioni pubbliche esistenti e configurarle in modo che recuperino i dati necessari.

Visualizzazioni pubbliche

Per maggiore praticità, è disponibile un set di visualizzazioni pubbliche nel database di Kaspersky Security Center. È possibile trovare la descrizione di queste visualizzazioni pubbliche nel documento klakdb.chm.

La visualizzazione pubblica v_akpub_ev_event contiene un set di campi che rappresentano i parametri degli eventi nel database. Nel documento klakdb.chm è inoltre possibile trovare informazioni sulle visualizzazioni pubbliche che corrispondono ad altre entità di Kaspersky Security Center, ad esempio dispositivi, applicazioni o utenti. È possibile utilizzare queste informazioni nelle query.

Questa sezione contiene le istruzioni per l'esecuzione di una query SQL tramite l'utilità klsql2 e un esempio di query.

Per creare query SQL o visualizzazioni di database, è anche possibile utilizzare qualsiasi altro programma per l'utilizzo dei database. Le informazioni su come visualizzare i parametri per la connessione al database di Kaspersky Security Center, ad esempio il nome istanza e il nome database, sono indicate nella sezione corrispondente.

Esecuzione di una query SQL tramite l'utilità klsql2

Questo articolo descrive come scaricare e utilizzare l'utilità klsql2 e come eseguire una query SQL utilizzando questa utilità.

Per utilizzare l'utilità klsql2:

1. Individuare l'utilità klsql2 nella cartella di installazione di Kaspersky Security Center. Il percorso di installazione predefinito è <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center. Non utilizzare le versioni dell'utilità klsql2 destinate alle versioni precedenti di Kaspersky Security Center.

2. Creare un file con l'estensione .sql in qualsiasi editor di testo e posizionare il file nella stessa cartella con l'utilità.

3. Nel file .sql creato, digitare la query SQL desiderata e salvare il file.

4. Nel dispositivo in cui è installato Kaspersky Security Center Administration Server digitare nella riga di comando il seguente comando per eseguire la query SQL dal file .sql e salvare i risultati nel file result.xml:
   ```
   klsql2 -i src.sql -u <nome utente> -p <password> -o result.xml
   ```
   dove `<nome utente>` e `<password>` sono le credenziali dell'account utente che ha accesso al database.

5. Se richiesto, inserire account utente e password dell'account utente che ha accesso al database.

6. Aprire i file result.xml creati per visualizzare i risultati della query SQL.

È possibile modificare il file .sql e creare qualsiasi query SQL sulle visualizzazioni pubbliche. Eseguire la query SQL dalla riga di comando e salvare i risultati in un file.

Esempio di una query SQL nell'utilità klsql2

Questa sezione fornisce un esempio di query SQL, eseguita tramite l'utilità klsql2.

I seguenti esempi illustrano il recupero degli eventi che si sono verificati nei dispositivi negli ultimi sette giorni e la visualizzazione degli eventi ordinati in base all'ora in cui si sono verificati. Gli eventi più recenti vengono visualizzati per primi.

Esempio per Microsoft SQL Server:

```
SELECT
  /* identificatore dell'evento */
  e.nId,

  /* ora in cui si è verificato l'evento */
  e.tmRiseTime,

  /* nome interno del tipo di evento */
  e.strEventType,

  /* nome visualizzato dell'evento */
  e.wstrEventTypeDisplayName,

  /* descrizione visualizzata dell'evento */
  e.wstrDescription,

  /* nome del gruppo a cui appartiene il dispositivo */
  e.wstrGroupName,

  /* nome visualizzato del dispositivo in cui si è verificato l'evento */
  h.wstrDisplayName,
  CAST(((h.nIp / 16777216) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 65536) & 255) AS varchar(4)) + '.' +
  CAST(((h.nIp / 256) & 255) AS varchar(4)) + '.' +

  /* indirizzo IP del dispositivo, in cui si è verificato l'evento */
  CAST(((h.nIp) & 255) AS varchar(4)) as strIp
FROM v_akpub_ev_event e
  INNER JOIN v_akpub_host h ON h.nId=e.nHostId
WHERE e.tmRiseTime>=DATEADD(Day, -7, GETUTCDATE())
ORDER BY e.tmRiseTime DESC
```

Esempio per PostgreSQL:

```
SELECT
  /* identificatore dell'evento */
  "e"."nId",

  /* ora in cui si è verificato l'evento */
  "e"."tmRiseTime",

  /* nome interno del tipo di eventoe */
  "e"."strEventType",

  /* nome visualizzato dell'evento*/
  "e"."wstrEventTypeDisplayName",

  /* descrizione visualizzata dell'evento */
  "e"."wstrDescription",

  /* descrizione visualizzata dell'evento */
  "e"."wstrGroupName",

  /* nome visualizzato del dispositivo in cui si è verificato l'evento */
  "h"."wstrDisplayName",
  (
    CAST((("h"."nIp" / 16777216 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 65536 )& 255 ) AS VARCHAR(4))  || '.'  ||
    CAST((("h"."nIp" / 256 )& 255 ) AS VARCHAR(4))  || '.'  ||

    /* indirizzo IP del dispositivo, in cui si è verificato l'evento */
    CAST((("h"."nIp" )& 255 ) AS VARCHAR(4))
  )  AS "strIp"
FROM "v_akpub_ev_event"  AS "e"
  INNER JOIN  "v_akpub_host"  AS "h" ON "h"."nId" = "e"."nHostId"
WHERE "e"."tmRiseTime" >= NOW() AT TIME ZONE 'utc'  + make_interval(days => CAST(-7  AS INT))
ORDER BY "e"."tmRiseTime" DESC ;
```

Esempio per MySQL o MariaDB:

```
SELECT

  /* identificatore dell'evento */
  `e`.`nId`,

  /* ora in cui si è verificato l'evento */
  `e`.`tmRiseTime`,

  /* nome interno del tipo di eventoe */
  `e`.`strEventType`,

  /* nome visualizzato dell'evento */
  `e`.`wstrEventTypeDisplayName`,

  /* descrizione visualizzata dell'evento */
  `e`.`wstrDescription`,

  /* nome del gruppo di dispositivi */
  `e`.`wstrGroupName`,

  /* nome visualizzato del dispositivo in cui si è verificato l'evento */
  `h`.`wstrDisplayName`,
  CONCAT(
    LEFT(CAST(((`h`.`nIp`  DIV  1677721) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  65536) & 255) AS CHAR), 4), '.',
    LEFT(CAST(((`h`.`nIp`  DIV  256) & 255) AS CHAR), 4), '.',

    /* indirizzo IP del dispositivo, in cui si è verificato l'evento */
    LEFT(CAST(((`h`.`nIp`) & 255) AS CHAR), 4)
  )  AS `strIp`
FROM `v_akpub_ev_event`  AS `e`
  INNER JOIN  `v_akpub_host`  AS `h` ON `h`.`nId` = `e`.`nHostId`
WHERE `e`.`tmRiseTime` >= ADDDATE( UTC_TIMESTAMP( ) , INTERVAL -7  DAY)
ORDER BY `e`.`tmRiseTime` DESC ;
```

Visualizzazione del nome del database di Kaspersky Security Center

Se si desidera accedere al database di Kaspersky Security Center tramite gli strumenti di gestione database SQL Server, MySQL o MariaDB, è necessario conoscere il nome del database per connettersi dall'editor degli script SQL.

Per visualizzare il nome del database di Kaspersky Security Center:

1. Nel menu principale, fare clic sull'icona delle impostazioni ( ) accanto al nome dell'Administration Server richiesto.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale**, selezionare la sezione **Dettagli del database corrente**.

Il nome del database è specificato nel campo **Nome database**. Utilizzare il nome del database per fare riferimento al database nelle query SQL.

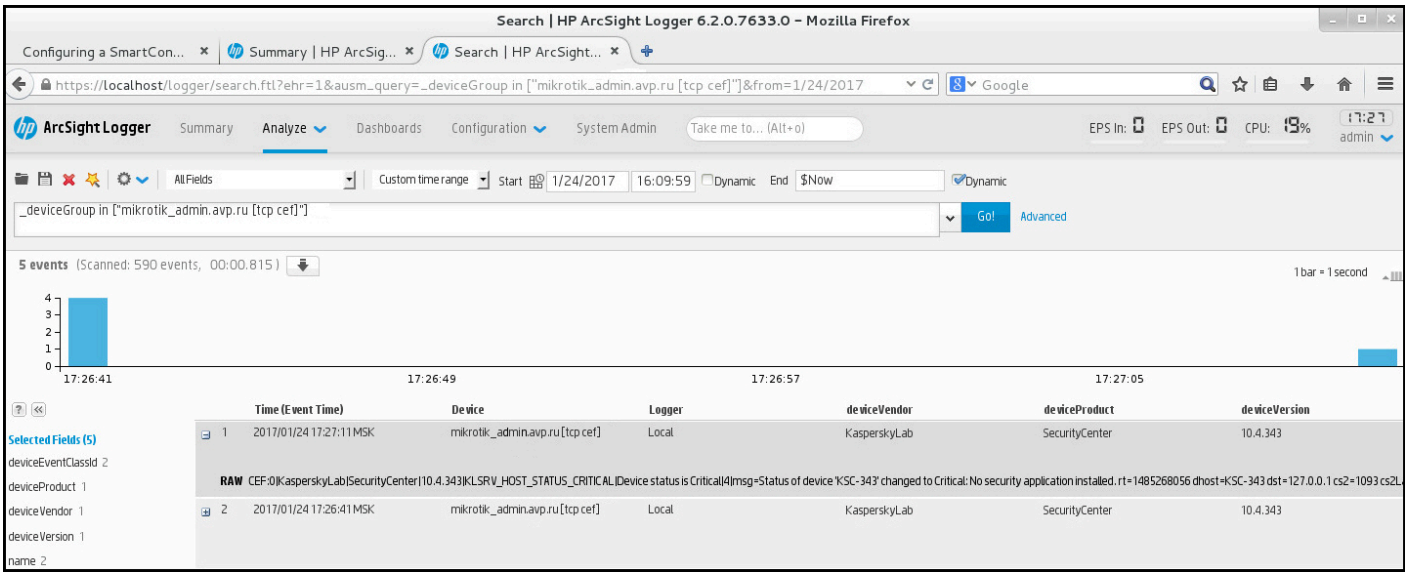
Visualizzazione dei risultati dell'esportazione

È possibile controllare il completamento della procedura di esportazione degli eventi. A tale scopo, controllare se i messaggi con gli eventi esportati vengono ricevuti dal sistema SIEM.

Se gli eventi inviati da Kaspersky Security Center vengono ricevuti e analizzati correttamente dal sistema SIEM, la configurazione su entrambi i lati è stata eseguita correttamente. In caso contrario, controllare le impostazioni specificate in Kaspersky Security Center rispetto alla configurazione del sistema SIEM.

La figura seguente illustra gli eventi esportati in ArcSight. Ad esempio, il primo evento è un evento critico di Administration Server: "*Lo stato del dispositivo è Critico*".

La rappresentazione degli eventi esportati nel sistema SIEM varia in base al sistema SIEM in uso.



Esempio di eventi

Utilizzo di Kaspersky Security Center Web Console in un ambiente cloud

Questa sezione fornisce informazioni sulle funzionalità di Kaspersky Security Center Web Console relative alla distribuzione e alla manutenzione di Kaspersky Security Center negli ambienti cloud, ad esempio Amazon Web Services, Microsoft Azure o Google Cloud.

Per l'utilizzo in un ambiente cloud è necessaria una licenza speciale. Se non si dispone di tale licenza, gli elementi dell'interfaccia relativi ai dispositivi cloud non vengono visualizzati.

Configurazione dell'ambiente cloud in Kaspersky Security Center Web Console

Per configurare Kaspersky Security Center con la procedura guidata Configura ambiente cloud, sono necessari i seguenti prerequisiti:

- Credenziali specifiche per un ambiente cloud:
  - Un ruolo IAM che dispone dei diritti per il polling del segmento cloud o un account utente IAM che dispone dei diritti per il polling del segmento cloud (per l'utilizzo con Amazon Web Services)
  - ID applicazione Azure, password e sottoscrizione (per l'utilizzo con Microsoft Azure)
  - E-mail client Google, ID progetto e chiave privata (per l'utilizzo con Google Cloud)
- Pacchetti di installazione:
  - Network Agent per Windows
  - Network Agent per Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in Web per Kaspersky Endpoint Security for Linux
- Almeno uno dei seguenti componenti:
  - Pacchetto di installazione e plug-in Web per Kaspersky Endpoint Security for Windows (consigliato)
  - Pacchetto di installazione e plug-in Web per Kaspersky Security for Windows Server

La procedura guidata Configura ambiente cloud viene avviata automaticamente la prima volta che ci si connette ad Administration Server tramite Administration Console se si distribuisce Kaspersky Security Center da un'immagine pronta all'uso. È anche possibile avviare manualmente la procedura guidata in qualsiasi momento.

Per avviare manualmente la procedura guidata Configura ambiente cloud:

Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Configura ambiente cloud**.

Verrà avviata la procedura guidata.

Una sessione di lavoro media per la configurazione dell'ambiente cloud ha una durata di circa 15 minuti.

Passaggio 1. Controllo dei plug-in e dei pacchetti di installazione necessari

Questo passaggio non viene visualizzato se si dispone di tutti i plug-in Web e dei pacchetti di installazione necessari elencati di seguito.

Per configurare un ambiente cloud, è necessario disporre dei seguenti componenti:

- Pacchetti di installazione:
  - Network Agent per Windows
  - Network Agent per Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in Web per Kaspersky Endpoint Security for Linux
- Almeno uno dei seguenti componenti:
  - Pacchetto di installazione e plug-in Web per Kaspersky Endpoint Security for Windows (consigliato)
  - Pacchetto di installazione e plug-in Web per Kaspersky Security for Windows Server

    Si consiglia di utilizzare Kaspersky Endpoint Security for Windows anziché Kaspersky Security for Windows Server.

Kaspersky Security Center rileva automaticamente i componenti di cui si dispone già ed elenca solo quelli mancanti. Scaricare i componenti elencati facendo clic su **Seleziona le applicazioni da scaricare**, quindi selezionare i plug-in e i pacchetti di installazione necessari. Dopo aver scaricato un componente, è possibile utilizzare il pulsante **Aggiorna** per aggiornare l'elenco dei componenti mancanti.

Passaggio 2. Informazioni sull'applicazione

Questo passaggio viene visualizzato solo se si utilizza un'immagine AMI BYOL e l'applicazione non è stata attivata con una licenza Kaspersky Security for Virtualization o una licenza Kaspersky Hybrid Cloud Security.

Specificare la chiave di licenza e fare clic su **Avanti** per continuare.

La chiave di licenza viene aggiunta all'archivio dell'Administration Server.

Se si esegue nuovamente la procedura guidata, questo passaggio non viene visualizzato.

Passaggio 3. Selezione dell'ambiente cloud e autorizzazione

Questa sezione descrive le funzionalità applicabili solo a Kaspersky Security Center 12.1 o versioni successive.

Specificare le seguenti impostazioni:

- **Ambiente cloud**

  Selezionare l'ambiente cloud in cui distribuire Kaspersky Security Center: AWS, Azure o Google Cloud.

  Se si prevede di utilizzare più di un ambiente cloud, selezionare un ambiente ed eseguire nuovamente la procedura guidata.

- **Nome della connessione**

  Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

  Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

  Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

Immettere le credenziali per ricevere l'autorizzazione nell'ambiente cloud specificato.

AWS

Se è stato selezionato AWS come tipo di segmento cloud, è necessario un ruolo IAM o una chiave di accesso AWS IAM per eseguire ulteriormente il polling del segmento cloud.

- **Ruolo IAM AWS assegnato all'istanza EC2**

  Selezionare questa opzione se si dispone di un ruolo IAM con i diritti richiesti per Administration Server.

- **Utente IAM AWS**

  Selezionare questa opzione se si dispone di una chiave di accesso AWS IAM. Immettere i dati chiave:

  - **ID chiave di accesso**

    L'ID chiave di accesso IAM è una sequenza di caratteri alfanumerici. L'ID chiave è stato ricevuto al momento della creazione dell'account utente IAM.

    Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

  - **Chiave segreta**

    Chiave segreta ricevuta con l'ID chiave di accesso al momento della creazione dell'account utente IAM.

    I caratteri della chiave segreta sono visualizzati come asterischi. Quando si inizia a immettere la chiave segreta, viene visualizzato il pulsante **Mostra**. Tenere premuto questo pulsante per visualizzare i caratteri immessi.

    Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

    Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

Azure

Se è stato selezionato Azure come tipo di segmento cloud, specificare le seguenti impostazioni per la connessione da utilizzare per il polling del segmento cloud:

- **ID applicazione Azure**

  L'ID applicazione è stato creato dall'utente nel portale di Azure.

  È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

- **ID sottoscrizione Azure**

  La sottoscrizione è stata creata dall'utente nel portale di Azure.

- **Password dell'applicazione Azure**

  La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

  I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

- **Nome dell'account di archiviazione Azure**

  È stato creato il nome dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

- **Chiave di accesso all'archivio Azure**

  È stata ricevuta una password (chiave) durante la creazione dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

  La chiave è disponibile nella sezione "Panoramica dell'account di archiviazione Azure", nella sottosezione "Chiavi".

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

Google Cloud

Se è stato selezionato Google Cloud come tipo di segmento cloud, specificare le seguenti impostazioni per la connessione da utilizzare per il polling del segmento cloud:

- **Indirizzo e-mail client**

  L'e-mail client è l'indirizzo e-mail utilizzato per la registrazione del progetto in Google Cloud.

- **ID progetto**

  L'ID progetto è l'ID ricevuto durante la registrazione del progetto in Google Cloud.

- **Chiave privata**

  La chiave privata è la sequenza di caratteri ricevuta come chiave privata durante la registrazione del progetto in Google Cloud. È consigliabile copiare e incollare questa sequenza per evitare errori.

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

La connessione specificata viene salvata nelle impostazioni dell'applicazione.

La procedura guidata Configura ambiente cloud consente di specificare un solo segmento. Successivamente è possibile specificare più connessioni per gestire altri segmenti cloud.

Fare clic su **Avanti** per continuare.

Passaggio 4. Polling dei sistemi, configurazione della sincronizzazione con il cloud e selezione delle azioni successive

In questo passaggio viene avviato il polling dei segmenti cloud e viene automaticamente creato uno speciale gruppo di amministrazione per i dispositivi cloud. I dispositivi rilevati durante il polling vengono inseriti in questo gruppo. La pianificazione del polling dei segmenti cloud è configurata (ogni 5 minuti per impostazione predefinita; è possibile modificare questa impostazione in un secondo momento).

Viene inoltre creata una regola di spostamento automatico **Sincronizza con il cloud**. Per ogni successiva scansione della rete cloud, i dispositivi virtuali rilevati verranno spostati nel sottogruppo corrispondente all'interno del gruppo **Dispositivi gestiti\Cloud**.

Definire le seguenti impostazioni:

- **Sincronizza gruppi di amministrazione con la struttura cloud**

  Se questa opzione è abilitata, viene creato automaticamente il gruppo **Cloud** all'interno del gruppo **Dispositivi gestiti** e viene avviata una device discovery cloud. Le istanze e le macchine virtuali rilevate durante ciascuna scansione della rete cloud sono inserite nel gruppo Cloud. La struttura dei sottogruppi di amministrazione all'interno di questo gruppo corrisponde alla struttura del segmento cloud (in AWS, le zone di disponibilità e i gruppi di collocazione non sono rappresentati nella struttura; in Azure, le subnet non sono rappresentate nella struttura). I dispositivi che non sono stati identificati come istanze nell'ambiente cloud si trovano nel gruppo **Dispositivi non assegnati**. La struttura di questo gruppo consente di utilizzare le attività di installazione di gruppo per installare le applicazioni anti-virus nelle istanze, nonché di configurare diversi criteri per diversi gruppi.

  Se questa opzione è disabilitata, viene creato il gruppo **Cloud** e viene avviata una device discovery cloud, tuttavia all'interno del gruppo non vengono creati i sottogruppi che corrispondono alla struttura del segmento cloud. Tutte le istanze rilevate si trovano nel gruppo di amministrazione **Cloud**, pertanto vengono visualizzate in un unico elenco. Se l'utilizzo di Kaspersky Security Center richiede la sincronizzazione, è possibile modificare le proprietà della regola **Sincronizza con il cloud** e quindi applicarla. Applicando la regola viene modificata la struttura dei sottogruppi nel gruppo Cloud in modo da creare la corrispondenza con la struttura del segmento cloud.

  Per impostazione predefinita, questa opzione è disabilitata.

- **Distribuisci protezione**

  Se questa opzione è selezionata, la procedura guidata crea un'attività per l'installazione delle applicazioni di protezione nelle istanze. Al termine della procedura guidata, verrà avviata automaticamente la Distribuzione guidata della protezione nei dispositivi nei segmenti cloud e sarà possibile installare Network Agent e le applicazioni di protezione in tali dispositivi.

  Kaspersky Security Center può eseguire la distribuzione tramite i propri strumenti nativi. Se non si dispone delle autorizzazioni per installare le applicazioni in istanze EC2 o nelle macchine virtuali Azure, è possibile configurare l'attività **Installazione remota** manualmente e specificare un account con le autorizzazioni richieste. In questo caso l'attività di installazione remota non funzionerà per i dispositivi rilevati utilizzando API AWS o Azure. Questa attività funzionerà solo per i dispositivi rilevati tramite il polling di Active Directory, dei domini Windows o dell'intervallo IP.

  Se questa opzione è deselezionata, la Distribuzione guidata della protezione non viene avviata e non vengono create attività per l'installazione delle applicazioni di protezione nelle istanze. È possibile eseguire manualmente entrambe le operazioni in un secondo momento.

Se si seleziona l'opzione Distribuisci protezione, la sezione **Riavvio dei dispositivi** diventa disponibile. In questa sezione è necessario scegliere quale operazione eseguire quando il sistema operativo di un dispositivo di destinazione deve essere riavviato. Scegliere se riavviare le istanze qualora il sistema operativo del dispositivo debba essere riavviato durante l'installazione delle applicazioni:

- **Non riavviare**

  Se questa opzione è selezionata, il dispositivo non verrà riavviato dopo l'installazione dell'applicazione di protezione.

- **Riavvia**

  Se questa opzione è selezionata, il dispositivo verrà riavviato dopo l'installazione dell'applicazione di protezione.

Fare clic su **Avanti** per continuare.

Per Google Cloud, è possibile eseguire la distribuzione solo con gli strumenti nativi di Kaspersky Security Center. Se è stato selezionato Google Cloud, l'opzione **Distribuisci protezione** non è disponibile.

Passaggio 5. Selezione di un'applicazione per la quale creare criteri e attività

Questo passaggio viene visualizzato solo se si dispone dei pacchetti di installazione e dei plug-in per Kaspersky Endpoint Security for Windows e Kaspersky Security for Windows Server. Se si dispone di un plug-in e di un pacchetto di installazione solo di una di queste applicazioni, questo passaggio viene ignorato e Kaspersky Security Center crea un criterio e attività per l'applicazione esistente.

Selezionare un'applicazione per cui si desidera creare un criterio e attività.

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

Passaggio 6. Configurazione di Kaspersky Security Network per Kaspersky Security Center

Specificare le impostazioni per la trasmissione delle informazioni sulle operazioni di Kaspersky Security Center alla Knowledge Base di Kaspersky Security Network (KSN). Selezionare una delle seguenti opzioni:

- **Accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center e le applicazioni gestite installate nei dispositivi client trasferiranno automaticamente i dettagli sull'esecuzione a Kaspersky Security Network. La partecipazione a Kaspersky Security Network garantisce aggiornamenti più rapidi dei database contenenti le informazioni sui virus e sulle altre minacce, assicurando una risposta più rapida alle minacce per la sicurezza emergenti.

- **Non accetto di utilizzare Kaspersky Security Network**

  Kaspersky Security Center e le applicazioni gestite non forniranno informazioni a Kaspersky Security Network.

  Se si seleziona questa opzione, l'utilizzo di Kaspersky Security Network sarà disabilitato.

Kaspersky consiglia la partecipazione a Kaspersky Security Network.

È inoltre possibile visualizzare i contratti KSN per le applicazioni gestite. Se si accetta di utilizzare Kaspersky Security Network, l'applicazione gestita invierà i dati a Kaspersky. Se non si accetta di partecipare a Kaspersky Security Network, l'applicazione gestita non invierà i dati a Kaspersky. È possibile modificare questa impostazione in un secondo momento nei criteri dell'applicazione.

Fare clic su **Avanti** per continuare.

Passaggio 7. Creazione di una configurazione iniziale della protezione

È possibile esaminare un elenco dei criteri e delle attività creati.

Attendere il completamento della creazione di criteri e attività, quindi fare clic su **Avanti** per procedere. Nell'ultima pagina della procedura guidata, fare clic sul pulsante **Fine** per uscire.

Polling dei segmenti di rete tramite Kaspersky Security Center Web Console

Le informazioni sulla struttura (e sui dispositivi) della rete vengono ricevute da Administration Server tramite il polling periodico dei segmenti cloud mediante gli strumenti API AWS, API Azure o API Google. Kaspersky Security Center utilizza queste informazioni per aggiornare il contenuto delle cartelle Dispositivi non assegnati e Dispositivi gestiti. Se i dispositivi sono stati configurati in modo da essere spostati automaticamente nei gruppi di amministrazione, i dispositivi rilevati sono inclusi nei gruppi di amministrazione.

Per consentire ad Administration Server di eseguire il polling dei segmenti cloud, è necessario disporre dei diritti corrispondenti forniti con un ruolo IAM o un account utente IAM (in AWS) o con un ID applicazione e una password (in Azure) o con l'e-mail client di Google, l'ID progetto di Google e una chiave privata (in Google Cloud).

È possibile aggiungere ed eliminare le connessioni, nonché configurare la pianificazione di polling per ogni segmento cloud.

Aggiunta di connessioni per il polling dei segmenti cloud

Per aggiungere una connessione per il polling dei segmenti cloud all'elenco delle connessioni disponibili:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Cloud**.
2. Nella finestra visualizzata fare clic su **Proprietà**.
3. Nella finestra **Impostazioni** visualizzata fare clic su **Aggiungi**.
   Verrà visualizzata la finestra **Impostazioni segmento cloud**.

4. Specificare il nome dell'ambiente cloud per la connessione da utilizzare per il successivo polling del segmento cloud:

- **Ambiente cloud**

  Selezionare l'ambiente cloud in cui distribuire Kaspersky Security Center: AWS, Azure o Google Cloud.

  Se si prevede di utilizzare più di un ambiente cloud, selezionare un ambiente ed eseguire nuovamente la procedura guidata.

- **Nome della connessione**

  Immettere un nome per la connessione. Il nome non può contenere più di 256 caratteri. Sono consentiti solo caratteri Unicode.

  Questo nome verrà utilizzato anche come nome per il gruppo di amministrazione per i dispositivi cloud.

  Se si prevede di utilizzare più di un ambiente cloud, è consigliabile includere il nome dell'ambiente nel nome della connessione, ad esempio "Segmento Azure", "Segmento AWS" o "Segmento Google".

5. Immettere le credenziali per ricevere l'autorizzazione nell'ambiente cloud specificato.

- Se è stato selezionato AWS, specificare le seguenti impostazioni:

  - **Usa ruolo IAM AWS**

    Selezionare questa opzione se è stato già creato un ruolo IAM per l'utilizzo dei servizi AWS da parte di Administration Server.

  - **Credenziali account utente IAM AWS**

    Selezionare questa opzione se si dispone di un account utente IAM con le autorizzazioni richieste ed è possibile immettere un ID chiave e una chiave segreta.

    Se è stato specificato che si dispone dell'opzione Credenziali account utente IAM AWS, specificare quanto segue:

    - **ID chiave di accesso**

      L'ID chiave di accesso IAM è una sequenza di caratteri alfanumerici. L'ID chiave è stato ricevuto al momento della creazione dell'account utente IAM.

      Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

    - **Chiave segreta**

      Chiave segreta ricevuta con l'ID chiave di accesso al momento della creazione dell'account utente IAM.

      I caratteri della chiave segreta sono visualizzati come asterischi. Quando si inizia a immettere la chiave segreta, viene visualizzato il pulsante **Mostra**. Tenere premuto questo pulsante per visualizzare i caratteri immessi.

      Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

    Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

- Se è stato selezionato Azure, specificare le seguenti impostazioni:

  - **ID applicazione Azure**

    L'ID applicazione è stato creato dall'utente nel portale di Azure.

    È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

  - **ID sottoscrizione Azure**

    La sottoscrizione è stata creata dall'utente nel portale di Azure.

  - **Password dell'applicazione Azure**

La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

- **Nome dell'account di archiviazione di Azure**

  È stato creato il nome dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

- **Chiave di accesso per l'archiviazione di Azure**

  È stata ricevuta una password (chiave) durante la creazione dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

  La chiave è disponibile nella sezione "Panoramica dell'account di archiviazione Azure", nella sottosezione "Chiavi".

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

Se è stato selezionato Google Cloud, specificare le seguenti impostazioni:

- **Indirizzo e-mail client**

  L'e-mail client è l'indirizzo e-mail utilizzato per la registrazione del progetto in Google Cloud.

- **ID progetto**

  L'ID progetto è l'ID ricevuto durante la registrazione del progetto in Google Cloud.

- **Chiave privata**

  La chiave privata è la sequenza di caratteri ricevuta come chiave privata durante la registrazione del progetto in Google Cloud. È consigliabile copiare e incollare questa sequenza per evitare errori.

  Per visualizzare i caratteri immessi, tenere premuto il pulsante **Mostra**.

6. Se lo si desidera, fare clic su **Imposta pianificazione di polling** e modificare le impostazioni predefinite.

La connessione viene salvata nelle impostazioni dell'applicazione.

Dopo la prima esecuzione del polling del nuovo segmento cloud, il sottogruppo corrispondente a tale segmento viene visualizzato nel gruppo di amministrazione **Dispositivi gestiti\Cloud**.

Se si specificano credenziali errate, non verranno individuate istanze durante il polling del segmento cloud e non verrà visualizzato un nuovo sottogruppo nel gruppo di amministrazione **Dispositivi gestiti\Cloud**.

Eliminazione di una connessione per il polling dei segmenti cloud

Se non è più necessario eseguire il polling di uno specifico segmento cloud, è possibile eliminare la connessione corrispondente dall'elenco delle connessioni disponibili. È anche possibile eliminare una connessione se, ad esempio, le autorizzazioni per il polling di un segmento cloud sono state trasferite a un altro utente con credenziali diverse.

Per eliminare una connessione:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Cloud**.
2. Nella finestra visualizzata fare clic su **Proprietà**.
3. Nella finestra **Impostazioni** visualizzata fare clic sul nome del segmento che si desidera eliminare.
4. Fare clic su **Elimina**.
5. Nella finestra visualizzata fare clic sul pulsante **OK** per confermare la selezione.

La connessione viene eliminata. I dispositivi nel segmento cloud corrispondente a questa connessione vengono automaticamente eliminati dai gruppi di amministrazione.

Configurazione della pianificazione di polling tramite Kaspersky Security Center Web Console

Il polling dei segmenti cloud viene eseguito in base a una pianificazione. È possibile impostare la frequenza di polling.

La frequenza di polling è impostata automaticamente su 5 minuti nelle impostazioni di Configura ambiente cloud. È possibile modificare il valore in qualsiasi momento e impostare una pianificazione diversa. Non è tuttavia consigliabile configurare il polling per l'esecuzione con una frequenza inferiore a 5 minuti perché potrebbero verificarsi errori nel funzionamento dell'API.

Per configurare la pianificazione del polling dei segmenti cloud:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Cloud**.
2. Nella finestra visualizzata fare clic su **Proprietà**.
3. Nella finestra **Impostazioni** visualizzata fare clic sul nome del segmento per il quale si desidera configurare una pianificazione di polling.

   Verrà visualizzata la finestra **Impostazioni segmento cloud**.
4. Nella finestra **Impostazioni segmento cloud** fare clic sul pulsante **Imposta pianificazione di polling**.

   Verrà visualizzata la finestra **Pianificazione**.

5. Nella finestra **Pianificazione** specificare le seguenti impostazioni:

- **Avvio pianificato**

  Opzioni per la pianificazione di polling:

  - **Ogni N giorni**

    Il polling viene eseguito periodicamente, con l'intervallo specificato in giorni, a partire dalla data e dall'ora specificate.

    Per impostazione predefinita, il polling viene eseguito ogni giorno, a partire dalla data e dall'ora di sistema correnti.

  - Ogni N minuti

    Il polling viene eseguito periodicamente, con l'intervallo specificato in minuti, a partire dall'ora specificata.

    Per impostazione predefinita, il polling viene eseguito ogni 5 minuti, a partire dall'ora di sistema corrente.

  - In base ai giorni della settimana

    Il polling viene eseguito periodicamente, nei giorni specificati della settimana, all'ora specificata.

    Per impostazione predefinita, il polling viene eseguito ogni venerdì alle 18:00:00.

  - Ogni mese nei giorni specificati delle settimane selezionate

    Il polling viene eseguito periodicamente, nei giorni specificati di ogni mese, all'ora specificata.

    Per impostazione predefinita, non sono selezionati giorni del mese. L'ora di inizio predefinita è 18:00:00.

- **Intervallo di avvio**

  Specificare a cosa equivale N (per minuti o giorni).

- **A partire da**

  Specificare quando avviare il primo polling.

- **Esegui attività non effettuate**

  Se l'Administration Server è spento o non disponibile nel momento in cui è pianificato il polling, l'Administration Server può avviare il polling subito dopo l'accensione o attendere la successiva pianificazione del polling.

  Se questa opzione è abilitata, l'Administration Server avvia il polling subito dopo l'accensione.

  Se questa opzione è disabilitata, l'Administration Server attende la successiva pianificazione del polling.

  Per impostazione predefinita, questa opzione è abilitata.

6. Salvare le modifiche.

La pianificazione di polling per il segmento verrà configurata e salvata.

Visualizzazione dei risultati del polling dei segmenti cloud tramite Kaspersky Security Center Web Console

È possibile visualizzare i risultati del polling dei segmenti cloud, ovvero visualizzare l'elenco dei dispositivi cloud gestiti da Administration Server.

Per visualizzare i risultati del polling dei segmenti cloud,

Nel menu principale accedere a **Individuazione e distribuzione** → **Individuazione** → **Cloud**.

Consente di visualizzare i segmenti cloud disponibili per il polling.

Visualizzazione delle proprietà dei dispositivi cloud tramite Kaspersky Security Center Web Console

È possibile visualizzare le proprietà di ciascun dispositivo cloud.

Per visualizzare le proprietà di un dispositivo cloud:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Dispositivi gestiti**.
2. Fare clic sul nome del dispositivo di cui si desidera visualizzare le proprietà.

   Verrà visualizzata una finestra delle proprietà con la sezione **Generale** selezionata.
3. Se si desidera visualizzare le proprietà specifiche per i dispositivi cloud, selezionare la sezione **Sistema** nella finestra delle proprietà.

   Le proprietà vengono visualizzate in base alla piattaforma cloud del dispositivo.

   Per i dispositivi in AWS, vengono visualizzate le seguenti proprietà:

   - **Dispositivo rilevato tramite API** (valore: **AWS**)
   - **Regioni cloud**
   - **VPC cloud**
   - **Zona di disponibilità cloud**
   - **Sottorete cloud**
   - **Gruppo di collocazione Cloud** (questa unità viene visualizzata solo se l'istanza appartiene a un gruppo di collocazione; in caso contrario, non viene visualizzata)

   Per i dispositivi in Azure, vengono visualizzate le seguenti proprietà:

   - **Dispositivo rilevato tramite API** (valore: **Microsoft Azure**)
   - **Regioni cloud**
   - **Sottorete cloud**

   Per i dispositivi in Google Cloud, vengono visualizzate le seguenti proprietà:

   - **Dispositivo rilevato tramite API** (valore: **Google Cloud**)
   - **Regioni cloud**
   - **VPC cloud**
   - **Zona di disponibilità cloud**
   - **Sottorete cloud**

Sincronizzazione con il cloud: configurazione della regola di spostamento

Durante l'esecuzione di Configura ambiente cloud, viene automaticamente creata la regola Sincronizza con il cloud. La regola consente di spostare automaticamente i dispositivi rilevati in ogni polling dal gruppo Dispositivi non assegnati al gruppo Dispositivi gestiti\Cloud per rendere disponibili tali dispositivi per la gestione centralizzata. Per impostazione predefinita, la regola è attiva dopo la creazione. È possibile disabilitare, modificare o applicare la regola in qualsiasi momento.

Per modificare le proprietà della regola Sincronizza con il cloud e/o applicare la regola:

1. Nel menu principale accedere a **Individuazione e distribuzione** → **Distribuzione e assegnazione** → **Regole di spostamento**.

   Viene aperto un elenco delle regole di spostamento.

2. Nell'elenco delle regole di spostamento selezionare **Sincronizza con il cloud**.

   Verrà visualizzata la finestra delle proprietà delle regole.

3. Se necessario, specificare le seguenti impostazioni nella scheda **Condizioni delle regole**, nella scheda **Segmenti cloud**:

- **Il dispositivo si trova in un segmento cloud**

  La regola viene applicata solo ai dispositivi inclusi nel segmento cloud selezionato. In caso contrario, la regola viene applicata a tutti i dispositivi individuati.

  Per impostazione predefinita, questa opzione è selezionata.

- **Includi gli oggetti figlio**

  La regola viene applicata a tutti i dispositivi nel segmento selezionato e in tutte le sottosezioni cloud nidificate. In caso contrario, la regola viene applicata solo ai dispositivi inclusi nel segmento radice.

  Per impostazione predefinita, questa opzione è selezionata.

- **Sposta i dispositivi dagli oggetti nidificati nei sottogruppi corrispondenti**

  Se questa opzione è abilitata, i dispositivi vengono spostati automaticamente dagli oggetti nidificati ai sottogruppi corrispondenti alla relativa struttura.

  Se questa opzione è disabilitata, i dispositivi vengono spostati automaticamente dagli oggetti nidificati alla radice del sottogruppo Cloud senza ulteriori ramificazioni.

  Per impostazione predefinita, questa opzione è abilitata.

- **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati**

  Se questa opzione è abilitata, quando la struttura del gruppo **Dispositivi gestiti\Cloud** non ha sottogruppi corrispondenti alla sezione che contiene il dispositivo, Kaspersky Security Center crea tali sottogruppi. Ad esempio, se viene rilevata una nuova subnet durante la device discovery, verrà creato un nuovo gruppo con lo stesso nome nel gruppo **Dispositivi gestiti\Cloud**.

  Se questa opzione è disabilitata, Kaspersky Security Center non crea nuovi sottogruppi. Ad esempio, se viene rilevata una nuova subnet durante il polling della rete, non verrà creato un nuovo gruppo con lo stesso nome nel gruppo **Dispositivi gestiti\Cloud** e i dispositivi presenti nella subnet verranno spostati nel gruppo **Dispositivi gestiti\Cloud**.

  Per impostazione predefinita, questa opzione è abilitata.

- **Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud**

  Se questa opzione è abilitata, l'applicazione elimina dal gruppo Cloud tutti i sottogruppi a cui non corrisponde alcun oggetto cloud esistente.

  Se questa opzione è disabilitata, vengono mantenuti i sottogruppi a cui non corrisponde alcun oggetto cloud esistente.

  Per impostazione predefinita, questa opzione è abilitata.

Se è stata abilitata l'opzione **Sincronizza gruppi di amministrazione con la struttura cloud** durante la configurazione dell'ambiente cloud, la regola **Sincronizza con il cloud** viene creata con le opzioni **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati** e **Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud** abilitate.

Se non è stata abilitata l'opzione **Sincronizza gruppi di amministrazione con la struttura cloud**, la regola **Sincronizza con il cloud** viene creata con queste opzioni disabilitate (deselezionate). Se l'utilizzo di Kaspersky Security Center richiede che la struttura dei sottogruppi nel sottogruppo di **Dispositivi gestiti\Cloud** corrisponda alla struttura dei segmenti cloud, selezionare le caselle di controllo **Crea i sottogruppi corrispondenti ai contenitori dei nuovi dispositivi rilevati** ed **Elimina i sottogruppi per cui non viene trovata una corrispondenza nei segmenti cloud** nelle proprietà della regola e quindi applicare la regola.

4. Nell'elenco a discesa **Dispositivo rilevato tramite l'API** selezionare uno dei seguenti valori:

   - **No**. Il dispositivo non può essere rilevato tramite l'API AWS, Azure o Google, ad esempio perché si trova all'esterno dell'ambiente cloud oppure si trova nell'ambiente cloud ma non può essere rilevato tramite un'API per qualche motivo.
   - **AWS**. Il dispositivo viene rilevato tramite l'API AWS, ovvero è nell'ambiente cloud AWS.
   - **Azure**. Il dispositivo è individuato tramite l'API Azure, ovvero è nell'ambiente cloud Azure.
   - **Google Cloud**. Il dispositivo è individuato tramite l'API Google, ovvero è nell'ambiente cloud Google.
   - Nessun valore. Il criterio non può essere applicato.

5. Se necessario, configurare le proprietà delle altre regole nelle altre sezioni.

Verrà configurata la regola di spostamento.

Installazione remota delle applicazioni nelle macchine virtuali Azure

È necessario disporre di una licenza valida per installare le applicazioni nelle macchine virtuali di Microsoft Azure.

Kaspersky Security Center supporta i seguenti scenari:

- Un dispositivo client viene rilevato tramite l'API Azure; anche l'installazione viene eseguita tramite un'API. L'utilizzo dell'API di Azure indica che è possibile installare solo le seguenti applicazioni:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- Un dispositivo client viene rilevato tramite l'API Azure; l'installazione viene eseguita tramite un punto di distribuzione o, se non sono presenti punti di distribuzione, manualmente, utilizzando pacchetti di installazione indipendenti. È possibile installare qualsiasi applicazione supportata da Kaspersky Security Center in questo modo.

Per creare un'attività per l'installazione remota dell'applicazione nelle macchine virtuali Azure:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.
3. Seguire le istruzioni della procedura guidata:

   a. Selezionare **Installa l'applicazione in remoto** come tipo di attività.

   b. Nella pagina **Pacchetti di installazione**, selezionare **Installazione remota eseguita da Microsoft Azure API**.

   c. Quando si seleziona l'account per accedere ai dispositivi, utilizzare un account Azure esistente o fare clic su **Aggiungi** e inserire le credenziali dell'account Azure:

   - **Nome account Azure**

     Inserire un nome per le credenziali specificate. Questo nome verrà visualizzato nell'elenco degli account per l'esecuzione dell'attività.

   - **ID applicazione Azure**

     L'ID applicazione è stato creato dall'utente nel portale di Azure.

     È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

   - **Password dell'applicazione Azure**

     La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

     I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

   d. Selezionare i dispositivi interessati nel gruppo **Dispositivi gestiti\Cloud**.

Al termine della procedura guidata, l'attività di installazione remota dell'applicazione viene visualizzata nell'elenco delle attività.

Creazione dell'attività Backup dei dati di Administration Server con l'utilizzo di un DBMS cloud

Le attività di backup sono attività di Administration Server. Viene creata un'attività di backup se si desidera utilizzare un DBMS situato in un ambiente cloud (AWS o Azure).

Per creare un'attività di backup dei dati di Administration Server:

1. Nel menu principale accedere a **Risorse (dispositivi)** → **Attività**.
2. Fare clic su **Aggiungi**.

   Verrà avviata la Creazione guidata nuova attività.

3. Nell'elenco **Applicazione** della prima pagina della procedura guidata selezionare **Kaspersky Security Center 15.1** e nell'elenco **Tipo di attività** selezionare **Backup dei dati di Administration Server**.

4. Nella pagina corrispondente della procedura guidata, specificare le seguenti impostazioni:

   - Se si utilizza un database in AWS:

     - **Nome del bucket S3**

       Nome del bucket S3 che è stato creato per il backup.

     - **ID chiave di accesso**

       L'ID chiave (sequenza di caratteri alfanumerici) è stato ricevuto al momento della creazione dell'account utente IAM per l'utilizzo dell'istanza di archiviazione del bucket S3.

       Il campo è disponibile se è stato selezionato il database RDS in un bucket S3.

     - **Chiave segreta**

       Chiave segreta ricevuta con l'ID chiave di accesso al momento della creazione dell'account utente IAM.

       I caratteri della chiave segreta sono visualizzati come asterischi. Quando si inizia a immettere la chiave segreta, viene visualizzato il pulsante **Mostra**. Tenere premuto questo pulsante per visualizzare i caratteri immessi.

       Il campo è disponibile se per l'autorizzazione è stata selezionata una chiave di accesso AWS IAM anziché un ruolo IAM.

   - Se si utilizza un database in Microsoft Azure:

     - **Nome dell'account di archiviazione Azure**

       È stato creato il nome dell'account di archiviazione Azure per l'utilizzo di Kaspersky Security Center.

     - **ID sottoscrizione Azure**

       La sottoscrizione è stata creata dall'utente nel portale di Azure.

     - **Password Azure**

       La password dell'ID applicazione è stata ricevuta al momento della creazione dell'ID applicazione.

       I caratteri della password sono visualizzati come asterischi. Quando si inizia a immettere la password, diventerà disponibile il pulsante **Mostra**. Tenere questo pulsante per visualizzare i caratteri immessi.

     - **ID applicazione Azure**

L'ID applicazione è stato creato dall'utente nel portale di Azure.

È possibile specificare un solo ID applicazione Azure per il polling e altri scopi. Se si desidera eseguire il polling di un altro segmento di Azure, è prima necessario eliminare la connessione Azure esistente.

- **Nome del server SQL Azure**

  Il nome e il gruppo di risorse sono disponibili nelle proprietà del server SQL Azure.

- **Gruppo di risorse del server SQL Azure**

  Il nome e il gruppo di risorse sono disponibili nelle proprietà del server SQL Azure.

- **Chiave di accesso all'archivio Azure**

  Disponibile nelle proprietà dell'account di archiviazione, nella sezione Chiavi di accesso. È possibile utilizzare qualsiasi chiave (chiave1 o chiave2).

L'attività verrà creata e visualizzata nell'elenco delle attività. Se si abilita l'opzione **Apri i dettagli dell'attività al termine della creazione** è possibile modificare le impostazioni predefinite dell'attività subito dopo la creazione dell'attività. Se non si abilita questa opzione, l'attività viene creata con le impostazioni predefinite. È possibile modificare le impostazioni predefinite in seguito in qualsiasi momento.

Diagnostica remota dei dispositivi client

È possibile utilizzare la diagnostica remota per l'esecuzione remota delle seguenti operazioni nei dispositivi client basati su Windows e basati su Linux:

- Abilitazione e disabilitazione del tracciamento, modifica del livello di traccia e download del file di traccia
- Download di informazioni sul sistema e impostazioni dell'applicazione
- Download dei registri eventi
- Generazione di un file di dump per un'applicazione
- Avvio della diagnostica e download dei rapporti
- Avvio, arresto e riavvio delle applicazioni

È possibile utilizzare i registri eventi e i rapporti di diagnostica scaricati da un dispositivo client per eseguire autonomamente la risoluzione dei problemi. Inoltre, se si contatta il Servizio di assistenza tecnica Kaspersky, uno specialista del Servizio di assistenza tecnica potrebbe richiedere di scaricare file di traccia, file di dump, registri eventi e rapporti di diagnostica da un dispositivo client per ulteriori analisi da parte di Kaspersky.

Apertura della finestra di diagnostica remota

Per eseguire la diagnostica remota in dispositivi client basati su Windows e basati su Linux, è prima necessario aprire la finestra di diagnostica remota.

Per aprire la finestra di diagnostica remota:

1. Per selezionare il dispositivo per cui si desidera aprire la finestra di diagnostica remota, eseguire una delle seguenti operazioni:

   - Se il dispositivo appartiene a un gruppo di amministrazione, nel menu principale passare a **Risorse (dispositivi)** → **Dispositivi gestiti**.

   - Se il dispositivo appartiene al gruppo Dispositivi non assegnati, nel menu principale passare a **Individuazione e distribuzione** → **Dispositivi non assegnati**.

2. Fare clic sul nome del dispositivo desiderato.

3. Nella finestra delle proprietà del dispositivo visualizzata selezionare la scheda **Avanzate**.

4. Nella finestra visualizzata fare clic su **Diagnostica remota**.

   Viene aperta la finestra **Diagnostica remota** di un dispositivo client. Se la connessione tra Administration Server e il dispositivo client non viene stabilita, viene visualizzato il messaggio di errore.

In alternativa, se è necessario ottenere tutte le informazioni diagnostiche su un dispositivo client basato su Linux, è possibile eseguire lo script collect.sh in questo dispositivo.

Abilitazione e disabilitazione del tracciamento per le applicazioni

È possibile abilitare e disabilitare il tracciamento per le applicazioni, incluso il tracciamento Xperf.

Abilitazione e disabilitazione del tracciamento

Per abilitare o disabilitare il tracciamento in un dispositivo remoto:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.

3. Nell'elenco delle applicazioni, selezionare l'applicazione per cui si desidera disabilitare il tracciamento.

   Si apre l'elenco delle opzioni di diagnostica remota.

4. Se si desidera abilitare il tracciamento:

   a. Nella sezione **Traccia**, fare clic su **Abilita traccia**.

   b. Nella finestra **Modifica livello di traccia** visualizzata è consigliabile mantenere i valori predefiniti delle impostazioni. Se necessario, uno specialista del Servizio di assistenza tecnica fornirà il supporto richiesto per il processo di configurazione. Sono disponibili le seguenti impostazioni:

   - **Livello di traccia**

     Il livello di traccia definisce la quantità di dettagli contenuti nel file di traccia.

   - **Traccia basata sulla rotazione**

     L'applicazione sovrascrive le informazioni di tracciamento per evitare un aumento eccessivo delle dimensioni del file di traccia. Specificare il numero massimo di file da utilizzare per archiviare le informazioni di tracciamento e la dimensione massima di ciascun file. Se viene eseguita la scrittura del numero massimo di file di traccia della dimensione massima, il file di traccia meno recente viene eliminato in modo da consentire la creazione di un nuovo file di traccia.

     Questa impostazione è disponibile solo per Kaspersky Endpoint Security.

   c. Fare clic su **Salva**.

   Il tracciamento è abilitato per l'applicazione selezionata. In alcuni casi, è necessario riavviare un'applicazione di protezione e la relativa attività per abilitare il tracciamento.

   Nei dispositivi client basati su Linux, il tracciamento per il componente Updater of Network Agent è regolata dalle impostazioni di Network Agent. Pertanto, le opzioni **Abilita traccia** e **Modifica livello di traccia** sono disabilitate per questo componente nei dispositivi client in cui viene eseguito Linux.

5. Se si desidera disabilitare il tracciamento per l'applicazione selezionata, fare clic sul pulsante **Disabilita traccia**.

   Il tracciamento è disabilitato per l'applicazione selezionata.

Abilitazione del tracciamento Xperf

Per Kaspersky Endpoint Security, uno specialista del Servizio di assistenza tecnica può richiedere di abilitare il tracciamento Xperf per ottenere informazioni sulle prestazioni del sistema.

Per abilitare e configurare il tracciamento Xperf o disabilitarlo:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.

3. Nell'elenco delle applicazioni selezionare Kaspersky Endpoint Security for Windows.

   Viene visualizzato l'elenco delle opzioni di diagnostica remota per Kaspersky Endpoint Security for Windows.

4. Nella sezione **Traccia Xperf**, fare clic su **Abilita traccia Xperf**.

   Se il tracciamento Xperf è già abilitato, viene invece visualizzato il pulsante **Disabilita traccia Xperf**. Fare clic su questo pulsante se si desidera disabilitare il tracciamento Xperf per Kaspersky Endpoint Security for Windows.

5. Nella finestra **Modifica livello di traccia Xperf** visualizzata, a seconda di quanto richiesto dallo specialista del Servizio di assistenza tecnica, eseguire una delle seguenti azioni:

   a. Selezionare uno dei seguenti livelli di traccia:

   - **Livello superficiale**

     Un file di traccia di questo tipo contiene la quantità minima di informazioni sul sistema.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Livello approfondito**

     Un file di traccia di questo tipo contiene informazioni più dettagliate rispetto ai file di traccia di tipo *Superficiale* e può essere richiesto dagli specialisti del Servizio di assistenza tecnica quando un file di traccia di tipo *Superficiale* non è sufficiente per la valutazione delle prestazioni. Un file di traccia *Approfondito* contiene informazioni tecniche sul sistema, incluse informazioni su hardware, sistema operativo, elenco di processi e applicazioni avviati e arrestati, eventi utilizzati per la valutazione delle prestazioni ed eventi raccolti da Strumento Valutazione sistema Windows.

   b. Selezionare uno dei seguenti tipi di tracciamento Xperf:

   - **Tipologia di base**

     Le informazioni di tracciamento vengono ricevute durante l'esecuzione dell'applicazione Kaspersky Endpoint Security.

     Per impostazione predefinita, questa opzione è selezionata.

   - **Tipologia al riavvio**

     Le informazioni di tracciamento vengono ricevute all'avvio del sistema operativo nel dispositivo gestito. Questo tipo di tracciamento è utile quando il problema che influisce sulle prestazioni del sistema si verifica dopo l'accensione del dispositivo e prima dell'avvio di Kaspersky Endpoint Security.

   Potrebbe anche essere necessario abilitare l'opzione **Dimensioni del file con rotazione (MB)** per impedire un aumento eccessivo delle dimensioni del file di traccia. Specificare quindi la dimensione massima del file di traccia. Quando il file raggiunge la dimensione massima, le informazioni di tracciamento meno recenti vengono sovrascritte da quelle nuove.

   c. Definire le dimensioni del file di rotazione.

   d. Fare clic su **Salva**.

   Il tracciamento Xperf è abilitato e configurato.

6. Se si desidera disabilitare il tracciamento Xperf per Kaspersky Endpoint Security for Windows, fare clic su **Disabilita traccia Xperf** nella sezione **Traccia Xperf**.

   Il tracciamento Xperf è disabilitato.

Download dei file di traccia di un'applicazione

Per scaricare un file di traccia di un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni, selezionare l'applicazione per la quale si desidera scaricare un file di traccia.
4. Nella sezione **Traccia** fare clic sul pulsante **File di traccia**.

   Viene aperta la finestra **Log di traccia del dispositivo**, dove viene visualizzato un elenco dei file di traccia.
5. Nell'elenco dei file di traccia, selezionare il file che si desidera scaricare.
6. Eseguire una delle seguenti operazioni:

   - Scaricare il file selezionato facendo clic su **Scarica**. È possibile selezionare uno o più file da scaricare.
   - Scaricare una parte del file selezionato:

     a. Fare clic su **Scarica una parte**.

     Non è possibile scaricare parti di più file contemporaneamente. Se si seleziona più di un file di traccia, il pulsante **Scarica una parte** sarà disabilitato.

     b. Nella finestra visualizzata specificare il nome e la parte del file da scaricare, in base alle esigenze.

     Per i dispositivi basati su Linux, la modifica del nome di parte del file non è disponibile.

     c. Fare clic su **Scarica**.

Il file selezionato, o la relativa parte, viene scaricato nella posizione specificata.

Eliminazione dei file di traccia

È possibile eliminare i file di traccia non più necessari.

Per eliminare un file di traccia:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra di diagnostica remota visualizzata, selezionare la scheda **Log eventi**.

3. Nella sezione **File di traccia**, fare clic su **Log di Windows Update** o **Log di installazione remota**, in base ai file di traccia che si desidera eliminare.

   Il collegamento ai **Log di Windows Update** è disponibile solo per i dispositivi client basati su Windows.

   Viene aperta la finestra **Log di traccia del dispositivo**, dove viene visualizzato un elenco dei file di traccia.

4. Nell'elenco dei file di traccia, selezionare uno o più file da eliminare.

5. Fare clic sul pulsante **Rimuovi**.

I file di traccia selezionati vengono eliminati.

Download delle impostazioni delle applicazioni

Per scaricare le impostazioni dell'applicazione da un dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

3. Nella sezione **Impostazioni applicazione**. fare clic sul pulsante **Scarica** per scaricare le informazioni sulle impostazioni delle applicazioni installate nel dispositivo client.

L'archivio ZIP con le informazioni viene scaricato nella posizione specificata.

Download dei registri eventi

Per scaricare un registro eventi da un dispositivo remoto:

1. Aprire la finestra di diagnostica remota di un dispositivo client.

2. Nella finestra della diagnostica remota, nella scheda **Log eventi**, fare clic su **Tutti i log del dispositivo**.

3. Nella finestra **Tutti i log del dispositivo**, selezionare uno o più log pertinenti.

4. Eseguire una delle seguenti operazioni:

   - Scaricare il log selezionato facendo clic su **Scarica l'intero file**.

   - Scaricare una parte del log selezionato:

     a. Fare clic su **Scarica una parte**.

        Non è possibile scaricare parti di più registri contemporaneamente. Se si seleziona più di un registro eventi, il pulsante **Scarica una parte** sarà disabilitato.

     b. Nella finestra visualizzata specificare il nome e la parte del registro da scaricare, in base alle esigenze.

        Per i dispositivi basati su Linux, la modifica del nome di parte del registro non è disponibile.

     c. Fare clic su **Scarica**.

Il registro eventi selezionato, o la relativa parte, viene scaricato nella posizione specificata.

Avvio, arresto, riavvio dell'applicazione

È possibile avviare, arrestare e riavviare le applicazioni in un dispositivo client.

Per avviare, arrestare o riavviare un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni selezionare l'applicazione che si desidera avviare, arrestare o riavviare.
4. Selezionare un'azione facendo clic su uno dei seguenti pulsanti:

   - **Arresta applicazione**

     Questo pulsante è disponibile solo se l'applicazione è attualmente in esecuzione.
   - **Riavvia applicazione**

     Questo pulsante è disponibile solo se l'applicazione è attualmente in esecuzione.
   - **Avvia applicazione**

     Questo pulsante è disponibile solo se l'applicazione non è attualmente in esecuzione.

   A seconda dell'azione selezionata, l'applicazione richiesta viene avviata, arrestata o riavviata nel dispositivo client.

Se si riavvia Network Agent, viene visualizzato un messaggio che indica che la connessione corrente del dispositivo ad Administration Server andrà persa.

Esecuzione della diagnostica remota di Kaspersky Security Center Network Agent e download dei risultati

Per avviare la diagnostica per Kaspersky Security Center Network Agent in un dispositivo remoto e scaricare i risultati:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Applicazioni Kaspersky**.

   Nella sezione **Gestione applicazioni**, viene mostrato l'elenco delle applicazioni Kaspersky installate nel dispositivo.
3. Nell'elenco delle applicazioni, selezionare **Kaspersky Security Center Network Agent**.

   Si apre l'elenco delle opzioni di diagnostica remota.

4. Nella sezione **Rapporto di diagnostica**, fare clic sul pulsante **Esegui diagnostica**.

   In questo modo si avvia la procedura di diagnostica remota e si genera un rapporto di diagnostica. Al termine della procedura di diagnostica, il pulsante **Scarica il rapporto di diagnostica** diventa disponibile.

5. Fare clic sul pulsante **Scarica il rapporto di diagnostica** per scaricare il rapporto.

Il rapporto viene scaricato nella posizione specificata.

Esecuzione di un'applicazione in un dispositivo client

Potrebbe essere necessario eseguire un'applicazione nel dispositivo client, se richiesto da uno specialista dell'Assistenza tecnica di Kaspersky. Non è necessario installare l'applicazione nel dispositivo.

Per eseguire un'applicazione nel dispositivo client:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Esecuzione di un'applicazione remota**.
3. Nella sezione **File dell'applicazione**, fare clic sul pulsante **Sfoglia** per selezionare un archivio ZIP contenente l'applicazione che si desidera eseguire nel dispositivo client.

   L'archivio ZIP deve includere la cartella dell'utilità. Questa cartella contiene il file eseguibile da eseguire in un dispositivo remoto.

   È possibile specificare il nome del file eseguibile e gli argomenti della riga di comando, se necessario. A tale scopo, compilare i campi **Executable file in an archive to be run on a remote device** e **Argomenti della riga di comando**.

4. Facendo clic sul pulsante **Carica ed esegui** per eseguire l'applicazione specificata in un dispositivo client.
5. Seguire le istruzioni dell'esperto dell'Assistenza Kaspersky.

Generazione di un file di dump per un'applicazione

Un file di dump dell'applicazione consente di visualizzare i parametri dell'applicazione in esecuzione in un dispositivo client in un determinato momento. Questo file contiene anche informazioni sui moduli che sono stati caricati per un'applicazione.

L'ottenimento dei file di dump da dispositivi basati su Linux non è supportato.

Per ottenere i file di dump tramite la diagnostica remota, viene utilizzata l'utilità kldumper. Questa utilità è progettata per ottenere i file di dump dei processi delle applicazioni Kaspersky su richiesta degli specialisti dell'Assistenza tecnica. Informazioni dettagliate sui requisiti per l'utilizzo dell'utilità kldumper sono fornite nella Knowledge Base di Kaspersky Security Center.

Per creare un file di dump per un'applicazione:

1. Aprire la finestra di diagnostica remota di un dispositivo client.
2. Nella finestra della diagnostica remota, selezionare la scheda **Esecuzione di un'applicazione remota**.
3. Nella sezione **Generazione del file di dump della memoria del processo in corso**, specificare il file eseguibile dell'applicazione per la quale si desidera generare un file dump.
4. Fare clic sul pulsante **Scarica file di dump**.

   Viene scaricato un archivio con il file di dump per l'applicazione specificata.

   Se l'applicazione specificata non è in esecuzione nel dispositivo client, la cartella "result" contenuta nell'archivio scaricato sarà vuota.

   Se l'applicazione specificata è in esecuzione, ma il download non riesce con un errore o la cartella "result" contenuta nell'archivio scaricato è vuota, fare riferimento alla Knowledge Base di Kaspersky Security Center.

Esecuzione della diagnostica remota in un dispositivo client basato su Linux

Kaspersky Security Center consente di scaricare le informazioni diagnostiche di base da un dispositivo client. In alternativa, è possibile ottenere le informazioni diagnostiche su un dispositivo basato su Linux utilizzando lo script collect.sh di Kaspersky. Questo script viene eseguito nel dispositivo client basato su Linux che deve essere diagnosticato, quindi genera un file con le informazioni diagnostiche, le informazioni di sistema su questo dispositivo, i file di traccia delle applicazioni, i registri del dispositivo e un file di dump per le applicazioni terminate di emergenza.

È consigliabile utilizzare lo script collect.sh per ottenere tutte le informazioni diagnostiche sul dispositivo client basato su Linux contemporaneamente. Se si scaricano le informazioni diagnostiche da remoto tramite Kaspersky Security Center, sarà necessario esaminare tutte le sezioni dell'interfaccia di diagnostica remota. Inoltre, è probabile che le informazioni diagnostiche di un dispositivo basato su Linux non vengano ottenute completamente.

Se è necessario inviare il file generato con le informazioni diagnostiche all'Assistenza tecnica di Kaspersky, eliminare tutte le informazioni riservate prima di inviare il file.

Per scaricare le informazioni diagnostiche da un dispositivo client basato su Linux utilizzando lo script collect.sh:

1. Scaricare lo script collect.sh contenuto nell'archivio collect.tar.gz.
2. Copiare l'archivio scaricato nel dispositivo client basato su Linux da diagnosticare.
3. Eseguire il seguente comando per decomprimere l'archivio collect.tar.gz:

   ```
   # tar -xzf collect.tar.gz
   ```

4. Eseguire il seguente comando per specificare i diritti di esecuzione dello script:

   ```
   # chmod +x collect.sh
   ```

5. Eseguire lo script collect.sh utilizzando un account con diritti di amministratore:

   ```
   # ./collect.sh
   ```

Un file con le informazioni diagnostiche viene generato e salvato nella cartella /tmp/$HOST_NAME-collect.tar.gz.

Download ed eliminazione dei file da Quarantena e Backup

Questa sezione fornisce informazioni su come scaricare ed eliminare file da Quarantena e Backup in Kaspersky Security Center Web Console.

Download dei file da Quarantena e Backup

È possibile scaricare i file da Quarantena e Backup solo se viene soddisfatta una delle due condizioni: l'opzione **Non eseguire la disconnessione da Administration Server** è abilitata nelle impostazioni del dispositivo oppure è in uso un gateway di connessione. In caso contrario, il download non è possibile.

Per salvare una copia del file dalla cartella Quarantena o Backup sul disco rigido:

1. Eseguire una delle seguenti operazioni:

   - Se si desidera salvare una copia del file dalla Quarantena, nel menu principale passare a **Operazioni** → **Archivi** → **Quarantena**.
   - Se si desidera salvare una copia del file da Backup, nel menu principale passare a **Operazioni** → **Archivi** → **Backup**.

2. Nella finestra visualizzata selezionare un file che si desidera scaricare e fare clic su **Scarica**.

   Il download viene avviato. Una copia del file che era stato inserito in Quarantena nel dispositivo client viene salvata nella cartella specificata.

Modifica della lingua dell'interfaccia di Kaspersky Security Center Web Console

È possibile selezionare la lingua dell'interfaccia di Kaspersky Security Center Web Console.

Per modificare la lingua dell'interfaccia:

1. Nel menu principale, passare a **Impostazioni** → **Lingua**.
2. Selezionare una delle lingue di localizzazione supportate.

Guida di riferimento API

Questa guida di riferimento di Kaspersky Security Center OpenAPI è progettata per assistere nelle seguenti attività:

- Automazione e personalizzazione. È possibile automatizzare le attività che è meglio non gestire manualmente utilizzando Administration Console. È inoltre possibile implementare scenari personalizzati non ancora supportati in Administration Console. Come amministratore è ad esempio possibile utilizzare Kaspersky Security Center OpenAPI per creare ed eseguire script che faciliteranno lo sviluppo della struttura dei gruppi di amministrazione e manterranno aggiornata tale struttura.

- Sviluppo personalizzato. È ad esempio possibile sviluppare un'Administration Console basata su MMC alternativa per i client, che consente un set limitato di azioni.

Nella guida di riferimento OpenAPI è possibile utilizzare il campo di ricerca nella parte destra dello schermo per individuare le informazioni necessarie.

GUIDA DI RIFERIMENTO OPENAPI

Esempi di script

La guida di riferimento OpenAPI contiene gli esempi di script Python elencati nella tabella seguente. Gli esempi mostrano come chiamare i metodi OpenAPI ed eseguire automaticamente varie attività per proteggere la rete, ad esempio creare una gerarchia di tipo "primario/secondario", eseguire attività in Kaspersky Security Center o assegnare punti di distribuzione. È possibile eseguire gli esempi così come sono o creare script personalizzati basati sugli esempi.

Per chiamare i metodi OpenAPI ed eseguire gli script:

1. Scaricare l'archivio KlAkOAPI.tar.gz. Questo archivio include il pacchetto KlAkOAPI e gli esempi (è possibile copiarli dall'archivio o dalla guida di riferimento OpenAPI). L'archivio KlAkOAPI.tar.gz si trova anche nella cartella di installazione di Kaspersky Security Center.

2. Installare il pacchetto KlAkOAPI dall'archivio KlAkOAPI.tar.gz in un dispositivo in cui è installato Administration Server.

   È possibile chiamare i metodi OpenAPI, eseguire gli esempi e gli script personalizzati solo nei dispositivi in cui sono installati Administration Server e il pacchetto KlAkOAPI.

Corrispondenza tra scenari utente ed esempi di metodi Kaspersky Security Center OpenAPI

Esempio	Finalità dell'esempio	Scenario
Registro KlAkParams	È possibile estrarre ed elaborare i dati utilizzando la struttura di dati `KlAkParams`. L'esempio mostra come utilizzare questa struttura di dati. Il risultato dell'esempio può presentarsi in diversi modi. È possibile ottenere i dati per inviare un metodo HTTP o per utilizzarlo nel proprio codice.	Monitoraggio e generazione dei rapporti
Creazione ed eliminazione di una gerarchia "primaria/secondaria"	È possibile aggiungere un Administration Server secondario e stabilire una gerarchia "primaria/secondaria". In alternativa, è possibile disconnettere l'Administration Server secondario dalla gerarchia.	• Creazione di una gerarchia di Administration Server: l'aggiunta un Administration Server secondario • Eliminazione di una gerarchia di Administration Server
Creare la gerarchia dei gruppi con una struttura basata sull'unità Active Directory	È possibile eseguire il polling dell'unità Active Directory e formare una gerarchia dei gruppi di dispositivi rilevati.	Creazione dei gruppi di amministrazione
Creare la gerarchia dei gruppi con una struttura basata sull'unità Active Directory memorizzata nella cache	È possibile formare una gerarchia dei gruppi di dispositivi gestiti basata sull'unità Active Directory di cui è stato precedentemente eseguito il polling. Se vengono visualizzati nuovi dispositivi in Active Directory dopo l'ultimo polling, questi non vengono aggiunti al gruppo perché non sono tra i risultati del polling salvati.	Creazione dei gruppi di amministrazione
Scaricare i file dell'elenco di reti tramite il gateway di connessione nel dispositivo specificato	È possibile connettersi a Network Agent nel dispositivo necessario utilizzando un gateway di connessione, quindi scaricare un file con l'elenco di reti nel dispositivo.	Regolazione di punti di distribuzione e gateway di connessione
Installazione di una chiave di licenza archiviata nell'archivio primario dell'Administration Server sugli Administration Server secondari	È possibile connettersi all'Administration Server primario, scaricare una chiave di licenza richiesta da questo e trasmettere tale chiave a tutti gli Administration Server secondari inclusi in una gerarchia.	Licensing delle applicazioni gestite
Creare un rapporto dei diritti utente effettivi	È possibile creare diversi rapporti. È ad esempio possibile generare il rapporto dei diritti utente effettivi utilizzando questo esempio. Questo rapporto descrive i diritti di cui dispone un utente, a seconda del relativo gruppo e ruolo. È possibile scaricare il rapporto in formato HTML, PDF o Excel.	Generazione e visualizzazione di un rapporto
Avviare un'attività per un dispositivo	È possibile connettersi a Network Agent nel dispositivo necessario utilizzando un gateway di connessione, quindi eseguire l'attività necessaria.	Avvio manuale di un'attività

Esempio	Finalità dell'esempio	Scenario
Creare subnet IP basate su sito e servizi di Active Directory	È possibile creare una subnet IP basata sull'unità Active Directory utilizzata. L'esempio avvia il polling dell'intervallo IP specificato ed elimina le subnet rilevate per evitare il conflitto con una nuova subnet. Di conseguenza, non eseguire questo esempio nella rete in cui è importante mantenere le subnet. Dopo il polling, l'esempio fa riferimento ad Active Directory, esamina ogni dispositivo al suo interno e crea la subnet IP. A tale scopo, l'esempio utilizza le maschere e gli indirizzi IP di tutti i dispositivi.	Configurazione della protezione di rete
Registrare i punti di distribuzione per i dispositivi in un gruppo	È possibile assegnare dispositivi gestiti come punti di distribuzione (precedentemente noti come Update Agent).	Aggiornamento di database e applicazioni Kaspersky
Enumerare tutti i gruppi	È possibile eseguire varie azioni con i gruppi di amministrazione. L'esempio mostra come effettuare le seguenti operazioni: • Ottenere un identificatore del gruppo radice "Dispositivi gestiti" • Spostarsi nella gerarchia dei gruppi • Recuperare la gerarchia completa ed estesa dei gruppi, insieme ai relativi nomi e livelli di nidificazione	Configurazione di Administration Server
Enumerare le attività, eseguire query sulle statistiche delle attività ed eseguire un'attività	È possibile trovare le seguenti informazioni: • Cronologia dell'avanzamento dell'attività • Stato dell'attività corrente • Numero di attività con diversi stati È inoltre possibile eseguire un'attività. Per impostazione predefinita, l'esempio esegue un'attività dopo aver generato le statistiche.	Monitoraggio dell'esecuzione delle attività
Creare ed eseguire un'attività	È possibile creare un'attività. Specificare i seguenti parametri dell'attività nell'esempio: • Tipo • Metodo di esecuzione • Nome • Gruppo di dispositivi per cui verrà utilizzata l'attività Per impostazione predefinita, l'esempio crea un'attività con il tipo "Mostra messaggio". È possibile eseguire questa attività per tutti i dispositivi gestiti di Administration Server. Se necessario, è possibile specificare i propri parametri dell'attività.	Creazione di un'attività
Enumerare le chiavi di licenza	È possibile ottenere un elenco di tutte le chiavi di licenza attive per le applicazioni Kaspersky installate nei dispositivi gestiti di Administration Server. L'elenco contiene dati dettagliati su ogni chiave di licenza, tra cui nome, tipo o data di scadenza.	Visualizzazione delle informazioni sulle chiavi di licenza in uso
Creare e trovare un utente interno	È possibile creare un account per utilizzi successivi.	Selezione dell'account per l'avvio di Administration Server
Creare una categoria personalizzata	È possibile creare la categoria di applicazioni con i parametri necessari.	Creazione di una categoria di applicazioni con contenuto aggiunto manualmente
Enumerare gli utenti utilizzando SrvView	È possibile utilizzare la classe SrvView per richiedere informazioni dettagliate da Administration Server. È ad esempio possibile ottenere un elenco di utenti utilizzando questo esempio.	Gestione degli account utente

Applicazioni che interagiscono con Kaspersky Security Center tramite OpenAPI

Alcune applicazioni interagiscono con Kaspersky Security Center tramite OpenAPI. Tra queste applicazioni sono incluse, ad esempio, Kaspersky Anti Targeted Attack Platform o Kaspersky Security for Virtualization. Può anche trattarsi di un'applicazione client personalizzata sviluppata dall'utente su OpenAPI.

Le applicazioni che interagiscono con Kaspersky Security Center tramite OpenAPI si connettono ad Administration Server. Se è stato configurato un elenco di indirizzi IP consentiti per la connessione ad Administration Server, aggiungere gli indirizzi IP dei dispositivi in cui sono installate le applicazioni che utilizzano Kaspersky Security Center OpenAPI. Per scoprire se l'applicazione in uso funziona con OpenAPI, vedere la Guida di tale applicazione.

Procedure consigliate per i provider di servizi

Questa sezione fornisce informazioni su come configurare e utilizzare Kaspersky Security Center.

Questa sezione contiene raccomandazioni relative alla distribuzione, alla configurazione e all'utilizzo dell'applicazione e descrive come risolvere i problemi più comuni che possono verificarsi durante l'esecuzione dell'applicazione.

Pianificazione della distribuzione di Kaspersky Security Center

Durante la pianificazione della distribuzione dei componenti di Kaspersky Security Center nella rete di un'organizzazione, è necessario tenere conto delle dimensioni e dell'ambito del progetto, in particolare per quanto riguarda i seguenti fattori:

- Numero totale di dispositivi
- Numero di client MSP

Un solo Administration Server può supportare un massimo di 100.000 dispositivi. Se il numero totale di dispositivi nella rete di un'organizzazione è superiore a 100.000, il provider di servizi deve distribuire più Administration Server, che possono essere combinati in una gerarchia per gestirli comodamente in modo centralizzato.

È possibile creare fino a 500 Server virtuali in un singolo Administration Server, pertanto è richiesto un singolo Administration Server ogni 500 client MSP.

In fase di pianificazione della distribuzione, deve essere valutata l'assegnazione di uno speciale certificato X.509 all'Administration Server. L'assegnazione del certificato X.509 all'Administration Server può essere utile nei seguenti casi (elenco parziale):

- Ispezione del traffico SSL (Secure Sockets Layer) per mezzo di un proxy con terminazione SSL
- Specificazione dei valori richiesti nei campi del certificato
- Specificazione del livello di criptaggio richiesto di un certificato

Concessione dell'accesso via Internet all'Administration Server

Per consentire ai dispositivi nella rete client di accedere ad Administration Server via Internet, è necessario rendere disponibili le seguenti porte di Administration Server:

- TCP 13000: porta TLS di Administration Server per la connessione dei Network Agent distribuiti nella rete client
- TCP 8061: porta HTTPS per la pubblicazione dei pacchetti indipendenti utilizzando gli strumenti di Administration Console

- TCP 8060: porta HTTP per la pubblicazione dei pacchetti indipendenti utilizzando gli strumenti di Administration Console

- TCP 13292: porta TLS necessaria solo se sono presenti dispositivi mobili da gestire

Se si desidera offrire ai client le opzioni di base per l'amministrazione della rete tramite Kaspersky Security Center Web Console, è necessario aprire anche la porta 8080 TCP (porta HTTPS) di Kaspersky Security Center Web Console:

Configurazione standard di Kaspersky Security Center

Uno o più Administration Server vengono distribuiti nei server degli MSP. Il numero di Administration Server che è possibile selezionare può essere basato sull'hardware disponibile, sul numero totale di client MSP gestiti o sul numero totale di dispositivi gestiti.

Un solo Administration Server può supportare fino a 100.000 dispositivi. È necessario tenere conto della possibilità di aumentare il numero di dispositivi gestiti in futuro: può essere utile connettere un numero più limitato di dispositivi a un singolo Administration Server.

È possibile creare fino a 500 Server virtuali in un singolo Administration Server, pertanto è richiesto un singolo Administration Server ogni 500 client MSP.

Se vengono utilizzati più server, è consigliabile combinarli in una gerarchia. L'utilizzo di una gerarchia di Administration Server consente di evitare la duplicazione di criteri e attività e di amministrare l'intero set di dispositivi gestiti come se fossero gestiti da un singolo Administration Server (ricerca di dispositivi, creazione di selezioni di dispositivi e generazione di rapporti).

In ogni server virtuale corrispondente a un client MSP è necessario assegnare uno o più punti di distribuzione. Se i client MSP e Administration Server sono collegati via Internet, può essere utile creare un'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per i punti di distribuzione, in modo che scarichino gli aggiornamenti direttamente dai server di Kaspersky, invece che da Administration Server.

Se alcuni dispositivi della rete client MSP non hanno accesso diretto a Internet, è necessario attivare la modalità gateway di connessione per i punti di distribuzione. In questo caso, i Network Agent nei dispositivi nella rete del client MSP saranno connessi per l'ulteriore sincronizzazione ad Administration Server, ma attraverso il gateway, non direttamente.

Poiché in genere Administration Server non è in grado di eseguire il polling nella rete del client MSP, può essere utile assegnare questa funzione a un punto di distribuzione.

Administration Server non potrà inviare notifiche tramite la porta UDP 15000 ai dispositivi gestiti posizionati dietro il NAT nella rete del client MSP. Per risolvere questo problema, può essere utile abilitare la modalità di connessione continua ad Administration Server nelle proprietà dei dispositivi che operano come punti di distribuzione e vengono eseguiti in modalità gateway di connessione (casella di controllo **Non eseguire la disconnessione da Administration Server**). La modalità di connessione continua è disponibile se il numero totale di punti di distribuzione non è superiore a 300.

Informazioni sui punti di distribuzione

Il dispositivo in cui è installato Network Agent può essere utilizzato come punto di distribuzione. In questa modalità, Network Agent può eseguire le seguenti funzioni:

- Trasferire file ai dispositivi client, tra cui:
  - Aggiornamenti dei moduli software e database Kaspersky

    Gli aggiornamenti possono essere recuperati dall'Administration Server o dai server di Kaspersky. Nel secondo caso, è necessario creare l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* per il dispositivo che opera come punto di distribuzione.
  - Aggiornamenti software di terze parti
  - Pacchetti di installazione
  - Aggiornamenti di Windows quando si utilizza Administration Server come server WSUS
- Installare il software (inclusa la distribuzione iniziale dei Network Agent) in altri dispositivi.
- Eseguire il polling della rete per rilevare nuovi dispositivi e aggiornare le informazioni sui dispositivi esistenti. Un punto di distribuzione può applicare gli stessi metodi di device discovery di Administration Server.

La distribuzione dei punti di distribuzione nella rete di un'organizzazione ha i seguenti obiettivi:

- Ridurre il carico su Administration Server se questo opera come sorgente degli aggiornamenti.
- Ottimizzare il traffico Internet poiché, in questo caso, ogni dispositivo nella rete del client MSP non deve accedere ai server di Kaspersky o ad Administration Server per gli aggiornamenti.
- Concedere l'accesso ad Administration Server ai dispositivi dietro il NAT (rispetto ad Administration Server) della rete del client MSP, consentendo ad Administration Server di eseguire le seguenti azioni:
  - Inviare notifiche ai dispositivi tramite UDP nella rete IPv4 o IPv6
  - Eseguire il polling della rete IPv4 o IPv6
  - Eseguire la distribuzione iniziale
  - Fungere da server push

Un punto di distribuzione viene assegnato a un gruppo di amministrazione. In questo caso, l'ambito del punto di distribuzione include tutti i dispositivi contenuti nel gruppo di amministrazione e in tutti i relativi sottogruppi. Tuttavia, il dispositivo che opera come punto di distribuzione può non essere incluso nel gruppo di amministrazione a cui è stato assegnato.

È possibile far funzionare un punto di distribuzione come gateway di connessione. In questo caso, i dispositivi nell'ambito del punto di distribuzione saranno connessi all'Administration Server tramite il gateway, non direttamente. È possibile utilizzare questa modalità negli scenari che non consentono di stabilire una connessione diretta tra i dispositivi con Network Agent e un Administration Server.

I dispositivi che operano come punti di distribuzione devono essere protetti, anche da un punto di vista fisico, da qualsiasi accesso non autorizzato.

Gerarchia di Administration Server

Un MSP può eseguire diversi Administration Server. Poiché può essere scomodo amministrare più Administration Server distinti, è possibile applicare una gerarchia. Una configurazione "primario/secondario" per due Administration Server fornisce le seguenti opzioni:

- Un Administration Server secondario eredita i criteri e le attività dall'Administration Server primario, evitando così la duplicazione delle impostazioni.
- Le selezioni di dispositivi nell'Administration Server primario possono includere i dispositivi degli Administration Server secondari.
- I rapporti nell'Administration Server primario possono contenere dati (incluse informazioni dettagliate) ottenuti dagli Administration Server secondari.

L'Administration Server primario riceve i dati solo dagli Administration Server secondari non virtuali nell'ambito delle opzioni elencate sopra. Questa limitazione non si applica agli Administration Server virtuali, che condividono il database con l'Administration Server primario.

Administration Server virtuali

Sulla base di un Administration Server fisico, è possibile creare più Administration Server virtuali, simili agli Administration Server secondari. Rispetto al modello di accesso discrezionale, che è basato su elenchi di controllo di accesso (ACL), il modello degli Administration Server virtuali è più funzionale e fornisce un maggior livello di isolamento. Oltre a una struttura dedicata di gruppi di amministrazione per i dispositivi assegnati con criteri e attività, ogni Administration Server virtuale dispone di un proprio gruppo di dispositivi non assegnati, di insiemi di rapporti, dispositivi ed eventi selezionati, pacchetti di installazione, regole di spostamento e così via. Per il massimo isolamento reciproco dei client MSP, è consigliabile scegliere Administration Server virtuali come funzionalità da utilizzare. Inoltre, la creazione di un Administration Server virtuale per ogni client MSP consente di offrire ai client opzioni di base per l'amministrazione della rete tramite Kaspersky Security Center Web Console.

Gli Administration Server virtuali sono molto simili agli Administration Server secondari, ma con le seguenti distinzioni:

- Un Administration Server virtuale non dispone della maggior parte delle impostazioni globali e di specifiche porte TCP.
- Un Administration Server virtuale non dispone di Administration Server secondari.
- Un Administration Server virtuale non include altri Administration Server virtuali.
- Un Administration Server fisico visualizza i dispositivi, i gruppi, gli eventi e gli oggetti nei dispositivi gestiti (elementi in Quarantena, registro delle applicazioni e così via) di tutti i relativi Administration Server virtuali.
- Un Administration Server virtuale può eseguire solo la scansione della rete a cui sono connessi punti di distribuzione.

Gestione dei dispositivi mobili con Kaspersky Endpoint Security for Android

I dispositivi mobili in cui è installato Kaspersky Endpoint Security for Android™ (di seguito denominati dispositivi KES) sono gestiti tramite l'Administration Server. Kaspersky Security Center supporta le seguenti funzionalità per la gestione dei dispositivi KES:

- Gestione dei dispositivi mobili come dispositivi client:
  - Appartenenza ai gruppi di amministrazione
  - Monitoraggio, ad esempio la visualizzazione di stati, eventi e rapporti
  - Modifica delle impostazioni locali e assegnazione di criteri per Kaspersky Endpoint Security for Android
- Invio di comandi in modalità centralizzata
- Installazione remota di pacchetti app mobili

Administration Server gestisce i dispositivi KES tramite TLS, porta TCP 13292.

Distribuzione e configurazione iniziale

Kaspersky Security Center è un'applicazione distribuita. Kaspersky Security Center include le seguenti applicazioni:

- Administration Server - Il componente principale, progettato per la gestione dei dispositivi di un'organizzazione e l'archiviazione dei dati in un sistema DBMS.
- Administration Console - Lo strumento di base per l'amministratore. Administration Console è distribuito insieme ad Administration Server, ma può anche essere installato singolarmente in uno o più dispositivi eseguiti dall'amministratore.
- Kaspersky Security Center Web Console — Un'interfaccia Web per Administration Server pensata per le operazioni di base. È possibile installare il componente in qualsiasi dispositivo che soddisfi i requisiti hardware e software.
- Network Agent: utilizzato per gestire l'applicazione di protezione installata in un dispositivo, nonché per ottenere informazioni sul dispositivo. I Network Agent vengono installati nei dispositivi di un'organizzazione.

La distribuzione di Kaspersky Security Center nella rete di un'organizzazione viene eseguita come segue:

- Installazione di Administration Server
- Installazione di Kaspersky Security Center Web Console
- Installazione di Administration Console nel dispositivo dell'amministratore
- Installazione di Network Agent e dell'applicazione di protezione nei dispositivi dell'organizzazione

Raccomandazioni sull'installazione di Administration Server

Questa sezione contiene raccomandazioni su come installare Administration Server. Vengono inoltre illustrati gli scenari per l'utilizzo di una cartella condivisa nel dispositivo con Administration Server per distribuire Network Agent nei dispositivi client.

Creazione degli account per i servizi di Administration Server in un cluster di failover

Per impostazione predefinita, il programma di installazione crea automaticamente account senza privilegi per i servizi di Administration Server. Questo comportamento è il più appropriato per l'installazione di Administration Server in un normale dispositivo.

Tuttavia, l'installazione di Administration Server in un cluster di failover richiede uno scenario diverso:

1. Creare account di dominio senza privilegi per i servizi di Administration Server e includerli in un gruppo di sicurezza di dominio globale denominato KLAdmins.

2. Nel programma di installazione di Administration Server specificare gli account di dominio che sono stati creati per i servizi.

Selezione di un DBMS

Durante la selezione del sistema di gestione database (DBMS) che deve essere utilizzato da un Administration Server, è necessario tenere conto del numero di dispositivi coperti dall'Administration Server.

Nella seguente tabella, sono elencate le opzioni DBMS valide, nonché i suggerimenti e le limitazioni per il relativo utilizzo.

Suggerimenti e limitazioni su DBMS

DBMS	Suggerimenti e limitazioni
SQL Server Express Edition 2016 o versione successiva	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 10.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. È possibile limitare il numero massimo di eventi nell'archivio eventi per evitare l'overflow del database. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database. L'utilizzo simultaneo del DBMS SQL Server Express Edition da parte di Administration Server e di un'altra applicazione non è consentito. Il database Microsoft SQL Express non è supportato per l'attività **Esegui sincronizzazione di Windows Update**.
Edizione di SQL Server in locale diversa da Express, 2016 o versione successiva	Nessuna limitazione.
Edizione di SQL Server in remoto diversa da Express, 2016 o successiva	Valida solo se entrambi i dispositivi si trovano nello stesso dominio Windows®. Se i domini sono differenti, è necessario stabilire una relazione di trust bidirezionale tra di essi.

DBMS	Suggerimenti e limitazioni
MySQL 5.5, 5.6 o 5.7 in locale o in remoto (le versioni 5.5.1, 5.5.2, 5.5.3, 5.5.4 e 5.5.5 di MySQL non sono più supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 10.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database.
MySQL 8.0.20 locale o remoto o versioni successive	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 50.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database.
MariaDB locale o remoto (vedere le versioni supportate)	Utilizzare questo DBMS se si intende eseguire un singolo Administration Server per meno di 20.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database.
PostgreSQL, Postgres Pro (vedere le versioni supportate)	Utilizzare uno di questi DBMS se si intende eseguire un singolo server di amministrazione per meno di 50.000 dispositivi. Si consiglia di disabilitare l'attività Inventario software e disabilitare (nelle impostazioni del criterio di Kaspersky Endpoint Security) le notifiche di Administration Server nelle applicazioni avviate. Fare riferimento al seguente argomento per i dettagli: Calcolo dello spazio del database.

Se si utilizza un DBMS PostgreSQL, MariaDB o MySQL, la scheda **Eventi** potrebbe mostrare un elenco incompleto di eventi per il dispositivo client selezionato. Questo si verifica quando il DBMS archivia una quantità molto elevata di eventi. È possibile aumentare il numero di eventi visualizzati effettuando una delle seguenti operazioni:

- Rimozione degli eventi non necessari.
- Riduzione del periodo di archiviazione per gli eventi non necessari.

Per visualizzare un elenco completo degli eventi registrati in Administration Server per il dispositivo, utilizzare Rapporti.

Se si utilizza SQL Server 2019 come DBMS e non si dispone della patch cumulativa CU12 o versione successiva, è necessario eseguire le seguenti operazioni dopo l'installazione di Kaspersky Security Center:

1. Stabilire la connessione a SQL Server utilizzando SQL Management Studio.
2. Eseguire il seguente comando (se è stato selezionato un nome diverso per il database, utilizza quel nome invece di KAV):

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. Riavviare il servizio SQL Server 2019.

In alternativa, l'utilizzo di SQL Server 2019 può generare errori, ad esempio "Memoria di sistema insufficiente nel pool di risorse 'interno' per l'esecuzione di questa query".

Specificazione dell'indirizzo dell'Administration Server

Durante l'installazione di Administration Server, è necessario specificare l'indirizzo esterno di Administration Server. Questo indirizzo sarà utilizzato come indirizzo predefinito al momento della creazione dei pacchetti di installazione di Network Agent. Sarà quindi possibile modificare l'indirizzo dell'host di Administration Server utilizzando gli strumenti di Administration Console. L'indirizzo non sarà modificato automaticamente nei pacchetti di installazione di Network Agent che sono stati già creati.

Configurazione della protezione nella rete di un'organizzazione client

Al termine dell'installazione di Administration Server, Administration Console viene avviato e richiede di eseguire la configurazione iniziale tramite la procedura guidata appropriata. Durante l'esecuzione dell'Avvio rapido guidato, i seguenti criteri e attività vengono creati nel gruppo di amministrazione radice:

- Criterio di Kaspersky Endpoint Security
- Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security
- Attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security
- Criterio di Network Agent
- Attività Scansione vulnerabilità (attività di Network Agent)
- Attività di installazione degli aggiornamenti e correzione delle vulnerabilità (attività di Network Agent)

I criteri e le attività sono creati con le impostazioni predefinite, che possono risultare non ottimali o perfino non utilizzabili per l'organizzazione. È pertanto necessario verificare le proprietà degli oggetti che sono stati creati e modificarle manualmente, se necessario.

Questa sezione contiene informazioni sulla configurazione manuale di criteri, attività e altre impostazioni di Administration Server, nonché le informazioni sul punto di distribuzione, sulla creazione di una struttura di gruppi di amministrazione e di una gerarchia di attività e altre impostazioni.

Configurazione manuale del criterio di Kaspersky Endpoint Security

Questa sezione fornisce raccomandazioni su come configurare il criterio di Kaspersky Endpoint Security, creato dall'Avvio rapido guidato. È possibile eseguire la configurazione nella finestra delle proprietà del criterio.

Durante la modifica di un'impostazione, tenere presente che è necessario fare clic sull'icona di blocco sopra l'impostazione appropriata per consentire l'utilizzo del relativo valore su una workstation.

Configurazione del criterio nella sezione Protezione minacce avanzata

Per una descrizione completa delle impostazioni in questa sezione, fare riferimento alla documentazione di Kaspersky Endpoint Security for Windows.

Nella sezione **Protezione minacce avanzata** è possibile configurare l'utilizzo di Kaspersky Security Network per Kaspersky Endpoint Security for Windows. È inoltre possibile configurare i moduli di Kaspersky Endpoint Security for Windows, ad esempio Rilevamento del Comportamento, Prevenzione Exploit, Prevenzione Intrusioni Host e Motore di Remediation.

Nella sottosezione **Kaspersky Security Network** è consigliabile abilitare l'opzione **Kaspersky Security Network**. L'utilizzo di questa opzione consente di ridistribuire e ottimizzare il traffico nella rete. Se l'opzione **Kaspersky Security Network** è disabilitata, è possibile abilitare l'uso diretto dei server KSN.

Configurazione del criterio nella sezione Protezione minacce essenziale

Per una descrizione completa delle impostazioni in questa sezione, fare riferimento alla documentazione di Kaspersky Endpoint Security for Windows.

Nella sezione **Protezione minacce essenziale** della finestra delle proprietà del criterio, si consiglia di specificare impostazioni aggiuntive nelle sottosezioni **Firewall** e **Protezione minacce file**.

La sottosezione **Firewall** contiene le impostazioni che consentono di controllare le attività di rete delle applicazioni sui dispositivi client. Un dispositivo client utilizza una rete a cui è assegnato uno dei seguenti stati: pubblico, locale o attendibile. A seconda dello stato della rete, Kaspersky Endpoint Security può consentire o negare le attività di rete su un dispositivo. Quando si aggiunge una nuova rete all'organizzazione, è necessario assegnare uno stato di rete appropriato a questa. Ad esempio, se il dispositivo client è un laptop, si consiglia che questo dispositivo utilizzi la rete pubblica o attendibile, poiché il laptop non è sempre connesso alla rete locale. Nella sottosezione **Firewall**, è possibile verificare se sono stati assegnati correttamente gli stati alle reti utilizzate nell'organizzazione.

Per controllare l'elenco delle reti:

1. Nelle proprietà del criterio, passare a **Protezione minacce essenziale** → **Firewall**.
2. Nella sezione **Reti disponibili**, fare clic sul pulsante **Impostazioni**.
3. Nella finestra **Firewall** visualizzata, passare alla scheda **Reti** per visualizzare l'elenco delle reti.

Nella sottosezione **Protezione minacce file**, è possibile disabilitare la scansione delle unità di rete. La scansione delle unità di rete può comportare un carico significativo per le unità di rete. È più pratico eseguire la scansione indiretta sui file server.

Per disabilitare la scansione delle unità di rete:

1. Nelle proprietà del criterio, passare a **Protezione minacce essenziale** → **Protezione minacce file**.
2. Nella sezione **Livello di sicurezza**, fare clic sul pulsante **Impostazioni**.
3. Nella finestra **Protezione minacce file** visualizzata, nella scheda **Generali**, deselezionare la casella di controllo **Tutte le unità di rete**.

Configurazione del criterio nella sezione Impostazioni generali

Per la descrizione completa delle impostazioni in questa sezione, fare riferimento alla documentazione di Kaspersky Endpoint Security.

Di seguito sono descritte le operazioni di configurazione avanzate che è consigliabile eseguire nella sezione **Impostazioni generali** della finestra delle proprietà del criterio di Kaspersky Endpoint Security.

Sezione Impostazioni generali, sottosezione Rapporti e archivi

Nella sezione **Trasferimento dei dati ad Administration Server**, notare la casella di controllo **Informazioni sulle applicazioni avviate**. Se questa casella di controllo è selezionata, il database di Administration Server salva informazioni su tutte le versioni di tutti i moduli software nei dispositivi connessi alla rete. Queste informazioni possono richiedere una quantità significativa di spazio su disco nel database di Kaspersky Security Center (decine di gigabyte). Pertanto, se la casella di controllo **Informazioni sulle applicazioni avviate** è ancora selezionata nel criterio di primo livello, deve essere deselezionata.

Sezione Impostazioni generali, sottosezione Interfaccia

Se la protezione dalle minacce nella rete dell'organizzazione deve essere gestita in modalità centralizzata tramite Administration Console, è necessario disabilitare la visualizzazione dell'interfaccia di utente di Kaspersky Endpoint Security nelle workstation (deselezionando la casella di controllo **Visualizza interfaccia applicazione** nella sezione **Interazione con l'utente**) e abilitare la protezione tramite password (selezionando la casella di controllo **Abilita la protezione tramite password** nella sezione **Protezione tramite password**).

Configurazione del criterio nella sezione Configurazione eventi

Nella sezione **Configurazione eventi** è consigliabile disabilitare il salvataggio di qualsiasi evento in Administration Server, tranne i seguenti:

- Nella scheda **Critico**:
  - *L'esecuzione automatica dell'applicazione è disabilitata*
  - *Accesso negato*
  - *Avvio dell'applicazione non consentito*
  - *Disinfezione impossibile*
  - *Contratto di licenza con l'utente finale violato*
  - *Impossibile caricare il modulo di criptaggio*
  - *Impossibile avviare due attività contemporaneamente*
  - *È stata rilevata una minaccia attiva. Si consiglia di avviare Disinfezione avanzata*
  - *Attacco di rete rilevato*
  - *Non tutti i componenti sono stati aggiornati*
  - *Errore di attivazione*
  - *Errore durante l'abilitazione della modalità portatile*
  - *Errore durante l'interazione con Kaspersky Security Center*
  - *Errore durante la disabilitazione della modalità portatile*
  - *Errore durante la modifica dei componenti dell'applicazione*
  - *Errore durante l'applicazione delle regole di criptaggio/decriptaggio dei file*
  - *Il criterio non può essere applicato*
  - *Processo terminato*
  - *Attività di rete bloccata*
- Nella scheda **Errore funzionale**: *Impostazioni attività non valide. Impostazioni non applicate*

- Nella scheda **Avviso**:
  - *L'Auto-difesa è disabilitata*
  - *Chiave di riserva errata*
  - *L'utente ha scelto di non applicare il criterio di criptaggio*
- Nella scheda **Informazioni**: *Avvio dell'applicazione non consentito in modalità di test*

Configurazione manuale dell'attività di gruppo di aggiornamento per Kaspersky Endpoint Security

Se Administration Server opera come sorgente degli aggiornamenti, l'opzione di pianificazione ottimale e consigliata per Kaspersky Endpoint Security è **Quando vengono scaricati nuovi aggiornamenti nell'archivio** con la casella di controllo **Usa automaticamente il ritardo casuale per l'avvio delle attività** selezionata.

Se si crea un'attività locale di download degli aggiornamenti dai server Kaspersky nell'archivio in ogni punto di distribuzione, la pianificazione periodica sarà ottimale e consigliata per l'attività di aggiornamento di gruppo di Kaspersky Endpoint Security. In questo caso, il valore dell'intervallo con impostazione casuale deve essere impostato su 1 ora.

Configurazione manuale dell'attività di gruppo per la scansione di un dispositivo con Kaspersky Endpoint Security

L'Avvio rapido guidato crea un'attività di gruppo per la scansione di un dispositivo. Per impostazione predefinita, all'attività viene assegnata una pianificazione **Esegui il venerdì alle 19:00** con un'impostazione casuale automatica e la casella di controllo **Esegui attività non effettuate** è deselezionata.

Di conseguenza, se i dispositivi in un'organizzazione vengono spenti ad esempio il venerdì alle 18:30, l'attività di scansione del dispositivo non verrà eseguita. È necessario impostare la pianificazione appropriata per questa attività in base alle regole per l'ambiente di lavoro adottate nell'organizzazione.

Pianificazione dell'attività Trova vulnerabilità e aggiornamenti richiesti

L'Avvio rapido guidato crea l'attività *Trova vulnerabilità e aggiornamenti richiesti* per Network Agent. Per impostazione predefinita, all'attività viene assegnata una pianificazione **Esegui il martedì alle 19:00** con un'impostazione casuale automatica e la casella di controllo **Esegui attività non effettuate** è selezionata.

Se le regole dell'organizzazione per l'ambiente di lavoro prevedono lo spegnimento di tutti i dispositivi in tale orario, l'attività *Trova vulnerabilità e aggiornamenti richiesti* verrà eseguita dopo la riaccensione dei dispositivi, il mercoledì mattina. Un'attività di questo tipo potrebbe essere indesiderabile perché una Scansione vulnerabilità può aumentare il carico sui sottosistemi del disco e della CPU. È necessario impostare la pianificazione appropriata per l'attività in base alle regole per l'ambiente di lavoro adottate nell'organizzazione.

Configurazione manuale dell'attività di gruppo per l'installazione degli aggiornamenti e la correzione delle vulnerabilità

L'Avvio rapido guidato crea un'attività di gruppo per l'installazione degli aggiornamenti e la correzione delle vulnerabilità per Network Agent. Per impostazione predefinita, l'attività è impostata per l'esecuzione ogni giorno alle 01:00, con un'impostazione casuale automatica, e l'opzione **Esegui attività non effettuate** non è abilitata.

Se le regole dell'organizzazione per l'ambiente di lavoro prevedono lo spegnimento dei dispositivi durante la notte, l'installazione degli aggiornamenti non verrà eseguita. È necessario impostare la pianificazione appropriata per l'attività Scansione vulnerabilità in base alle regole per l'ambiente di lavoro adottate nell'organizzazione. È anche importante tenere presente che l'installazione degli aggiornamenti può richiedere il riavvio del dispositivo.

Creazione di una struttura di gruppi di amministrazione e assegnazione dei punti di distribuzione

Una struttura di gruppi di amministrazione in Kaspersky Security Center esegue le seguenti funzioni:

- Imposta l'ambito dei criteri.

  È disponibile un metodo alternativo per l'applicazione delle impostazioni appropriate nei dispositivi, utilizzando i profili criterio. In questo caso, l'ambito dei criteri viene definito ad esempio con tag, posizioni dei dispositivi nelle unità organizzative di Active Directory e appartenenza a gruppi di protezione di Active Directory.

- Imposta l'ambito delle attività di gruppo.

  Esiste un approccio alla definizione dell'ambito delle attività di gruppo che non è basato su una gerarchia di gruppi di amministrazione: l'utilizzo di attività per selezioni dispositivi e di attività per dispositivi specifici.

- Imposta i diritti di accesso a dispositivi, Administration Server virtuali e Administration Server secondari.

- Assegna i punti di distribuzione.

Al momento della creazione della struttura dei gruppi di amministrazione, è necessario tenere conto della topologia della rete dell'organizzazione per l'assegnazione ottimale dei punti di distribuzione. La distribuzione ottimale dei punti di distribuzione consente di ridurre il traffico nella rete dell'organizzazione.

A seconda dello schema dell'organizzazione e della topologia di rete adottata dal client MSP, le seguenti configurazioni standard possono essere applicate alla struttura dei gruppi di amministrazione:

- Singola sede

- Più sedi separate di piccole dimensioni

Configurazione del client MSP standard: singola sede

In una configurazione standard con una singola sede, tutti i dispositivi si trovano nella rete dell'organizzazione e sono visibili reciprocamente. La rete dell'organizzazione può comprendere diversi componenti (reti o segmenti di rete) connessi tramite canali con larghezza di banda ridotta.

Sono disponibili i seguenti metodi per creare la struttura dei gruppi di amministrazione:

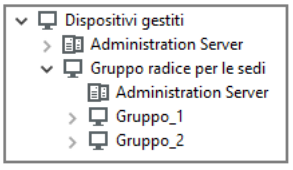
- Creazione della struttura dei gruppi di amministrazione tenendo conto della topologia di rete. La struttura dei gruppi di amministrazione potrebbe non riflettere la topologia di rete alla perfezione. Una corrispondenza tra i diversi componenti della rete e alcuni gruppi di amministrazione può essere sufficiente. È possibile utilizzare l'assegnazione automatica dei punti di distribuzione o assegnarli manualmente.

- Creazione della struttura dei gruppi di amministrazione senza tenere conto della topologia di rete. In questo caso è necessario disabilitare l'assegnazione automatica dei punti di distribuzione e quindi assegnare a uno o più dispositivi il ruolo di punti di distribuzione per un gruppo di amministrazione radice in ciascun componente della rete, ad esempio per il gruppo **Dispositivi gestiti**. Tutti i punti di distribuzione saranno allo stesso livello e avranno lo stesso ambito che comprende tutti i dispositivi della rete dell'organizzazione. In questo caso, tutti i Network Agent si connetteranno al punto di distribuzione con il percorso più vicino. Il percorso di un punto di distribuzione è monitorabile con l'utilità tracert.

Configurazione del client MSP standard: più sedi remote di piccole dimensioni

Questa configurazione standard prevede la presenza di diverse sedi remote, che possono comunicare con la sede centrale via Internet. Ogni sede remota è situata dietro il NAT, ovvero la connessione da una sede remota all'altra non è possibile perché le sedi sono isolate tra loro.

La configurazione deve essere riflessa nella struttura dei gruppi di amministrazione: è necessario creare un gruppo di amministrazione distinto per ogni sede remota (i gruppi **Sede 1** e **Sede 2** nella figura seguente).



Le sedi remote sono incluse nella struttura dei gruppi di amministrazione

È necessario assegnare uno o più punti di distribuzione a ogni gruppo di amministrazione che corrisponde a una sede. I punti di distribuzione devono essere dispositivi nella sede remota con una quantità sufficiente di spazio libero su disco. I dispositivi distribuiti nel gruppo **Sede 1**, ad esempio, accederanno ai punti di distribuzione assegnati al gruppo di amministrazione **Sede 1**.

Se alcuni utenti si spostano fisicamente tra le sedi con i loro computer portatili, è necessario selezionare due o più dispositivi (oltre ai punti di distribuzione esistenti) in ogni sede remota e assegnare loro il ruolo di punti di distribuzione per un gruppo di amministrazione di primo livello (**Gruppo radice per le sedi** nella figura precedente).

Esempio: un computer portatile è distribuito nel gruppo di amministrazione **Sede 1** e quindi viene spostato fisicamente nella sede che corrisponde al gruppo di amministrazione **Sede 2**. Dopo lo spostamento del portatile, Network Agent tenta di accedere ai punti di distribuzione assegnati al gruppo **Sede 1**, ma tali punti di distribuzione non sono disponibili. Network Agent inizia quindi a tentare di accedere ai punti di distribuzione che sono stati assegnati al **Gruppo radice per le sedi**. Poiché le sedi remote sono isolate tra loro, i tentativi di accedere ai punti di distribuzione assegnati al gruppo di amministrazione **Gruppo radice per le sedi** avranno esito positivo solo quando Network Agent tenta di accedere ai punti di distribuzione nel gruppo **Sede 2**. In altre parole, il computer portatile rimarrà nel gruppo di amministrazione che corrisponde alla sede iniziale, ma utilizzerà il punto di distribuzione della sede in cui si trova fisicamente al momento.

Gerarchia di criteri tramite i profili criterio

Questa sezione fornisce informazioni su come applicare i criteri ai dispositivi nei gruppi di amministrazione. Questa sezione fornisce anche informazioni sui profili dei criteri.

Gerarchia dei criteri

In Kaspersky Security Center i criteri vengono utilizzati per definire una singola raccolta di impostazioni per più dispositivi. Ad esempio, l'ambito del criterio dell'applicazione P definito per il gruppo di amministrazione G include i dispositivi gestiti in cui è installata l'applicazione P che sono stati distribuiti nel gruppo G e in tutti i relativi sottogruppi, ad eccezione dei sottogruppi in cui la casella di controllo **Eredita da gruppo padre** è deselezionata nelle proprietà.

Un criterio differisce da qualsiasi impostazione locale in base alle icone di blocco (🔒) accanto alle relative impostazioni. Se un'impostazione (o un gruppo di impostazioni) è bloccata nelle proprietà del criterio, è necessario in primo luogo utilizzare questa impostazione (o gruppo di impostazioni) durante la creazione delle impostazioni da applicare e, in secondo luogo, scrivere le impostazioni o il gruppo di impostazioni nel criterio downstream.

La creazione delle impostazioni da applicare in un dispositivo può essere descritta come segue: i valori di tutte le impostazioni che non sono state bloccate vengono ottenuti dal criterio, quindi sono sovrascritti con i valori delle impostazioni locali. La raccolta risultante viene quindi sovrascritta con i valori delle impostazioni bloccate ottenuti dal criterio.

I criteri della stessa applicazione si influenzano reciprocamente attraverso la gerarchia dei gruppi di amministrazione: le impostazioni bloccate del criterio upstream sovrascrivono le stesse impostazioni del criterio downstream.

Esiste un criterio speciale per gli utenti fuori sede. Questo criterio ha effetto su un dispositivo quando il dispositivo passa in modalità fuori sede. I criteri fuori sede non influiscono sugli altri criteri attraverso la gerarchia dei gruppi di amministrazione.

Profili criterio

L'applicazione dei criteri ai dispositivi solo tramite la gerarchia dei gruppi di amministrazione in molte circostanze può essere poco pratica. Può essere necessario creare più istanze di un singolo criterio con una o due impostazioni differenti per gruppi di amministrazione diversi e sincronizzare i contenuti di questi criteri in futuro.

Per contribuire a evitare tali problemi, Kaspersky Security Center supporta *profili di criteri*. Un profilo criterio è un sottoinsieme denominato di impostazioni dei criteri. Questo sottoinsieme viene distribuito nei dispositivi di destinazione insieme al criterio, integrandolo in una condizione specifica definita *condizione di attivazione del profilo*. I profili contengono solo le impostazioni diverse dal criterio "di base" che è attivo sul dispositivo client (computer o dispositivo mobile). L'attivazione di un profilo determina la modifica delle impostazioni del criterio attivo nel dispositivo prima dell'attivazione del profilo. Tali impostazioni assumono i valori specificati nel profilo.

Attualmente ai profili criterio si applicano le seguenti limitazioni:

- Un criterio può includere al massimo 100 profili.
- Un profilo criterio non può contenere altri profili.
- Un profilo criterio non può contenere impostazioni di notifica.

Contenuto di un profilo

Un profilo criterio contiene i seguenti elementi:

- Nome. I profili con nomi identici si influenzano reciprocamente attraverso la gerarchia dei gruppi di amministrazione con regole comuni.
- Sottoinsieme di impostazioni dei criteri. A differenza del criterio, che contiene tutte le impostazioni, un profilo contiene solo le impostazioni che sono effettivamente richieste (le impostazioni bloccate).
- Condizione di attivazione è un'espressione logica con le proprietà del dispositivo. Un profilo è attivo (integra il criterio) solo quando la condizione di attivazione del profilo diventa vera. In tutti gli altri casi, il profilo è inattivo e viene ignorato. Le seguenti proprietà del dispositivo possono essere incluse nell'espressione logica:
  - Stato della modalità fuori sede.
  - Proprietà dell'ambiente di rete - Nome della regola attiva per la connessione di Network Agent.
  - Presenza o assenza dei tag specificati nel dispositivo.
  - Posizione del dispositivo in un'unità di Active Directory: esplicita (il dispositivo è direttamente nell'unità organizzativa specificata) o implicita (il dispositivo è in un'unità organizzativa che è contenuta nell'unità organizzativa specificata a qualsiasi livello di annidamento).
  - Appartenenza del dispositivo a un gruppo di protezione di Active Directory (esplicita o implicita).
  - Appartenenza del proprietario del dispositivo a un gruppo di protezione di Active Directory (esplicita o implicita).
- Casella di controllo per la disabilitazione del profilo. I profili disabilitati vengono sempre ignorati e le relative condizioni di attivazione non sono verificate.
- Priorità del profilo. Le condizioni di attivazione di differenti profili sono indipendenti, quindi è possibile attivare contemporaneamente più profili. Se i profili attivi contengono raccolte di impostazioni che non si sovrappongono, non si verifica alcun problema. Se invece due profili attivi contengono valori diversi della stessa impostazione, si verifica un'ambiguità. Questa ambiguità deve essere evitata tramite le priorità dei profili: il valore della variabile ambigua viene ottenuto dal profilo che ha la priorità più alta (quello al livello superiore nell'elenco dei profili).

Comportamento dei profili quando i criteri si influenzano reciprocamente attraverso la gerarchia

I profili con lo stesso nome vengono uniti in base alle regole di unione dei criteri. I profili di un criterio upstream hanno una priorità più alta rispetto ai profili di un criterio downstream. Se la modifica delle impostazioni non è consentita nel criterio upstream (è bloccata), il criterio downstream utilizza le condizioni di attivazione del profilo di quello upstream. Se la modifica delle impostazioni è consentita nel criterio upstream, vengono utilizzate le condizioni di attivazione del profilo del criterio downstream.

Poiché un profilo criterio può contenere la proprietà **Il dispositivo è offline** nella relativa condizione di attivazione, i profili sostituiscono completamente la funzionalità dei criteri per gli utenti fuori sede, che non saranno non più supportati.

Un criterio per gli utenti fuori sede può contenere profili, ma questi profili possono essere attivati solo una volta che il dispositivo passa alla modalità fuori sede.

Attività

Kaspersky Security Center consente di gestire le applicazioni di protezione Kaspersky installate nei dispositivi creando ed eseguendo *attività*. Le attività sono necessarie per l'installazione, l'avvio e l'arresto delle applicazioni, la scansione dei file, l'aggiornamento dei database e dei moduli software, oltre che per eseguire altre azioni sulle applicazioni.

Le attività per un'applicazione specifica possono essere create solo se è installato il plug-in di gestione per tale applicazione.

Le attività possono essere eseguite nell'Administration Server e nei dispositivi.

Le seguenti attività vengono eseguite nell'Administration Server:

- Distribuzione automatica dei rapporti
- Download degli aggiornamenti nell'archivio di Administration Server
- Backup dei dati di Administration Server
- Manutenzione del database
- Sincronizzazione di Windows Update
- Creazione di un pacchetto di installazione basato su un'immagine del sistema operativo di un dispositivo di riferimento

I seguenti tipi di attività vengono eseguiti nei dispositivi:

- *Attività locali* - Attività eseguite in un dispositivo specifico

  Le attività locali possono essere modificate dall'amministratore utilizzando gli strumenti di Administration Console oppure dall'utente di un dispositivo remoto (ad esempio, attraverso l'interfaccia dell'applicazione di protezione). Se un'attività locale viene modificata contemporaneamente dall'amministratore e dall'utente di un dispositivo gestito, hanno effetto le modifiche apportate dall'amministratore perché hanno una priorità più alta.

- *Attività di gruppo* - Attività eseguite su tutti i dispositivi di un gruppo specifico

  A meno che non sia diversamente specificato nelle proprietà dell'attività, un'attività di gruppo si applica anche a tutti i sottogruppi del gruppo selezionato. Un'attività di gruppo influisce anche (facoltativamente) sui dispositivi connessi agli Administration Server secondari e virtuali distribuiti nel gruppo o in uno dei relativi sottogruppi.

- *Attività globali* - Attività eseguite su un set di dispositivi, indipendentemente dalla loro appartenenza a un gruppo

Per ogni applicazione è possibile creare attività di gruppo, attività globali o attività locali.

È possibile apportare modifiche alle impostazioni delle attività, visualizzarne l'avanzamento, copiarle, esportarle, importarle ed eliminarle.

Le attività vengono avviate in un dispositivo solo se l'applicazione per cui l'attività è stata creata è in esecuzione.

I risultati delle attività sono salvati nel registro eventi di Microsoft Windows e nel registro eventi di Kaspersky Security Center, sia in modo centralizzato in Administration Server che localmente in ogni dispositivo.

Non includere dati privati nelle impostazioni dell'attività. Ad esempio, non specificare la password dell'amministratore del dominio.

Regole di spostamento dei dispositivi

È consigliabile automatizzare l'assegnazione dei dispositivi ai gruppi di amministrazione nel server virtuale corrispondente a un client MSP utilizzando le *regole di spostamento dei dispositivi*. Una regola di spostamento dei dispositivi comprende tre elementi principali: nome, condizione di esecuzione (espressione logica con gli attributi del dispositivo) e gruppo di amministrazione di destinazione. Una regola sposta un dispositivo nel gruppo di amministrazione di destinazione se gli attributi del dispositivo soddisfano la condizione di esecuzione della regola.

Tutte le regole di spostamento dei dispositivi hanno priorità. L'Administration Server verifica gli attributi del dispositivo per determinare se soddisfano la condizione di esecuzione di ogni regola, in ordine di priorità crescente. Se gli attributi del dispositivo soddisfano la condizione di esecuzione di una regola, il dispositivo viene spostato nel gruppo di destinazione, quindi l'elaborazione della regola è completa per questo dispositivo. Se gli attributi del dispositivo soddisfano le condizioni di più regole, il dispositivo viene spostato nel gruppo di destinazione della regola con la priorità più alta (al livello più alto nell'elenco delle regole).

Le regole di spostamento dei dispositivi possono essere create implicitamente. Ad esempio, nelle proprietà di un pacchetto di installazione o di un'attività di installazione remota è possibile specificare il gruppo di amministrazione in cui deve essere spostato il dispositivo dopo l'installazione di Network Agent. Inoltre, le regole di spostamento dei dispositivi possono essere create esplicitamente dall'amministratore di Kaspersky Security Center nell'elenco delle regole di spostamento. L'elenco è disponibile in Administration Console, nelle proprietà del gruppo **Dispositivi non assegnati**.

Per impostazione predefinita, una regola di spostamento dei dispositivi viene utilizzata per l'allocazione iniziale dei dispositivi ai gruppi di amministrazione. La regola sposta i dispositivi dal gruppo **Dispositivi non assegnati** una sola volta. Se in precedenza un dispositivo era stato spostato da questa regola, la regola non lo sposterà di nuovo, anche se si reinserisce manualmente il dispositivo nel gruppo **Dispositivi non assegnati**. Questo è il modo consigliato per applicare le regole di spostamento.

È possibile spostare i dispositivi che sono già stati assegnati ad alcuni gruppi di amministrazione. A tale scopo, nelle proprietà di una regola, deselezionare la casella di controllo **Sposta solo i dispositivi che non appartengono a un gruppo di amministrazione**.

L'applicazione delle regole di spostamento a dispositivi che sono già stati assegnati ad alcuni gruppi di amministrazione aumenta considerevolmente il carico sull'Administration Server.

È possibile creare una regola di spostamento da applicare ripetutamente a un singolo dispositivo.

È consigliabile evitare di spostare ripetutamente un singolo dispositivo da un gruppo all'altro (ad esempio, per applicare uno speciale criterio al dispositivo, eseguire una speciale attività di gruppo o aggiornare il dispositivo attraverso un punto di distribuzione specifico).

Tali scenari non sono supportati, perché comportano un notevole aumento del carico su Administration Server e del traffico di rete. Questi scenari anche sono in conflitto con i principi operativi di Kaspersky Security Center (in particolare nell'area di diritti di accesso, eventi e rapporti). Un'altra soluzione deve ad esempio essere trovata attraverso l'utilizzo di profili criterio, attività per selezioni dispositivi, l'assegnazione di Network Agent in base allo scenario di standard e così via.

Classificazione del software

Lo strumento principale per monitorare l'esecuzione delle applicazioni sono le *categorie Kaspersky* (di seguito denominate anche *categorie KL*). Le categorie KL consentono agli amministratori di Kaspersky Security Center di semplificare il supporto della classificazione del software e ridurre al minimo il traffico verso i dispositivi gestiti.

È necessario creare categorie utente per le applicazioni che non possono essere classificate in alcuna delle categorie KL esistenti (ad esempio, per il software personalizzato). Le categorie utente vengono create in base al pacchetto di installazione di un'applicazione (MSI) o a una cartella con pacchetti di installazione.

Se è disponibile una raccolta di software di grandi dimensioni che non è stata classificata tramite le categorie KL, può essere utile creare una categoria aggiornata automaticamente. I checksum dei file eseguibili saranno aggiunti automaticamente a questa categoria a ogni modifica della cartella che contiene i pacchetti di distribuzione.

Non creare categorie di software aggiornate automaticamente per le cartelle Documenti, %windir%, %ProgramFiles% e %ProgramFiles(x86)%. Il pool di file in queste cartelle è soggetto a modifiche frequenti, il che comporta un aumento del carico su Administration Server e del traffico di rete. È necessario creare una cartella dedicata con la raccolta del software e aggiungere periodicamente nuovi elementi a tale raccolta.

Informazioni sulle applicazioni multi-tenant

Kaspersky Security Center consente agli amministratori di provider di servizi e agli amministratori di tenant di utilizzare le applicazioni Kaspersky con supporto multi-tenancy. Dopo l'installazione di un'applicazione Kaspersky multi-tenant nell'infrastruttura di un provider di servizi, i tenant possono iniziare a utilizzare l'applicazione.

Per separare attività e criteri relativi a diversi tenant è necessario creare un Administration Server virtuale dedicato in Kaspersky Security Center per ciascun tenant. Tutte le attività e tutti i criteri per le applicazioni multi-tenant in esecuzione per un tenant devono essere creati per il gruppo di amministrazione Dispositivi gestiti dell'Administration Server virtuale corrispondente al tenant. Le attività create per i gruppi di amministrazione relativi all'Administration Server primario non riguardano i dispositivi dei tenant.

A differenza degli amministratori dei provider di servizi, un amministratore di tenant può creare e visualizzare criteri delle applicazioni e attività solo per i dispositivi del tenant corrispondente. I set di attività e le impostazioni dei criteri disponibili per gli amministratori dei provider di servizi e gli amministratori dei tenant sono diversi. Alcune attività e impostazioni dei criteri non sono disponibili per gli amministratori dei tenant.

All'interno della struttura gerarchica di un tenant, i criteri creati per le applicazioni multi-tenant vengono ereditati da gruppi di amministrazione di livello inferiore, nonché da gruppi di amministrazione di livello superiore: il criterio viene propagato a tutti i dispositivi client che appartengono al tenant.

Backup e ripristino delle impostazioni di Administration Server

Il backup delle impostazioni di Administration Server e del relativo database viene eseguito tramite l'attività di backup e l'utilità klbackup. Una copia di backup include tutte le impostazioni e gli oggetti principali relativi ad Administration Server, come certificati, chiavi primarie per il criptaggio delle unità nei dispositivi gestiti, chiavi per varie licenze, struttura dei gruppi di amministrazione con tutti i relativi contenuti, attività, criteri e così via. Con una copia di backup è possibile ripristinare il funzionamento di un Administration Server il prima possibile, un'operazione che richiede da una decina di minuti a un paio d'ore.

Se non è disponibile una copia di backup, un errore può comportare la perdita dei certificati e di tutte le impostazioni di Administration Server. In tal caso, sarà necessario riconfigurare completamente Kaspersky Security Center ed eseguire di nuovo la distribuzione iniziale di Network Agent nella rete dell'organizzazione. Andranno inoltre perse tutte le chiavi primarie per il criptaggio delle unità nei dispositivi gestiti, con il rischio di una perdita irrevocabile dei dati criptati nei dispositivi con Kaspersky Endpoint Security. Pertanto, non dimenticare di eseguire periodicamente backup di Administration Server utilizzando l'attività di backup standard.

L'Avvio rapido guidato crea l'attività di backup per le impostazioni di Administration Server e ne configura l'esecuzione quotidiana, alle 4:00. Le copie di backup vengono salvate per impostazione predefinita nella cartella %ALLUSERSPROFILE%\Application Data\KasperskySC.

Se si utilizza come DBMS un'istanza di Microsoft SQL Server installata in un altro dispositivo, è necessario modificare l'attività di backup specificando un percorso UNC, accessibile in scrittura sia dal servizio Administration Server che dal servizio SQL Server, come cartella per l'archiviazione delle copie di backup. Questo requisito deriva da una speciale funzionalità di backup nel DBMS Microsoft SQL Server.

Se si utilizza come DBMS un'istanza locale di Microsoft SQL Server, è anche consigliabile salvare copie di backup su un supporto dedicato per proteggerle dal danneggiamento insieme con Administration Server.

Poiché una copia di backup contiene dati importanti, l'attività di backup e l'utilità klbackup forniscono funzionalità di protezione tramite password delle copie di backup. Per impostazione predefinita, l'attività di backup viene creata con una password vuota. È necessario impostare una password nelle proprietà dell'attività di backup. Il mancato rispetto di questo requisito causa una situazione in cui tutte le chiavi dei certificati di Administration Server, le chiavi per le licenze e le chiavi primarie per il criptaggio delle unità nei dispositivi gestiti restano non criptate.

In aggiunta al backup periodico, è anche necessario creare una copia di backup prima di ogni modifica significativa, inclusa l'installazione di upgrade e patch di Administration Server.

Se si utilizza Microsoft SQL Server come DBMS, è possibile ridurre al minimo le dimensioni delle copie di backup. A tale scopo, abilitare l'opzione **Comprimi backup** nelle impostazioni di SQL Server.

Il ripristino da una copia di backup viene eseguito con l'utilità klbackup in un'istanza funzionante di Administration Server che è stata appena installata e con la stessa versione (o una versione successiva) di quella per cui è stata creata la copia di backup.

L'istanza di Administration Server in cui deve essere eseguito il ripristino deve utilizzare un DBMS dello stesso tipo (ad esempio, SQL Server o MariaDB) e della stessa versione o successiva. La versione di Administration Server può essere la stessa (con una patch identica o successiva) o una versione successiva.

In questa sezione sono descritti gli scenari standard per il ripristino delle impostazioni e degli oggetti di Administration Server.

Un dispositivo con Administration Server è inutilizzabile

Se un dispositivo con Administration Server risulta inutilizzabile a causa di un errore, è consigliabile eseguire le seguenti operazioni:

- Al nuovo Administration Server deve essere assegnato lo stesso indirizzo: nome NetBIOS, FQDN o IP statico (a seconda dell'elemento impostato al momento della distribuzione dei Network Agent).
- Installare Administration Server utilizzando un DBMS dello stesso tipo e della stessa versione (o di una versione successiva). È possibile installare la stessa versione del server (con una patch identica o successiva) o una versione successiva. Dopo installazione, non eseguire la configurazione iniziale tramite la procedura guidata.
- Nel menu **Start**, eseguire l'utilità klbackup e quindi eseguire il ripristino.

Le impostazioni di Administration Server o il database sono danneggiati

Se Administration Server risulta inutilizzabile perché le impostazioni o il database sono danneggiati (ad esempio, in seguito a una sovralimentazione), è consigliabile utilizzare il seguente scenario di ripristino:

1. Eseguire la scansione del file system nel dispositivo danneggiato.
2. Disinstallare la versione inutilizzabile di Administration Server.
3. Reinstallare Administration Server utilizzando un DBMS dello stesso tipo e della stessa versione (o di una versione successiva). È possibile installare la stessa versione del server (con una patch identica o successiva) o una versione successiva. Dopo installazione, non eseguire la configurazione iniziale tramite la procedura guidata.
4. Dal menu **Start** eseguire l'utilità klbackup e quindi eseguire il ripristino.

Non è consentito ripristinare Administration Server in un modo diverso dall'utilizzo dell'utilità klbackup.

Qualsiasi tentativo di ripristinare Administration Server tramite software di terze parti causerà inevitabilmente la mancata sincronizzazione dei dati nei nodi dell'applicazione Kaspersky Security Center distribuita e, di conseguenza, impedirà il corretto funzionamento dell'applicazione.

Distribuzione di Network Agent e dell'applicazione di protezione

Per gestire i dispositivi in un'organizzazione, è necessario installare Network Agent su ciascuno di essi. La distribuzione di Kaspersky Security Center nei dispositivi di un'organizzazione in genere ha inizio con l'installazione di Network Agent nei dispositivi.

In Microsoft Windows XP Network Agent potrebbe non eseguire correttamente le seguenti operazioni: download degli aggiornamenti direttamente dai server di Kaspersky (come punto di distribuzione); funzionamento come un server proxy KSN (come punto di distribuzione); e rilevamento di vulnerabilità di terze parti (se è in uso Vulnerability e patch management).

Distribuzione iniziale

Se Network Agent è già stato installato in un dispositivo, l'installazione remota delle applicazioni nel dispositivo viene eseguita tramite Network Agent. Il pacchetto di distribuzione di un'applicazione da installare viene trasferito mediante i canali di comunicazione tra i Network Agent e Administration Server, insieme alle impostazioni di installazione definite dall'amministratore. Per trasferire il pacchetto di distribuzione, è possibile utilizzare nodi di distribuzione per il trasferimento, cioè punti di distribuzione, recapito multicast e così via. Ulteriori dettagli su come installare le applicazioni nei dispositivi gestiti in cui è già installato Network Agent sono disponibili di seguito in questa sezione.

È possibile eseguire l'installazione iniziale di Network Agent nei dispositivi Windows utilizzando uno dei seguenti metodi:

- Con strumenti di terze parti per l'installazione remota delle applicazioni.
- Con i criteri di gruppo Windows: utilizzando gli strumenti di gestione standard di Windows per i criteri di gruppo.
- In modalità forzata, utilizzando speciali opzioni nell'attività di installazione remota di Kaspersky Security Center.
- Inviando agli utenti dei dispositivi collegamenti ai pacchetti indipendenti generati da Kaspersky Security Center. I pacchetti indipendenti sono moduli eseguibili che contengono i pacchetti di distribuzione delle applicazioni selezionate con le relative impostazioni definite.
- Manualmente, eseguendo i programmi di installazione delle applicazioni nei dispositivi.

Nelle piattaforme diverse da Microsoft Windows è necessario eseguire l'installazione iniziale di Network Agent nei dispositivi gestiti tramite gli strumenti di terze parti esistenti o manualmente, inviando agli utenti un archivio con un pacchetto di distribuzione preconfigurato. È possibile eseguire l'upgrade di Network Agent a una nuova versione o installare altre applicazioni Kaspersky nelle piattaforme non Windows, utilizzando i Network Agent (già installati nei dispositivi) per eseguire le attività di installazione remota. In questo caso, l'installazione è identica a quella dei dispositivi con sistema operativo Microsoft Windows.

Al momento della scelta di un metodo e di una strategia per la distribuzione delle applicazioni in una rete gestita, è necessario considerare diversi fattori (elenco parziale):

- Configurazione della rete aziendale
- Numero totale di dispositivi
- Presenza di domini Windows nella rete gestita, possibilità di modificare i criteri di gruppo Active Directory in tali domini
- Conoscenza degli account utente con diritti di amministratore locale nei dispositivi in cui è stata pianificata la distribuzione iniziale delle applicazioni Kaspersky (ad esempio disponibilità di un account utente di dominio con diritti di amministratore locale o presenza di account utente locali unificati con diritti di amministratore in tali dispositivi)
- Tipo di connessione e larghezza di banda dei canali di rete tra Administration Server e le reti client MSP, nonché la larghezza di banda dei canali all'interno di tali reti
- Impostazioni di sicurezza applicate ai dispositivi remoti all'inizio della distribuzione (ad esempio, utilizzo di Controllo dell'account utente e modalità Simple File Sharing)

Configurazione dei programmi di installazione

Prima di avviare la distribuzione delle applicazioni Kaspersky in una rete, è necessario specificare le impostazioni di installazione, ovvero quelle definite durante l'installazione dell'applicazione. Durante l'installazione di Network Agent, è necessario specificare almeno un indirizzo per la connessione ad Administration Server e le impostazioni proxy. Possono essere richieste anche alcune impostazioni avanzate. A seconda del metodo di installazione selezionato, è possibile definire le impostazioni in diversi modi. Nel caso più semplice (installazione manuale interattiva in un dispositivo selezionato), tutte le impostazioni attinenti possono essere definite tramite l'interfaccia utente del programma di installazione. Di conseguenza, in alcuni casi la distribuzione iniziale può anche essere eseguita inviando agli utenti un collegamento al pacchetto di distribuzione di Network Agent insieme alle impostazioni (indirizzo di Administration Server e così via) che l'utente deve immettere nell'interfaccia del programma di installazione.

L'utilizzo di questo metodo non è consigliabile dal momento che non risulta ottimale per gli utenti e implica un elevato rischio di errori durante la definizione manuale delle impostazioni. Non è inoltre utilizzabile con l'installazione automatica delle applicazioni nei gruppi di dispositivi. In generale, l'amministratore deve specificare i valori per le impostazioni in modalità centralizzata. Tali valori possono successivamente essere utilizzati per la creazione di pacchetti indipendenti. I pacchetti indipendenti sono archivi autoestraenti che contengono i pacchetti di distribuzione con le impostazioni definite dall'amministratore. I pacchetti indipendenti possono essere posizionati in risorse che consentono sia il download da parte degli utenti finali (ad esempio nel Server Web di Kaspersky Security Center) che l'installazione automatica nei dispositivi della rete selezionati.

Pacchetti di installazione

Il metodo principale per definire le impostazioni di installazione delle applicazioni è adatto per tutti i metodi di installazione, sia con gli strumenti di Kaspersky Security Center che con la maggior parte strumenti di terze parti. Questo metodo consiste nella creazione di pacchetti di installazione delle applicazioni in Kaspersky Security Center.

I pacchetti di installazione sono generati utilizzando i seguenti metodi:

- Automaticamente, dai pacchetti di distribuzione specificati, in base ai *descrittori* inclusi (file con estensione kud che contengono regole per l'installazione e l'analisi dei risultati e altre informazioni)

- Dai file eseguibili dei programmi di installazione o dai programmi di installazione in formato Microsoft Windows Installer (MSI) per le applicazioni standard o supportate

I pacchetti di installazione generati sono organizzati gerarchicamente come cartelle con sottocartelle e file. Oltre al pacchetto di distribuzione originale, un pacchetto di installazione contiene impostazioni modificabili (incluse le impostazioni del programma di installazione e le regole per elaborare casi come la necessità di riavviare il sistema operativo per completare l'installazione), nonché moduli ausiliari minori.

I valori delle impostazioni di installazione specifiche per il supporto di un'applicazione selezionata possono essere specificati nell'interfaccia utente di Administration Console durante la creazione di un pacchetto di installazione (altre impostazioni sono disponibili nelle proprietà di un pacchetto di installazione già creato). Durante l'esecuzione dell'installazione remota delle applicazioni tramite gli strumenti di Kaspersky Security Center, i pacchetti di installazione vengono inviati ai dispositivi di destinazione. L'esecuzione del programma di installazione di un'applicazione rende disponibili tutte le impostazioni definite dall'amministratore per tale applicazione. Quando si utilizzano strumenti di terze parti per l'installazione delle applicazioni Kaspersky, è sufficiente garantire la disponibilità dell'intero pacchetto di installazione nel dispositivo di destinazione, ovvero la disponibilità del pacchetto di distribuzione e delle relative impostazioni. I pacchetti di installazione vengono creati e archiviati da Kaspersky Security Center in un'apposita sottocartella della cartella dati condivisa.

Non specificare dettagli degli account privilegiati nei parametri dei pacchetti di installazione.

Per istruzioni sull'utilizzo di questo metodo di configurazione per le applicazioni Kaspersky prima della distribuzione mediante strumenti di terze parti, vedere la sezione "Distribuzione tramite i criteri di gruppo di Microsoft Windows".

Subito dopo l'installazione di Kaspersky Security Center, alcuni pacchetti di installazione vengono generati automaticamente: sono pronti per l'installazione e includono i pacchetti di Network Agent e i pacchetti delle applicazioni di protezione per Microsoft Windows.

In alcuni casi, l'utilizzo di pacchetti di installazione per la distribuzione delle applicazioni in una rete client MSP implica l'esigenza di creare pacchetti di installazione nei Server virtuali corrispondenti ai client MSP. La creazione dei pacchetti di installazione nei Server virtuali consente di utilizzare diverse impostazioni di installazione per diversi client MSP. Nella prima istanza ciò si rivela utile in fase di gestione dei pacchetti di installazione di Network Agent, dal momento che i Network Agent distribuiti nelle reti di diversi client MSP utilizzano indirizzi diversi per la connessione ad Administration Server. In realtà, l'indirizzo di connessione determina il Server a cui si connette Network Agent.

Oltre alla possibilità di creare immediatamente nuovi pacchetti di installazione in un Administration Server virtuale, la modalità di esecuzione principale per i pacchetti di installazione negli Administration Server virtuali è la "distribuzione" dei pacchetti di installazione dall'Administration Server primario a quelli virtuali. È possibile distribuire i pacchetti di installazione selezionati (o tutti i pacchetti di installazione) agli Administration Server virtuali (inclusi tutti i server all'interno di un gruppo di amministrazione selezionato) tramite l'attività di Administration Server corrispondente. È inoltre possibile selezionare l'elenco dei pacchetti di installazione dell'Administration Server primario durante la creazione di un nuovo Administration Server virtuale. I pacchetti selezionati verranno immediatamente distribuiti a un nuovo Administration Server virtuale creato.

Durante la distribuzione di un pacchetto di installazione, il relativo contenuto non viene copiato interamente. L'archivio file in un Administration Server virtuale, corrispondente al pacchetto di installazione distribuito, archivia solo i file delle impostazioni specifiche per tale server virtuale. La parte principale del pacchetto di installazione (incluso il pacchetto di distribuzione dell'applicazione da installare) rimane invariata e viene archiviata solo nell'archivio dell'Administration Server primario. In questo modo è possibile incrementare notevolmente le prestazioni di sistema e ridurre il volume disco necessario. Durante la gestione dei pacchetti di installazione distribuiti agli Administration Server virtuali (ad esempio durante l'esecuzione delle attività di installazione remota o la creazione di pacchetti di installazione indipendenti), i dati del pacchetto di installazione originale dell'Administration Server primario vengono "uniti" ai file delle impostazioni corrispondenti al pacchetto distribuito nell'Administration Server virtuale.

Anche se la chiave di licenza per un'applicazione può essere impostata nelle proprietà del pacchetto di installazione, è consigliabile evitare questo metodo di distribuzione delle licenze poiché è facile ottenere involontariamente l'accesso in lettura ai file della cartella. È necessario utilizzare chiavi di licenza distribuite automaticamente o le attività di installazione per le chiavi di licenza.

Proprietà e file di trasformazione MSI

Un altro modo per configurare l'installazione nella piattaforma Windows è definire le proprietà e i file di trasformazione MSI. Questo metodo può essere utilizzato durante l'esecuzione dell'installazione tramite gli strumenti di terze parti destinati ai programmi di installazione nel formato Microsoft Installer e durante l'esecuzione dell'installazione tramite i criteri di gruppo Windows utilizzando gli strumenti Microsoft standard o altri strumenti di terze parti progettati per la gestione dei criteri di gruppo Windows.

Distribuzione con strumenti di terze parti per l'installazione remota delle applicazioni

Se nell'organizzazione sono disponibili strumenti per l'installazione remota delle applicazioni (ad esempio, Microsoft System Center), è possibile eseguire la distribuzione iniziale utilizzando tali strumenti.

È necessario eseguire le seguenti operazioni:

- Selezionare il metodo per la configurazione dell'installazione più adatto per lo strumento di distribuzione da utilizzare.
- Definire il meccanismo per la sincronizzazione tra la modifica delle impostazioni dei pacchetti di installazione (attraverso l'interfaccia di Administration Console) e l'esecuzione degli strumenti di terze parti selezionati utilizzati per la distribuzione delle applicazioni dai dati dei pacchetti di installazione.

Informazioni generali sulle attività di installazione remota in Kaspersky Security Center

Kaspersky Security Center fornisce un'ampia gamma di metodi per l'installazione remota delle applicazioni, implementati come attività di installazione remota. È possibile creare un'attività di installazione remota sia per un gruppo di amministrazione specificato che per dispositivi specifici o per una selezione di dispositivi (tali attività sono visualizzate in Administration Console, nella cartella **Attività**). Durante la creazione di un'attività, è possibile selezionare i pacchetti di installazione (quelli di Network Agent e/o di un'altra applicazione) per l'installazione con questa attività, nonché specificare determinate impostazioni che definiscono il metodo di installazione remota.

Le attività per i gruppi di amministrazione influiscono sia sui dispositivi inclusi in un gruppo specificato che su tutti i dispositivi in tutti i sottogruppi compresi in tale gruppo di amministrazione. Un'attività copre i dispositivi degli Administration Server secondari inclusi in un gruppo o in qualsiasi dei relativi sottogruppi se l'impostazione corrispondente è abilitata nell'attività.

Le attività per dispositivi specifici aggiornano l'elenco dei dispositivi client a ogni esecuzione, in conformità con i contenuti della selezione al momento dell'avvio dell'attività. Se una selezione include dispositivi che sono stati connessi ad Administration Server secondari, l'attività verrà eseguita anche in tali dispositivi.

Per garantire la corretta esecuzione di un'attività di installazione remota nei dispositivi connessi agli Administration Server secondari, è necessario utilizzare l'attività di distribuzione per distribuire anticipatamente i pacchetti di installazione utilizzati dall'attività agli Administration Server secondari corrispondenti.

Distribuzione tramite i criteri di gruppo di Microsoft Windows

È consigliabile eseguire la distribuzione iniziale dei Network Agent tramite i criteri di gruppo di Microsoft Windows se sono soddisfatte le seguenti condizioni:

- Il dispositivo fa parte di un dominio Active Directory.
- L'accesso al controller di dominio viene concesso con i diritti di amministratore, che consentono di creare e modificare i criteri di gruppo di Active Directory.
- I pacchetti di installazione configurati possono essere spostati nella rete che ospita i dispositivi gestiti di destinazione (in una cartella condivisa disponibile per la lettura da parte di tutti i dispositivi di destinazione).
- Lo schema di distribuzione consente di attendere il successivo riavvio abituale dei dispositivi di destinazione prima di avviare la distribuzione nei Network Agent su di essi (oppure è possibile forzare l'applicazione di un criterio di gruppo di Windows in tali dispositivi).

Questo schema di distribuzione comprende quanto segue:

- Il pacchetto di distribuzione dell'applicazione in formato Microsoft Installer (pacchetto MSI) è disponibile in una cartella condivisa (una cartella per cui gli account LocalSystem dei dispositivi di destinazione dispongono di autorizzazioni di lettura).
- Nel criterio di gruppo di Active Directory, viene creato un oggetto di installazione per il pacchetto di distribuzione.
- L'ambito di installazione è impostato specificando l'unità organizzativa (UO) e / o il gruppo di protezione che include i dispositivi di destinazione.
- Al successivo accesso al dominio di un dispositivo di destinazione (prima che gli utenti del dispositivo accedano al sistema), tutte le applicazioni installate vengono esaminate per verificare che sia presente l'applicazione richiesta. Se l'applicazione non viene trovata, il pacchetto di distribuzione viene scaricato dalla risorsa specificata nel criterio e quindi viene installato.

Un vantaggio di questo schema di distribuzione è il fatto che le applicazioni assegnate sono installate nei dispositivi di destinazione durante il caricamento del sistema operativo, prima che l'utente acceda al sistema. Anche se un utente con diritti sufficienti rimuove l'applicazione, questa sarà reinstallata al successivo avvio del sistema operativo. Lo svantaggio di questo schema di distribuzione è che le modifiche apportate dall'amministratore al criterio di gruppo non hanno effetto finché i dispositivi non vengono riavviati (se non vengono utilizzati strumenti aggiuntivi).

È possibile utilizzare i criteri di gruppo per installare sia Network Agent che altre applicazioni se i relativi programmi di installazione sono in formato Windows Installer.

> L'installazione di Network Agent dal pacchetto MSI è possibile solo in modalità automatica, l'installazione interattiva dal pacchetto MSI non è supportata.

Inoltre, quando si seleziona questo metodo di distribuzione, è necessario valutare il carico sulla risorsa file da cui saranno copiati i file nei dispositivi di destinazione dopo l'applicazione del criterio di gruppo di Windows. È inoltre necessario scegliere il metodo di invio del pacchetto di installazione configurato a tale risorsa, nonché il metodo di sincronizzazione delle modifiche attinenti nelle relative impostazioni.

Gestione dei criteri di Microsoft Windows tramite l'attività di installazione remota di Kaspersky Security Center

Questo metodo di distribuzione è disponibile solo se l'accesso al controller di dominio, contenente i dispositivi di destinazione, è possibile dal dispositivo Administration Server, mentre la cartella condivisa di Administration Server (in cui vengono archiviati i pacchetti di installazione) è accessibile per la lettura dai dispositivi di destinazione. Per i motivi precedenti, questo metodo di distribuzione non viene considerato applicabile a MSP.

Installazione non assistita delle applicazioni tramite i criteri di Microsoft Windows

L'amministratore può creare autonomamente gli oggetti richiesti per l'installazione in un criterio di gruppo di Windows. In questo caso è necessario caricare i pacchetti in un file server indipendente e fornire un collegamento a tali pacchetti.

Sono possibili i seguenti scenari di installazione:

- L'amministratore crea un pacchetto di installazione e ne imposta le proprietà in Administration Console. L'amministratore copia quindi l'intera sottocartella EXEC di questo pacchetto dalla cartella condivisa di Kaspersky Security Center in una cartella su una risorsa file dedicata dell'organizzazione. L'oggetto criteri di gruppo fornisce un collegamento al file MSI di questo pacchetto archiviato in una sottocartella sulla risorsa file dedicata dell'organizzazione.

- L'amministratore scarica da Internet il pacchetto di distribuzione dell'applicazione (incluso quello di Network Agent) e lo carica nella risorsa file dedicata dell'organizzazione. L'oggetto criteri di gruppo fornisce un collegamento al file MSI di questo pacchetto archiviato in una sottocartella sulla risorsa file dedicata dell'organizzazione. Le impostazioni di installazione sono definite configurando le proprietà MSI o configurando i file di trasformazione MST.

Distribuzione forzata tramite l'attività di installazione remota di Kaspersky Security Center

Per eseguire la distribuzione iniziale di Network Agent o di altre applicazioni, è possibile forzare l'installazione dei pacchetti di installazione selezionati utilizzando l'attività di installazione remota di Kaspersky Security Center, a condizione che ogni dispositivo disponga di uno o più account utente con diritti di amministratore locali.

L'installazione forzata può anche essere applicata se i dispositivi non sono direttamente accessibili da Administration Server, ad esempio se i dispositivi sono in rete isolata o se si trovano in una rete locale mentre Administration Server è in una rete perimetrale.

In caso di distribuzione iniziale, Network Agent non è installato. Pertanto, nelle impostazioni dell'attività di installazione remota, non è possibile selezionare la distribuzione dei file richiesti per l'installazione dell'applicazione utilizzando Network Agent. È possibile scegliere di distribuire i file solo utilizzando le risorse del sistema operativo tramite Administration Server o i punti di distribuzione.

Il servizio Administration Server deve essere eseguito con un account con privilegi di amministratore nei dispositivi di destinazione. In alternativa, è possibile specificare un account che ha accesso alla condivisione admin$ nelle impostazioni dell'attività di installazione remota.

Per impostazione predefinita, l'attività di installazione remota si connette ai dispositivi utilizzando le credenziali dell'account con cui è in esecuzione Administration Server, ovvero l'account per accedere alla condivisione admin$. È necessario specificare questo account nelle impostazioni dell'attività di installazione remota solo se Network Agent non è installato nei dispositivi di destinazione.
Quando si crea l'attività di installazione remota da eseguire nei dispositivi basati su Linux, è sempre necessario specificare un account per la creazione di una connessione SSH.

È possibile specificare i dispositivi di destinazione esplicitamente (con un elenco), selezionando il gruppo di amministrazione di Kaspersky Security Center a cui appartengono o creando una selezione di dispositivi in base a un criterio specifico. L'ora di inizio dell'installazione è definita dalla pianificazione dell'attività. Se l'impostazione **Esegui attività non effettuate** è abilitata nelle proprietà dell'attività, l'attività può essere eseguita subito dopo l'accensione dei dispositivi di destinazione o quando vengono spostati nel gruppo di amministrazione di destinazione.

L'installazione forzata consiste nella distribuzione dei pacchetti di installazione ai dispositivi di destinazione, nella successiva copia dei file nella risorsa admin$ in ciascuno dei dispositivi di destinazione e nella registrazione remota dei servizi di supporto in tali dispositivi. L'invio dei pacchetti di installazione ai dispositivi di destinazione viene eseguito tramite una funzionalità di Kaspersky Security Center che garantisce l'interazione di rete. In questo caso, devono essere soddisfatte le seguenti condizioni:

- I dispositivi di destinazione sono accessibili dal lato di Administration Server o dal lato del punto di distribuzione.
- La risoluzione dei nomi per i dispositivi di destinazione funziona correttamente nella rete.
- Le condivisioni amministrative (admin$) rimangono abilitate nei dispositivi di destinazione.
- I seguenti servizi di sistema sono in esecuzione nei dispositivi di destinazione:
  - Server (LanmanServer)

    Per impostazione predefinita, questo servizio è in esecuzione.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- La porta TCP 445 è aperta nei dispositivi di destinazione per abilitare l'accesso remoto tramite gli strumenti di Windows.

  > TCP 139, UDP 137 e UDP 138 vengono utilizzati dai protocolli precedenti e non sono più necessari per le applicazioni correnti.

  Le porte di accesso dinamiche in uscita devono essere consentite nel firewall per le connessioni da Administration Server e dai punti di distribuzione ai dispositivi di destinazione.
- Le impostazioni di protezione del criterio di dominio di Active Directory possono fornire il funzionamento del protocollo NTLM durante la distribuzione di Network Agent.
- Nei dispositivi di destinazione che eseguono Microsoft Windows XP, la modalità Simple File Sharing è disabilitata.

- Nei dispositivi di destinazione, il modello di protezione e condivisione dell'accesso è impostato su *Classico: gli utenti locali eseguono l'autenticazione come se stessi*. Non può in alcun modo essere *Solo Guest: gli utenti locali si autenticano come Guest*.

- I dispositivi di destinazione sono utenti del dominio o vengono creati anticipatamente account uniformi con diritti di amministratore nei dispositivi di destinazione.

Per distribuire correttamente Network Agent o altre applicazioni in un dispositivo che non fa parte di un dominio Active Directory di Windows Server 2003 o versione successiva, è necessario disabilitare Controllo dell'account utente remoto in tale dispositivo. Controllo dell'account utente remoto è uno dei motivi che impedisce agli account amministrativi locali di accedere ad admin$, necessario per la distribuzione forzata di Network Agent o di altre applicazioni. La disabilitazione di Controllo dell'account utente remoto non influisce su Controllo dell'account utente locale.

Durante l'installazione in nuovi dispositivi che non sono stati ancora assegnati ad alcun gruppo di amministrazione di Kaspersky Security Center, è possibile aprire le proprietà dell'attività di installazione remota e specificare il gruppo di amministrazione in cui spostare i dispositivi dopo l'installazione di Network Agent.

Al momento della creazione di un'attività di gruppo, tenere presente che ogni attività di gruppo influisce su tutti i dispositivi in tutti i gruppi nidificati all'interno un gruppo selezionato. È pertanto necessario evitare di duplicare le attività di installazione nei sottogruppi.

Un modo semplificato per creare attività per l'installazione forzata delle applicazioni è l'installazione automatica. A tale scopo, è necessario aprire le proprietà del gruppo di amministrazione, aprire l'elenco dei pacchetti di installazione e selezionare quelli da installare nei dispositivi di questo gruppo. I pacchetti di installazione selezionati saranno installati automaticamente in tutti i dispositivi di questo gruppo e di tutti i relativi sottogruppi. L'intervallo di tempo richiesto per l'installazione dei pacchetti dipende dalla velocità effettiva della rete e dal numero totale di dispositivi in rete.

Per ridurre il carico su Administration Server durante la distribuzione dei pacchetti di installazione ai dispositivi di destinazione, è possibile selezionare l'installazione tramite i punti di distribuzione nell'attività di installazione. Tenere presente che questo metodo di installazione comporta un carico significativo per i dispositivi che operano come punti di distribuzione. Pertanto, si consiglia di selezionare i dispositivi che soddisfano i requisiti per i punti di distribuzione. Se si utilizzano punti di distribuzione, è necessario assicurarsi che siano presenti in ciascuna delle subnet isolate che ospitano i dispositivi di destinazione.

L'utilizzo dei punti di distribuzione come centri di installazione locali può anche essere utile durante l'installazione nei dispositivi in subnet che comunicano con Administration Server tramite un canale con una capacità limitata, mentre è disponibile un canale con una maggiore capacità tra i dispositivi nella stessa subnet.

Lo spazio libero su disco nella partizione con la cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit deve superare, di diverse volte, le dimensioni totali dei pacchetti di distribuzione delle applicazioni installate.

Esecuzione di pacchetti indipendenti creati tramite Kaspersky Security Center

I metodi descritti in precedenza per la distribuzione iniziale di Network Agent e delle altre applicazioni non possono essere sempre implementati perché non è possibile soddisfare tutte le condizioni applicabili. In tali casi, è possibile creare un comune file eseguibile denominato *pacchetto di installazione indipendente* tramite Kaspersky Security Center, utilizzando i pacchetti di installazione con le impostazioni di installazione appropriate che sono stati preparati dall'amministratore. Un pacchetto di installazione indipendente può essere pubblicato in un server Web interno (anche in Kaspersky Security Center) se considerato ragionevole (è stato configurato l'accesso esterno al server Web per gli utenti dei dispositivi di destinazione) o in un server Web distribuito in modo esclusivo incluso in Kaspersky Security Center Web Console. È inoltre possibile copiare i pacchetti indipendenti in un altro server Web.

È possibile utilizzare Kaspersky Security Center per inviare agli utenti selezionati un messaggio e-mail contenente un collegamento al file del pacchetto indipendente nel server Web utilizzato attualmente, richiedendo loro di eseguire il file (in modalità interattiva o con l'opzione "-s" per l'installazione automatica). È possibile allegare il pacchetto di installazione indipendente a un messaggio e-mail e quindi inviarlo agli utenti dei dispositivi che non hanno accesso al server Web. L'amministratore può anche copiare il pacchetto indipendente in un dispositivo esterno, distribuirlo a un dispositivo appropriato e quindi eseguirlo in un secondo momento.

È possibile creare un pacchetto indipendente da un pacchetto di Network Agent, un pacchetto di un'altra applicazione (ad esempio, l'applicazione di protezione) o entrambi. Se il pacchetto indipendente è stato creato da Network Agent e un'altra applicazione, l'installazione inizia da Network Agent.

Durante la creazione di un pacchetto indipendente con Network Agent, è possibile specificare il gruppo di amministrazione nel quale verranno automaticamente spostati i nuovi dispositivi (quelli che non sono stati allocati ad alcun gruppo di amministrazione) al termine dell'installazione di Network Agent.

I pacchetti indipendenti possono essere eseguiti in modalità interattiva (per impostazione predefinita), visualizzando il risultato dell'installazione delle applicazioni che contengono, o possono essere eseguiti in modalità automatica (con l'opzione "-s"). La modalità automatica può essere utilizzata per l'installazione tramite script, ad esempio script configurati per l'esecuzione dopo la distribuzione dell'immagine di un sistema operativo. Il risultato dell'installazione in modalità automatica è determinato dal codice restituito del processo.

Opzioni per l'installazione manuale delle applicazioni

Gli amministratori o gli utenti esperti possono installare manualmente le applicazioni in modalità interattiva. Possono utilizzare i pacchetti di distribuzione originali o pacchetti di installazione generati da questi ultimi e archiviati nella cartella condivisa di Kaspersky Security Center. Per impostazione predefinita, i programmi di installazione vengono eseguiti in modalità interattiva e richiedono agli utenti tutti i valori richiesti. Tuttavia, eseguendo il processo setup.exe dalla radice di un pacchetto di installazione con l'opzione "-s", il programma di installazione verrà eseguito in modalità automatica e con le impostazioni che sono state definite durante la configurazione del pacchetto di installazione.

Quando si esegue setup.exe dalla radice di un pacchetto di installazione, il pacchetto sarà prima copiato in una cartella locale temporanea e quindi sarà eseguito il programma di installazione dell'applicazione dalla cartella locale.

Installazione remota delle applicazioni nei dispositivi in cui è installato Network Agent

Se un Network Agent connesso all'Administration Server primario (o a uno dei relativi Server secondari) è installato in un dispositivo, è possibile eseguire l'upgrade di Network Agent in tale dispositivo, nonché installare, aggiornare o rimuovere qualsiasi applicazione supportata tramite Network Agent.

È possibile abilitare questa opzione se si seleziona la casella di controllo **Utilizzo di Network Agent** nelle proprietà dell'attività di installazione remota.

Se questa casella di controllo è selezionata, i pacchetti di installazione con le impostazioni di installazione definite dall'amministratore saranno trasferiti ai dispositivi di destinazione tramite i canali di comunicazione tra Network Agent e l'Administration Server.

Per ottimizzare il carico su Administration Server e ridurre al minimo il traffico tra Administration Server e i dispositivi, è consigliabile assegnare punti di distribuzione in ogni rete remota o in ogni dominio di trasmissione (vedere le sezioni Informazioni sui punti di distribuzione e Creazione di una struttura di gruppi di amministrazione e assegnazione dei punti di distribuzione). In questo caso, i pacchetti di installazione e le impostazioni del programma di installazione sono distribuiti dall'Administration Server ai dispositivi di destinazione tramite i punti di distribuzione.

È inoltre possibile utilizzare i punti di distribuzione per l'invio (multicast) dei pacchetti di installazione, che consente di ridurre considerevolmente il traffico di rete durante la distribuzione delle applicazioni.

Durante il trasferimento dei pacchetti di installazione ai dispositivi di destinazione tramite i canali di comunicazione tra i Network Agent e l'Administration Server, tutti i pacchetti di installazione che sono stati preparati per il trasferimento saranno anche memorizzati nella cache nella cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Quando si utilizzano diversi pacchetti di installazione di grandi dimensioni, di vari tipi e che coinvolgono numerosi punti di distribuzione, le dimensioni di questa cartella possono aumentare notevolmente.

I file non possono essere eliminati manualmente della cartella FTServer. Quando i pacchetti di installazione originali vengono eliminati, i dati corrispondenti sono eliminati automaticamente della cartella FTServer.

Tutti i dati ricevuti da parte dei punti di distribuzione sono salvati nella cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

I file non possono essere eliminati manualmente della cartella $FTCITmp. Al termine delle attività che utilizzano i dati in questa cartella, i contenuti della cartella saranno eliminati automaticamente.

Poiché i pacchetti di installazione sono distribuiti tramite i canali di comunicazione tra Administration Server e i Network Agent da un archivio intermedio in un formato ottimizzato per i trasferimenti in rete, non sono consentite modifiche ai pacchetti di installazione archiviati nella cartella originale di ogni pacchetto di installazione. Tali modifiche non saranno registrate automaticamente da Administration Server. Se è necessario modificare manualmente i file dei pacchetti di installazione (sebbene sia consigliabile evitare questo scenario), è necessario modificare qualsiasi impostazione di un pacchetto di installazione in Administration Console. La modifica delle impostazioni di un pacchetto di installazione in Administration Console fa sì che Administration Server aggiorni l'immagine del pacchetto nella cache che è stato preparato per il trasferimento nei dispositivi di destinazione.

Gestione dei riavvii dei dispositivi nell'attività di installazione remota

I dispositivi spesso richiedono un riavvio per completare l'installazione remota delle applicazioni (in particolare in Windows).

Se si utilizza l'attività Installazione remota di Kaspersky Security Center, nella Creazione guidata nuova attività o nella finestra delle proprietà dell'attività che è stata creata (sezione **Riavvio del sistema operativo**), è possibile selezionare l'azione da eseguire quando il dispositivo Windows richiede un riavvio:

- **Non riavviare il dispositivo**. In questo caso, non sarà eseguito alcun riavvio automatico. Per completare l'installazione, è necessario riavviare il dispositivo (ad esempio, manualmente o tramite l'attività di gestione del dispositivo). Le informazioni sul riavvio richiesto saranno salvate nei risultati dell'attività e nello stato del dispositivo. Questa opzione è adatta per le attività di installazione nei server e negli altri dispositivi per cui il funzionamento continuo è di importanza critica.

- **Riavvia il dispositivo**. In questo caso, il dispositivo viene sempre riavviato automaticamente quando è richiesto un riavvio per il completamento dell'installazione. Questa opzione è utile per le attività di installazione nei dispositivi per cui sono previste pause periodiche durante la relativa esecuzione (chiusura o riavvio).

- **Richiedi l'intervento dell'utente**. In questo caso, sarà visualizzata una notifica del riavvio sullo schermo del dispositivo client e verrà richiesto all'utente di riavviare il dispositivo manualmente. Per questa opzione è possibile definire alcune impostazioni avanzate: il testo del messaggio per l'utente, la frequenza di visualizzazione del messaggio e l'intervallo di tempo al termine del quale sarà forzato il riavvio (senza la conferma dell'utente). L'opzione **Richiedi l'intervento dell'utente** è la più adatta per le workstation, in cui gli utenti devono avere la possibilità di selezionare l'orario che preferiscono per un riavvio del sistema.

Aggiornamento dei database in un pacchetto di installazione di un'applicazione anti-virus

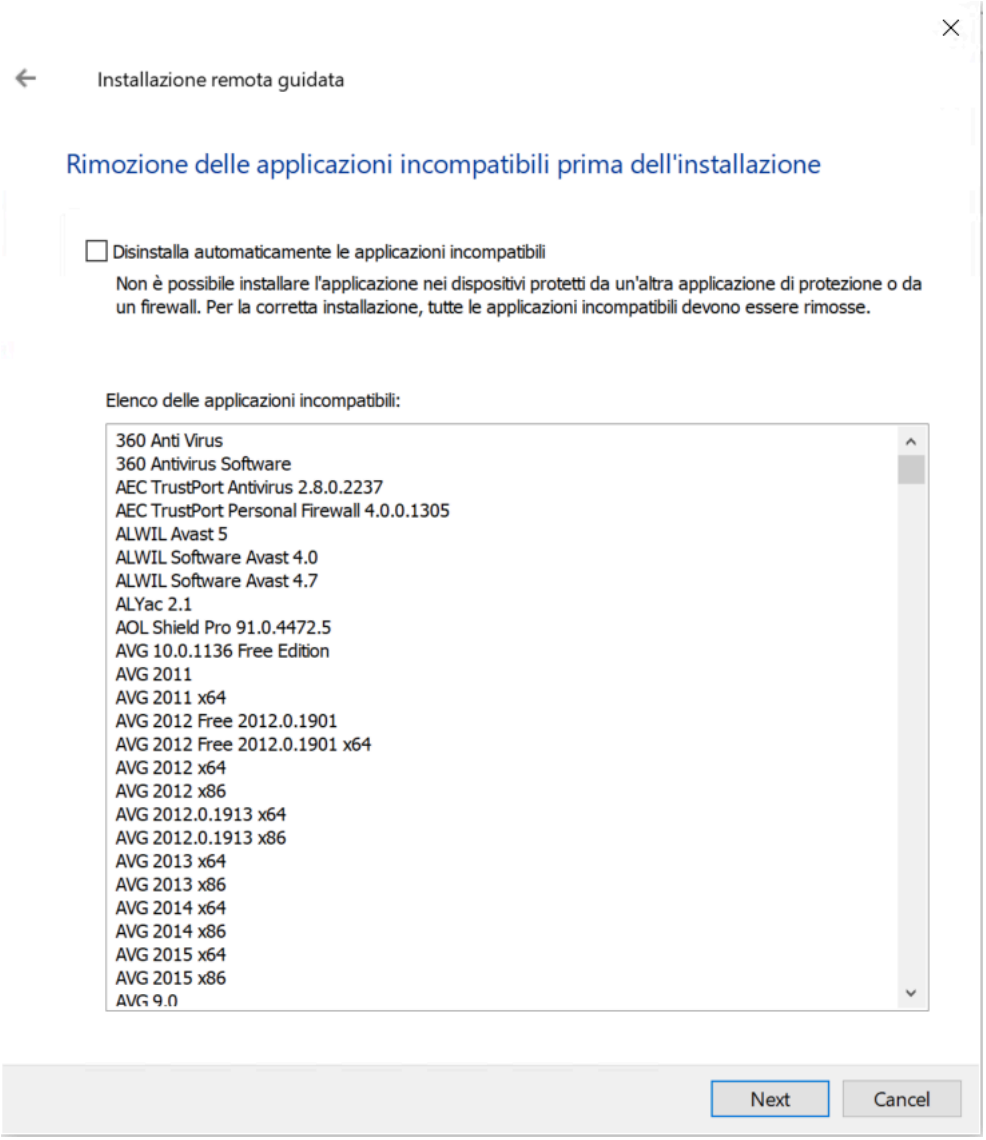
Prima di avviare la distribuzione della protezione, è necessario tenere presente che è possibile aggiornare i database anti-virus (inclusi i moduli delle patch automatiche) forniti con il pacchetto di distribuzione dell'applicazione di protezione. È consigliabile aggiornare i database nel pacchetto di installazione dell'applicazione prima di avviare la distribuzione (ad esempio, utilizzando il comando corrispondente nel menu di scelta rapida di un pacchetto di installazione selezionato). In tal modo, è possibile ridurre il numero di riavvii richiesti per il completamento della distribuzione della protezione nei dispositivi di destinazione. Se l'installazione remota interessa pacchetti di installazione che sono stati trasmessi a server virtuali dall'Administration Server primario, è sufficiente aggiornare i database nel pacchetto originale nel server primario. In questo caso, non è necessario aggiornare i database nei pacchetti trasmessi nei Server virtuali.

Rimozione di applicazioni di protezione di terzi non compatibili

L'Installazione delle applicazioni di protezione Kaspersky tramite Kaspersky Security Center può richiedere la rimozione di software di terze parti incompatibile con l'applicazione da installare. Esistono due modi principali per rimuovere le applicazioni di terze parti.

Eliminazione automatica delle applicazioni non compatibili tramite il programma di installazione

Quando si esegue il programma di installazione, viene visualizzato un elenco di applicazioni non compatibili con un'applicazione Kaspersky:



L'elenco delle applicazioni non compatibili visualizzato nell'Installazione guidata remota

Kaspersky Security Center rileva il software non compatibile. Di conseguenza, è possibile selezionare la casella di controllo **Disinstalla automaticamente le applicazioni incompatibili** per continuare l'installazione. Se si deseleziona questa casella di controllo e non si disinstalla il software non compatibile, si verifica l'errore e l'applicazione Kaspersky non viene installata.

La rimozione automatica delle applicazioni non compatibili è supportata da vari tipi di installazione.

Rimozione delle applicazioni incompatibili tramite un'attività dedicata

Per rimuovere le applicazioni incompatibili, utilizzare l'attività *Disinstalla l'applicazione in remoto*. Questa attività deve essere eseguita nei dispositivi prima dell'attività di installazione dell'applicazione di protezione. Ad esempio, nell'attività di installazione è possibile selezionare il tipo di pianificazione **Al completamento di un'altra attività**, dove l'altra attività è *Disinstalla l'applicazione in remoto*.

Questo metodo di disinstallazione è consigliabile quando il programma di installazione dell'applicazione di protezione non è in grado di rimuovere correttamente un'applicazione incompatibile.

Rimozione di Network Agent protetto da password utilizzando il prompt dei comandi

Per disinstallare da remoto il Network Agent per il quale è stata impostata una password di disinstallazione, è possibile utilizzare il prompt dei comandi.

Se si perde o si dimentica la password di Network Agent protetto da password installato nel dispositivo che non è più sotto la gestione di Kaspersky Security Center, non è possibile rimuovere Network Agent utilizzando l'utilità klmover, lo strumento Cleaner (cleaner.exe) o il prompt dei comandi. In questo caso, è necessario reinstallare il sistema operativo nel dispositivo in cui è installato Network Agent protetto da password.

Per disinstallare Network Agent tramite il prompt dei comandi:

1. Convertire la password di disinstallazione in un codice esadecimale.

   Utilizzare una risorsa Internet, un ambiente di programmazione, un editor di testo o un altro strumento adatto per convertire la password in codice esadecimale.

   > Assicurarsi che il delimitatore di output utilizzato per separare il codice esadecimale generato in parti sia impostato su `00`. Ad esempio, il codice esadecimale `51 77 65 72 74 79` non è corretto e il codice esadecimale `5100770065007200740079 00` è corretto.

2. Immettere il seguente comando nel prompt dei comandi, quindi premere **INVIO**:

   ```
   msiexec.exe /x{<product code>} /qn KLUNINSTPASSWD=<hex code of your uninstallation password>
   ```

   È possibile trovare il codice del prodotto del Network Agent nella tabella seguente.

Codici dei prodotti Network Agent

Localizzazione	Codice del prodotto
Arabo	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
Bulgaro	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
Ceco	{478A6A0B-D177-4402-B703-808C05C56B13}
Inglese	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
Francese	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
Tedesco	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
Ungherese	{8899A4D4-D678-49F8-AD96-0B784F58D355}
Italiano	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
Giapponese	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
Coreano	{70812A40-973B-4DA1-96B9-C2011280CD99}
Polacco	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
Portoghese	{0F05E4E5-5A89-482C-9A62-47CC58643788}
Rumeno	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
Russo	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
Cinese semplificato	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
Spagnolo	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
Spagnolo (Messico)	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
Cinese tradizionale	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
Turco	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

Utilizzo di strumenti per l'installazione remota di applicazioni in Kaspersky Security Center per l'esecuzione di file eseguibili nei dispositivi gestiti

Utilizzando la Creazione guidata nuovo pacchetto, è possibile selezionare qualsiasi file eseguibile e definire le impostazioni della riga di comando per tale file. È possibile aggiungere al pacchetto di installazione il file selezionato o l'intera cartella che lo contiene. È quindi necessario creare l'attività di installazione remota e selezionare il pacchetto di installazione che è stato creato.

Durante l'esecuzione dell'attività, il file eseguibile specificato con le impostazioni definite del prompt dei comandi verrà eseguito nei dispositivi di destinazione.

Se si utilizzano programmi di installazione in formato Microsoft Windows Installer (MSI), Kaspersky Security Center analizza i risultati dell'installazione per mezzo di strumenti standard.

Se è disponibile una licenza per Vulnerability e patch management, Kaspersky Security Center (durante la creazione di un pacchetto di installazione per qualsiasi applicazione supportata nell'ambiente aziendale) utilizza anche regole per l'installazione e l'analisi dei risultati dell'installazione presenti nel proprio database aggiornabile.

In caso contrario, l'attività predefinita per i file eseguibili attende il completamento del processo in esecuzione e di tutti i relativi processi secondari. Dopo completamento di tutti i processi in esecuzione, l'attività verrà completata correttamente, indipendentemente dal codice restituito del processo iniziale. Per modificare il comportamento di questa attività, prima di creare l'attività, è necessario modificare manualmente i file .kpd che sono stati generati da Kaspersky Security Center nella cartella del pacchetto di installazione appena creato e nelle relative sottocartelle.

I file .kpd utilizzano la codifica ASCII. I file .kud utilizzano la codifica Unicode.

Per fare in modo che l'attività non attenda il completamento del processo in esecuzione, impostare il valore dell'impostazione Wait su 0 nella sezione [SetupProcessResult]:

```
[SetupProcessResult]
Wait=0
```

Per fare in modo che l'attività attenda solo il completamento del processo in esecuzione in Windows, e non quello di tutti i processi secondari, impostare il valore dell'impostazione WaitJob su 0 nella sezione [SetupProcessResult], ad esempio:

```
[SetupProcessResult]
WaitJob=0
```

Affinché l'attività venga completata correttamente o restituisca un errore a seconda del codice di ritorno del processo in esecuzione, creare un file .bat eseguibile che salvi il codice di errore in un file, ad esempio:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

Quindi modificare i file .kud generati da Kaspersky Security Center nella cartella del pacchetto di installazione appena creato:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Installation completed successfully.
[SetupMainResult_ErrorCodes]
1=Installation script error
2=Custom error
```

In questo caso, qualsiasi codice diverso da quelli elencati determinerà la restituzione di un errore.

Per visualizzare nei risultati dell'attività una stringa con un commento relativo al completamento dell'attività o un errore, immettere brevi descrizioni degli errori che corrispondono ai codici restituiti del processo nelle sezioni [SetupProcessResult_SuccessCodes] e [SetupProcessResult_ErrorCodes], ad esempio:

```
[SetupProcessResult_SuccessCodes]
0=Installazione completata
3010=È necessario un riavvio per completare l'installazione
[SetupProcessResult_ErrorCodes]
1602=Installazione annullata dall'utente
1603=Errore irreversibile durante l'installazione
```

Per utilizzare gli strumenti di Kaspersky Security Center per gestire il riavvio del dispositivo (se è necessario un riavvio per completare un'operazione), elencare i codici restituiti del processo che indicano che deve essere eseguito un riavvio nella sezione [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
3010=
```

Monitoraggio della distribuzione

Per monitorare la distribuzione di Kaspersky Security Center e verificare che un'applicazione di protezione e Network Agent siano installati nei dispositivi gestiti, è necessario controllare l'indicatore a semaforo nella sezione **Distribuzione**. Questo indicatore a semaforo è disponibile nell'area di lavoro del nodo Administration Server nella finestra principale di Administration Console. L'indicatore a semaforo riflette lo stato corrente della distribuzione. Il numero di dispositivi con Network Agent e applicazioni di protezione installate è visualizzato accanto all'indicatore. Quando qualsiasi attività di installazione è in esecuzione, qui è possibile monitorarne lo stato di avanzamento. Se si verificano errori, il numero di errori viene visualizzato qui. È possibile visualizzare i dettagli di qualsiasi errore facendo clic sul collegamento.

È anche possibile utilizzare lo schema della distribuzione nell'area di lavoro della cartella **Dispositivi gestiti** nella scheda **Gruppi**. Il grafico riflette il processo di distribuzione, visualizzando il numero di dispositivi senza Network Agent, con Network Agent o con Network Agent e un'applicazione di protezione.

Per ulteriori informazioni sullo stato di avanzamento della distribuzione (o sull'esecuzione di una specifica attività di installazione), aprire la finestra dei risultati dell'attività di installazione remota appropriata: fare clic con il pulsante destro del mouse sull'attività, quindi selezionare **Risultati** nel menu di scelta rapida. La finestra visualizza due elenchi: quello superiore contiene gli stati dell'attività nei dispositivi, mentre quello inferiore contiene gli eventi dell'attività sul dispositivo attualmente selezionato nell'elenco superiore.

Le informazioni sugli errori di distribuzione vengono aggiunte al registro eventi Kaspersky su Administration Server. Le informazioni sugli errori sono disponibili anche nella selezione eventi corrispondente nella cartella **Rapporti e notifiche**, sottocartella **Eventi**.

Configurazione dei programmi di installazione

Questa sezione fornisce informazioni sui file dei programmi di installazione di Kaspersky Security Center e sulle impostazioni di installazione, oltre a raccomandazioni su come installare Administration Server e Network Agent in modalità automatica.

Informazioni generali

I programmi di installazione di Kaspersky Security Center 15.1 (Administration Server, Network Agent e Administration Console) sono basati sulla tecnologia Windows Installer. L'elemento fondamentale di un programma di installazione è un pacchetto MSI. Questo formato dei pacchetti consente di sfruttare tutti i vantaggi offerti da Windows Installer: la scalabilità, la disponibilità di un sistema di applicazione delle patch, il sistema di trasformazione, l'installazione centralizzata tramite soluzioni di terze parti e la registrazione trasparente con il sistema operativo.

Installazione in modalità automatica (con un file di risposta)

I programmi di installazione di Administration Server e Network Agent supportano l'utilizzo di un file di risposta (ss_install.xml), in cui sono integrate le parametri per l'installazione in modalità automatica senza la partecipazione dell'utente. Il file ss_install.xml è disponibile nella stessa cartella del pacchetto MSI e viene utilizzato automaticamente durante l'installazione in modalità automatica. È possibile abilitare la modalità di installazione automatica con il tasto della riga di comando "/s".

Un esempio di esecuzione del comando è il seguente:

```
setup.exe /s
```

Prima di avviare il programma di installazione in modalità automatica, leggere il Contratto di licenza con l'utente finale (EULA). Se il kit di distribuzione di Kaspersky Security Center non include un file TXT con il testo dell'EULA, è possibile scaricare il file dal sito Web di Kaspersky.

Il file ss_install.xml è un'istanza del formato interno dei parametri del programma di installazione di Kaspersky Security Center. I pacchetti di distribuzione contengono il file ss_install.xml con i parametri predefiniti.

Non modificare il file ss_install.xml manualmente. Questo file può essere modificato mediante gli strumenti di Kaspersky Security Center durante la modifica dei parametri dei pacchetti di installazione in Administration Console.

Per modificare il file di risposta per l'installazione di Administration Server:

1. Aprire il pacchetto di distribuzione di Kaspersky Security Center. Se si utilizza un file EXE del pacchetto completo, decomprimerlo.
2. Nella cartella Server, aprire la riga di comando e quindi eseguire il seguente comando:
   ```
   setup.exe /r ss_install.xml
   ```
   Viene avviato il programma di installazione di Kaspersky Security Center.
3. Seguire i passaggi della procedura guidata per configurare l'installazione di Kaspersky Security Center.

   Una volta completata la procedura guidata, il file di risposta viene modificato automaticamente in base alle nuove impostazioni specificate.

Installazione di Network Agent in modalità automatica (senza un file di risposta)

È possibile installare Network Agent con un singolo pacchetto .msi, specificando i valori delle proprietà MSI nella modalità standard. Questo scenario consente l'installazione di Network Agent tramite i criteri di gruppo.

Non rinominare il pacchetto di installazione Kaspersky Network Agent.msi. La ridenominazione del pacchetto potrebbe causare errori di installazione durante gli aggiornamenti futuri di Network Agent.

Per evitare conflitti tra i parametri definiti attraverso le proprietà MSI e i parametri definiti nel file di risposta, è possibile disabilitare il file di risposta impostando la proprietà `DONT_USE_ANSWER_FILE=1`. Il file MSI è disponibile nel pacchetto di distribuzione di Kaspersky Security Center, nella cartella Packages\NetAgent\exec. Un esempio di esecuzione del programma di installazione di Network Agent con un pacchetto .msi è il seguente.

L'installazione di Network Agent in modalità automatica richiede l'accettazione delle condizioni del Contratto di licenza con l'utente finale. Utilizzare il parametro `EULA=1` solo se l'utente ha letto, compreso e accettato i termini del Contratto di licenza con l'utente finale.

Esempio:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

È anche possibile definire i parametri di installazione per un pacchetto msi preparando in anticipo il file di risposta (con estensione mst). Questo comando si presenta come segue:

Esempio:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

È possibile specificare diversi file di risposta in un singolo comando.

Se si desidera aggiornare Network Agent tramite il programma di installazione di Windows, eseguire il seguente comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Configurazione parziale dell'installazione tramite setup.exe

Durante l'esecuzione dell'installazione delle applicazioni tramite setup.exe, è possibile aggiungere i valori di qualsiasi proprietà MSI al pacchetto MSI.

Questo comando si presenta come segue:

Esempio:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parametri di installazione di Administration Server

Nella tabella seguente sono descritte le proprietà MSI che è possibile configurare durante l'installazione di Administration Server. Tutti i parametri sono facoltativi, ad eccezione di EULA e PRIVACYPOLICY.

Proprietà MSI	Descrizione	Valori disponibili
EULA	Accettazione dei termini del Contratto di licenza (obbligatorio)	• 1 - Ho letto, compreso e accettato i termini del Contratto di licenza con l'utente finale. • Altri valori o nessun valore- Non accetto i termini del Contratto di licenza (l'installazione non viene eseguita).
PRIVACYPOLICY	Accettazione dei termini dell'Informativa sulla privacy (obbligatorio)	• 1 - Sono consapevole e accetto che i miei dati vengano gestiti e trasmessi (anche a paesi terzi) come descritto nell'Informativa sulla privacy. Confermo di aver letto e compreso l'Informativa sulla privacy. • Altro valore o nessun valore- Non accetto i termini dell'Informativa sulla privacy (l'installazione non viene eseguita).
INSTALLATIONMODETYPE	Tipo di installazione di Administration Server	• Standard. • Personalizzato.
INSTALLDIR	Cartella di installazione dell'applicazione	Valore stringa.
ADDLOCAL	Elenco dei componenti da installare (separati da virgole)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Elenco minimo di componenti sufficienti per la corretta installazione di Administration Server: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Dimensione della rete	• NRT_1_100 – Da 1 a 100 dispositivi. • NRT_100_1000 – Da 101 a 1000 dispositivi. • NRT_GREATER_1000 – Oltre 1000 dispositivi.
SRV_ACCOUNT_TYPE	Consente di specificare l'utente per l'esecuzione del servizio Administration Server	• SrvAccountDefault - L'account utente sarà creato automaticamente. • SrvAccountUser- L'account utente è definito manualmente.
SERVERACCOUNTNAME	Nome utente per il servizio	Valore stringa.
SERVERACCOUNTPWD	Password dell'utente per il servizio	Valore stringa.
DBTYPE	Tipo di database	• MySQL - Verrà utilizzato un database MySQL o MariaDB. • MSSQL - Verrà utilizzato il database Microsoft SQL Server (SQL Express).
MYSQLSERVERNAME	Nome completo del server MySQL o MariaDB	Valore stringa.
MYSQLSERVERPORT	Numero di porta per la connessione al server MySQL o MariaDB	Valore numerico.
MYSQLDBNAME	Nome del database del server MySQL o MariaDB	Valore stringa.
MYSQLACCOUNTNAME	Nome utente per la connessione al database del server MySQL o MariaDB	Valore stringa.
MYSQLACCOUNTPWD	Password utente per la connessione al database del server MySQL o MariaDB	Valore stringa.
MSSQLCONNECTIONTYPE	Tipo di utilizzo del database MSSQL	• InstallMSSEE - Installazione da un pacchetto. • ChooseExisting - Utilizzo del server installato.
MSSQLSERVERNAME	Nome completo dell'istanza di SQL Server	Valore stringa.
MSSQLDBNAME	Nome del database del server SQL	Valore stringa.

Proprietà MSI	Descrizione	Valori disponibili
MSSQLAUTHTYPE	Metodo di autenticazione per la connessione a SQL Server	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nome utente per la connessione a SQL Server in modalità SQLServer	Valore stringa.
MSSQLACCOUNTPWD	Password dell'utente per la connessione a SQL Server in modalità SQLServer	Valore stringa.

CREATE_SHARE_TYPE	Metodo per la specificazione della cartella condivisa	• Create - Creare una nuova cartella condivisa. In questo caso, è necessario definire le seguenti proprietà:
		  • SHARELOCALPATH - Percorso di una cartella locale.
		  • SHAREFOLDERNAME - Nome di rete di una cartella.
		• Null - Deve essere specificata la proprietà EXISTSHAREFOLDERNAME.

EXISTSHAREFOLDERNAME	Percorso completo di una cartella condivisa esistente	Valore stringa.
SERVERPORT	Numero di porta per la connessione ad Administration Server	Valore numerico.
SERVERSSLPORT	Numero di porta per la creazione di una connessione ad Administration Server	Valore numerico.
SERVERADDRESS	Indirizzo di Administration Server	Valore stringa.
SERVERCERT2048BITS	Dimensione della chiave per il certificato di Administration Server (in bit)	• 1 - La dimensione della chiave per il certificato di Administration Server è di 2048 bit. • 0 - La dimensione della chiave per il certificato di Administration Server è di 1024 bit. • Se non viene specificato alcun valore, la dimensione della chiave per il certificato di Administration Server è di 2048 bit.
MOBILESERVERADDRESS	Indirizzo dell'Administration Server per la connessione dei dispositivi mobili; ignorato se il componente MobileSupport non è stato selezionato	Valore stringa.

Impostazioni di installazione di Network Agent

Nella tabella seguente sono descritte le proprietà MSI che è possibile configurare durante l'installazione di Network Agent. Tutte le parametri sono facoltative, ad eccezione di SERVERADDRESS.

Proprietà di MSI

Proprietà MSI	Descrizione	Valori disponibili
DONT_USE_ANSWER_FILE	Leggere i parametri di installazione dal file di risposta	• 1 • Null
INSTALLDIR	Cartella di installazione	
SERVERADDRESS	Indirizzo di Administration Server (obbligatorio)	
SERVERPORT	Numero di porta per la connessione ad Administration Server	
SERVERSSLPORT	Numero di porta per la connessione SSL	

Proprietà MSI	Descrizione	Valori disponibili
USESSL	Specifica se utilizzare connessione SSL	• 1 • Null
OPENUDPPORT	Specifica se aprire una porta UDP	• 1 • Null
UDPPORT	Numero di porta UDP	
USEPROXY	Specifica se utilizzare un server proxy	• 1 • Null
PROXYADDRESS	Indirizzo proxy	
PROXYPORT	Numero di porta per la connessione ad Administration Server	
PROXYLOGIN	Account per la connessione a un server proxy	
PROXYPASSWORD	Password di un account per la connessione a un server proxy. Non specificare dettagli degli account privilegiati nei parametri dei pacchetti di installazione.	
GATEWAYMODE	Modalità di utilizzo del gateway di connessione	• 0 - Non utilizzare il gateway di connessione • 1 - Utilizza questo Network Agent come gateway di connessione • 2 - Connetti ad Administration Server utilizzando il gateway di connessione
GATEWAYADDRESS	Indirizzo gateway connessione	
CERTSELECTION	Metodo di ricezione di un certificato	• GetOnFirstConnection - Ricevere un certificato da Administration Server. • GetExistent - Selezionare un certificato esistente. Se questa opzione è selezionata, è necessario definire la proprietà CERTFILE.
CERTFILE	Percorso del file di certificato	
VMVDI	Abilita modalità dinamica per VDI	• 1 • Null
LAUNCHPROGRAM	Specifica se eseguire il servizio Network Agent dopo l'installazione	• 1 • Null

Infrastruttura virtuale

Kaspersky Security Center supporta l'utilizzo di macchine virtuali. È possibile installare Network Agent e l'applicazione di protezione in ogni macchina virtuale, nonché proteggere le macchine virtuali a livello di hypervisor. Nel primo caso è possibile utilizzare un'applicazione di protezione standard o Kaspersky Security for Virtualization Light Agent per proteggere le macchine virtuali. Nel secondo caso è possibile utilizzare Kaspersky Security for Virtualization Agentless.

Kaspersky Security Center supporta i rollback delle macchine virtuali allo stato precedente.

Suggerimenti per la riduzione del carico sulle macchine virtuali

Durante l'installazione di Network Agent in una macchina virtuale, è consigliabile valutare se disabilitare alcune funzionalità di Kaspersky Security Center che risultano di scarsa utilità per le macchine virtuali.

Quando si installa Network Agent in una macchina virtuale o in un modello utilizzato per la generazione di macchine virtuali, è consigliabile eseguire le seguenti azioni:

- Se si esegue un'installazione remota, nella finestra delle proprietà del pacchetto di installazione di Network Agent, nella sezione **Avanzate** selezionare l'opzione **Ottimizza le impostazioni per VDI**.
- Se si esegue un'installazione interattiva tramite una procedura guidata, nella finestra della procedura guidata selezionare l'opzione **Ottimizza le impostazioni di Network Agent per l'infrastruttura virtuale**.

La selezione di queste opzioni modifica le impostazioni di Network Agent in modo da mantenere disabilitate le seguenti funzionalità per impostazione predefinita (prima dell'applicazione di un criterio):

- Recupero delle informazioni sul software installato
- Recupero delle informazioni sull'hardware
- Recupero delle informazioni sulle vulnerabilità rilevate
- Recupero delle informazioni sugli aggiornamenti richiesti

In genere, queste funzionalità non sono necessarie nelle macchine virtuali perché utilizzano software uniforme e hardware virtuale.

La disabilitazione delle funzionalità è reversibile. Se è richiesta una delle funzionalità disabilitate, è possibile abilitarla tramite il criterio di Network Agent o mediante le impostazioni locali di Network Agent. Le impostazioni locali di Network Agent sono disponibili tramite il menu di scelta rapida del dispositivo appropriato in Administration Console.

Supporto delle macchine virtuali dinamiche

Kaspersky Security Center supporta le macchine virtuali dinamiche. Se nella rete dell'organizzazione è stata distribuita un'infrastruttura virtuale, in alcuni casi è possibile utilizzare macchine virtuali (temporanee) dinamiche. Le macchine virtuali dinamiche vengono create con nomi univoci in base a un modello che è stato preparato dall'amministratore. L'utente lavora su una macchina virtuale per un certo periodo e, dopo lo spegnimento, questa macchina virtuale sarà rimossa dall'infrastruttura virtuale. Se Kaspersky Security Center è stato distribuito nella rete dell'organizzazione, una macchina virtuale con Network Agent installato verrà aggiunta al database di Administration Server. Dopo lo spegnimento di una macchina virtuale, anche la voce corrispondente deve essere rimossa dal database di Administration Server.

Per rendere disponibile la funzionalità di rimozione automatica delle voci nelle macchine virtuali, durante l'installazione di Network Agent in un modello per le macchine virtuali dinamiche, selezionare l'opzione **Abilita modalità dinamica per VDI**:

- Per l'installazione remota - Nella finestra delle proprietà del pacchetto di installazione di Network Agent (sezione **Avanzate**)
- Per l'installazione interattiva - Nell'Installazione guidata di Network Agent

Evitare di selezionare l'opzione **Abilita modalità dinamica per VDI** durante l'installazione di Network Agent nei dispositivi fisici.

Se si desidera archiviare gli eventi generati dalle macchine virtuali dinamiche in Administration Server per un certo periodo dopo la rimozione delle macchine virtuali, nella finestra delle proprietà di Administration Server, nella sezione **Archivio eventi**, selezionare l'opzione **Archivia eventi dopo l'eliminazione dei dispositivi** e specificare il periodo di archiviazione massimo degli eventi (in giorni).

Non è consigliabile abilitare il criptaggio delle unità nelle macchine virtuali dinamiche.

Supporto della copia delle macchine virtuali

La copia di una macchina virtuale con Network Agent installato o la creazione di una macchina virtuale da un modello con Network Agent installato sono identiche alla distribuzione dei Network Agent tramite l'acquisizione e la copia di un'immagine del disco rigido. In generale, durante la copia delle macchine virtuali è necessario eseguire le stesse azioni previste durante la distribuzione di Network Agent tramite la copia un'immagine del disco.

Tuttavia, nei due casi descritti di seguito viene illustrato Network Agent, che rileva automaticamente la copia. Per i motivi indicati in precedenza, non è necessario eseguire le operazioni sofisticate descritte in "Distribuzione tramite l'acquisizione e la copia dell'immagine del disco rigido di un dispositivo":

- L'opzione **Abilita modalità dinamica per VDI** era selezionata durante l'installazione di Network Agent: dopo ogni riavvio del sistema operativo, questa macchina virtuale sarà riconosciuta come un nuovo dispositivo, indipendentemente dal fatto che sia stata copiata.
- È in uso uno dei seguenti hypervisor: VMware™, HyperV® o Xen®: Network Agent rileva la copia della macchina virtuale in base agli ID modificati dell'hardware virtuale.

L'analisi delle modifiche nell'hardware virtuale non è assolutamente affidabile. Prima di applicare questo metodo su larga scala, è necessario testarlo su un piccolo gruppo di macchine virtuali per la versione dell'hypervisor attualmente in uso nell'organizzazione.

Supporto del rollback del file system per i dispositivi con Network Agent

Kaspersky Security Center è un'applicazione distribuita. Il rollback del file system uno stato precedente in un dispositivo con Network Agent installato determinerà la mancata sincronizzazione dei dati e impedirà il corretto funzionamento di Kaspersky Security Center.

È possibile eseguire il rollback del file system (o di una sua parte) nei seguenti casi:

- Durante la copia di un'immagine del disco rigido.
- Durante il ripristino di uno stato della macchina virtuale tramite l'infrastruttura virtuale.
- Durante il ripristino dei dati da una copia di backup o da un punto di ripristino.

Gli scenari in cui software di terze parti nei dispositivi con Network Agent installato influisce sulla cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ sono solo scenari critici per Kaspersky Security Center. Pertanto, è necessario escludere sempre questa cartella dalla procedura di ripristino, se possibile.

Dal momento che le regole per l'ambiente di lavoro di alcune organizzazioni consentono i rollback del file system nei dispositivi, il supporto per il rollback del file system nei dispositivi con Network Agent installato è stato aggiunto a Kaspersky Security Center a partire dalla versione 10 Maintenance Release 1 (Administration Server e i Network Agent devono essere della versione 10 Maintenance Release 1 o successiva). Quando sono rilevati, tali dispositivi vengono riconnessi automaticamente all'Administration Server con una cancellazione completa dei dati e una sincronizzazione completa.

Per impostazione predefinita, il supporto per il rilevamento del rollback del file system è abilitato in Kaspersky Security Center 15.1.

Per quanto possibile, evitare di eseguire il rollback della cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ nei dispositivi con Network Agent installato, perché la risincronizzazione completa dei dati richiede una notevole quantità di risorse.

Non è assolutamente consentito un rollback dello stato del sistema in un dispositivo con Administration Server installato, né un rollback del database utilizzato da Administration Server.

È possibile ripristinare uno stato di Administration Server da una copia di backup solo con l'utilità klbackup standard.

Informazioni sui profili di connessione per gli utenti fuori sede

Gli utenti fuori sede con computer portatili (di seguito denominati anche "dispositivi") possono aver bisogno di modificare il metodo di connessione a un Administration Server o passare da un Administration Server all'altro a seconda della posizione corrente del dispositivo nella rete aziendale.

I profili di connessione sono supportati solo per i dispositivi che eseguono Windows e macOS.

Utilizzo di differenti indirizzi di un singolo Administration Server

I dispositivi con Network Agent installato possono connettersi all'Administration Server dalla rete Intranet dell'organizzazione o da Internet. Questa situazione può richiedere l'utilizzo da parte di Network Agent di differenti indirizzi per la connessione ad Administration Server: l'indirizzo esterno dell'Administration Server per la connessione Internet e l'indirizzo interno dell'Administration Server per la connessione dalla rete interna.

A tale scopo, è necessario aggiungere un profilo (per la connessione ad Administration Server da Internet) al criterio di Network Agent. Aggiungere il profilo nelle proprietà del criterio (sezione **Connettività**, sottosezione **Profili connessione**). Nella finestra di creazione del profilo è necessario disabilitare l'opzione **Usa per ricevere solo aggiornamenti** e selezionare l'opzione **Sincronizza le impostazioni di connessione con le impostazioni di Administration Server specificate nel profilo**. Se si utilizza un gateway di connessione per accedere ad Administration Server (ad esempio, in una configurazione di Kaspersky Security Center come quella descritta in Accesso a Internet: Network Agent come gateway nella rete perimetrale), è necessario specificare l'indirizzo del gateway di connessione nel campo corrispondente del profilo di connessione.

Passaggio da un Administration Server all'altro a seconda della rete corrente

Se l'organizzazione ha più sedi con diversi Administration Server e alcuni dispositivi con Network Agent installato si spostano tra di esse, è necessario che Network Agent si connetta all'Administration Server della rete locale nella sede in cui si trova attualmente il dispositivo.

In questo caso, è necessario creare un profilo per la connessione ad Administration Server nelle proprietà del criterio di Network Agent per ciascuna delle sedi, tranne che per la sede principale in cui si trova l'Administration Server principale originale. È necessario specificare gli indirizzi di Administration Server nei profili di connessione e abilitare o disabilitare l'opzione **Usa per ricevere solo aggiornamenti**:

- Selezionare l'opzione se è necessario sincronizzare Network Agent con l'Administration Server principale e utilizzare il server locale solo per scaricare gli aggiornamenti.
- Disabilitare questa opzione se è necessario che Network Agent sia completamente gestito dall'Administration Server locale.

Sarà quindi necessario impostare le condizioni per il passaggio ai nuovi profili creati: almeno una condizione per ciascuna delle sedi, tranne che per la sede principale. Lo scopo di ogni condizione consiste nel rilevamento degli elementi che sono specifici per l'ambiente di rete di una sede. Se una condizione è vera, il profilo corrispondente viene attivato. Se nessuna delle condizioni è vera, Network Agent passa all'Administration Server principale.

Distribuzione della funzionalità Mobile Device Management

Questa sezione fornisce informazioni sulla distribuzione iniziale della funzionalità Mobile Device Management.

Connessione dei dispositivi KES ad Administration Server

A seconda del metodo utilizzato per la connessione dei dispositivi ad Administration Server, sono possibili due schemi di distribuzione per Kaspersky Device Management for iOS per i dispositivi KES:

- Schema di distribuzione con connessione diretta dei dispositivi all'Administration Server
- Schema di distribuzione che coinvolge un proxy inverso che supporta la delega vincolata Kerberos

Connessione diretta dei dispositivi all'Administration Server

I dispositivi KES possono connettersi direttamente alla porta 13292 di Administration Server.

A seconda del metodo utilizzato per l'autenticazione, sono possibili due opzioni per la connessione dei dispositivi KES all'Administration Server:

- Connessione dei dispositivi con un certificato utente
- Connessione dei dispositivi senza un certificato utente

Connessione di un dispositivo con un certificato utente

Durante la connessione di un dispositivo con un certificato utente, il dispositivo viene associato all'account utente a cui è stato assegnato il certificato corrispondente tramite gli strumenti di Administration Server.

In questo caso verrà utilizzata l'autenticazione SSL bidirezionale (autenticazione reciproca). Sia l'Administration Server che il dispositivo verranno autenticati con certificati.

Connessione di un dispositivo senza un certificato utente

Durante la connessione di un dispositivo senza un certificato utente, il dispositivo non viene associato ad alcun account utente in Administration Server. Tuttavia, quando il dispositivo riceve un certificato, il dispositivo verrà associato all'utente a cui è stato assegnato il certificato corrispondente tramite gli strumenti di Administration Server.

Durante la connessione del dispositivo all'Administration Server, sarà applicata l'autenticazione SSL unidirezionale, il che significa che solo l'Administration Server viene autenticato con il certificato. Dopo il recupero del certificato utente da parte del dispositivo, il tipo di autenticazione diventerà autenticazione SSL bidirezionale (autenticazione SSL bidirezionale, autenticazione reciproca).

Schema per la connessione dei dispositivi KES al server tramite Kerberos Constrained Delegation (KCD)

Lo schema per la connessione dei dispositivi KES all'Administration Server tramite Kerberos Constrained Delegation (KCD) offre quanto segue:

- Integrazione con un proxy inverso che supporta KCD.
- Utilizzo di Kerberos Constrained Delegation (di seguito denominato KCD) per l'autenticazione dei dispositivi mobili.
- Integrazione con l'infrastruttura Public Key Infrastructure (di seguito denominata PKI) per l'applicazione dei certificati utente.

Quando si utilizza questo schema di connessione, tenere presente quanto segue:

- Il tipo di connessione dei dispositivi KES al proxy inverso deve essere l'autenticazione SSL bidirezionale: un dispositivo deve connettersi al proxy inverso tramite il relativo certificato utente proprietario. A tale scopo, è necessario integrare il certificato utente nel pacchetto di installazione di Kaspersky Endpoint Security for Android, che è stato installato nel dispositivo. Questo pacchetto KES deve essere creato dall'Administration Server specificamente per questo dispositivo (utente).

- È necessario specificare lo speciale certificato (personalizzato) invece del certificato server predefinito per il protocollo mobile:

  1. Nella finestra delle proprietà di Administration Server, nella sezione **Impostazioni**, selezionare la casella di controllo **Apri porta per i dispositivi mobili** e selezionare **Aggiungi certificato** nell'elenco a discesa.

  2. Nella finestra visualizzata specificare lo stesso certificato che è stato impostato nel proxy inverso al momento della pubblicazione del punto di accesso al protocollo mobile nell'Administration Server.

- I certificati utente per i dispositivi KES devono essere emessi dall'Autorità di certificazione (CA) del dominio. Tenere presente che se il dominio include più Autorità di certificazione radice, i certificati utente devono essere emessi dall'Autorità di certificazione che è stata impostata nella pubblicazione nel proxy inverso.

  È possibile garantire che il certificato utente sia conforme a tale requisito utilizzando uno dei seguenti metodi:

  - Specificare lo certificato utente speciale nella Creazione guidata nuovo pacchetto e nell'Installazione guidata certificato.

  - Integrare l'Administration Server con l'infrastruttura PKI del dominio e definire l'impostazione corrispondente nelle regole per l'emissione dei certificati:

    1. Nella struttura della console espandere la cartella **Mobile Device Management**, quindi selezionare la sottocartella **Certificati**.

    2. Nell'area di lavoro della cartella **Certificati** fare clic sul pulsante **Configura regole di emissione certificati** per aprire la finestra **Regole di emissione certificati**.

    3. Nella sezione **Integrazione con PKI** configurare l'integrazione con l'infrastruttura a chiave pubblica (PKI).

    4. Nella sezione **Emissione di certificati mobili** specificare l'origine dei certificati.

Di seguito è riportato un esempio di configurazione di Kerberos Constrained Delegation (KCD) con i seguenti presupposti:

- Il punto di accesso al protocollo mobile in Administration Server è impostato sulla porta 13292.

- Il nome del dispositivo con il proxy inverso è firewall.mydom.local.

- Il nome del dispositivo con Administration Server è ksc.mydom.local.

- Il nome della pubblicazione esterna del punto di accesso al protocollo mobile è kes4mob.mydom.global.

Account di dominio per Administration Server

È necessario creare un account di dominio (ad esempio, KSCMobileSrvcUsr) con cui verrà eseguito il servizio Administration Server. È possibile specificare un account per il servizio Administration Server al momento dell'installazione di Administration Server o tramite l'utilità klsrvswch. L'utilità klsrvswch è disponibile nella cartella di installazione di Administration Server. Il percorso di installazione predefinito: <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

È necessario specificare un account di dominio per i motivi seguenti:

- La funzionalità di gestione dei dispositivi KES è una parte integrante di Administration Server.
- Per garantire il corretto funzionamento di Kerberos Constrained Delegation (KCD), la parte ricevente (ovvero, Administration Server) deve essere in esecuzione con un account di dominio.

Nome dell'entità servizio per http/kes4mob.mydom.local

Nel dominio, con l'account KSCMobileSrvcUsr, aggiungere un SPN per pubblicare il servizio del protocollo mobile sulla porta 13292 del dispositivo con Administration Server. Per il dispositivo kes4mob.mydom.local con Administration Server, si presenta come segue:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Configurazione delle proprietà di dominio del dispositivo con il proxy inverso (firewall.mydom.local)

Per delegare il traffico, è necessario impostare come attendibile il dispositivo con il proxy inverso (firewall.mydom.local) per il servizio definito dall'SPN (http/kes4mob.mydom.local:13292).

Per impostare come attendibile il dispositivo con il proxy inverso per il servizio definito dall'SPN (http/kes4mob.mydom.local:13292), l'amministratore deve eseguire seguenti le operazioni:

1. Nello snap-in Microsoft Management Console "Utenti e computer di Active Directory" selezionare il dispositivo in cui è installato il proxy inverso (firewall.mydom.local).
2. Nelle proprietà del dispositivo, nella scheda **Delega**, impostare l'interruttore **Computer attendibile per la delega solo ai servizi specificati** su **Utilizza un qualsiasi protocollo di autenticazione**.
3. Nell'elenco **Servizi ai quali l'account può presentare credenziali delegate** aggiungere l'SPN http/kes4mob.mydom.local:13292.

Speciale certificato (personalizzato) per la pubblicazione (kes4mob.mydom.global)

Per pubblicare il protocollo mobile di Administration Server, è necessario emettere uno speciale certificato (personalizzato) per il nome FQDN kes4mob.mydom.global e specificarlo invece del certificato server predefinito nelle impostazioni del protocollo mobile di Administration Server in Administration Console. A tale scopo, nella finestra delle proprietà di Administration Server, nella sezione **Impostazioni**, selezionare la casella di controllo **Apri porta per i dispositivi mobili** e quindi selezionare **Aggiungi certificato** nell'elenco a discesa.

Il contenitore del certificato server (file con estensione p12 o pfx) deve anche contenere una catena di certificati radice (chiavi pubbliche).

Configurazione della pubblicazione nel proxy inverso

Nel proxy inverso, per il traffico dal dispositivo mobile alla porta 13292 kes4mob.mydom.global, è necessario configurare KCD sull'SPN (http/kes4mob.mydom.local:13292) utilizzando il certificato server emesso per il nome FQDN kes4mob.mydom.global. La pubblicazione e il punto di accesso pubblicato (la porta 13292 di Administration Server) devono condividere lo stesso certificato server.

Utilizzo di Firebase Cloud Messaging

Per garantire l'invio tempestivo dei comandi ai dispositivi KES gestiti dal sistema operativo Android, Kaspersky Security Center usa il meccanismo delle notifiche push. Le notifiche push vengono scambiate tra i dispositivi KES e Administration Server tramite Firebase Cloud Messaging (di seguito FCM). In Kaspersky Security Center Administration Console è possibile specificare le impostazioni di Cloud Firebase Messaging per la connessione dei dispositivi KES al servizio.

Per recuperare le impostazioni di Firebase Cloud Messaging, è necessario disporre di un account Google.

Per abilitare l'utilizzo di FCM:

1. In Administration Console selezionare il nodo **Mobile Device Management** e la cartella **Dispositivi mobili**.
2. Dal menu di scelta rapida della cartella **Dispositivi mobili** selezionare **Proprietà**.
3. Nelle proprietà della cartella selezionare la sezione **Impostazioni di Firebase Cloud Messaging**.
4. Nel campo **Numero progetto Firebase**, specificare l'ID del mittente FCM.
5. Nel campo **File della chiave privata (in formato JSON)**, selezionare il file della chiave privata.

   Alla successiva sincronizzazione con Administration Server, i dispositivi KES gestiti da sistemi operativi Android verranno connessi a Firebase Cloud Messaging.

È possibile modificare le impostazioni di Firebase Cloud Messaging facendo clic sul pulsante **Ripristina impostazioni**.

Quando si passa a un progetto Firebase diverso, è necessario attendere 10 minuti per il ripristino di FCM.

Il servizio FCM viene eseguito nei seguenti intervalli di indirizzi:

- Sul lato del dispositivo KES, è necessario l'accesso alle porte 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) e 5230 (HTTPS) dei seguenti indirizzi:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Tutti gli indirizzi IP elencati nell'ASN Google numero 15169
- Sul lato dell'Administration Server, è necessario l'accesso alla porta 443 (HTTPS) dei seguenti indirizzi:
  - fcm.googleapis.com
  - Tutti gli indirizzi IP elencati nell'ASN Google numero 15169

Se le impostazioni del server proxy (**Avanzate** / **Configurazione dell'accesso a Internet**) sono state specificate nelle proprietà di Administration Server in Administration Console, saranno utilizzate per l'interazione con FCM.

Configurazione di FCM: ottenere l'ID del mittente e il file della chiave privata

Per configurare il FCM:

1. Eseguire la registrazione nel portale Google.
2. Passare alla console Firebase.
3. Eseguire una delle seguenti operazioni:
   - Per creare un nuovo progetto, fare clic su **Crea un progetto** e seguire le istruzioni sullo schermo.
   - Aprire un progetto esistente.
4. Fare clic sull'icona a forma di ingranaggio e selezionare **Impostazioni progetto**.

   Verrà visualizzata la **finestra Impostazioni progetto**.
5. Selezionare la scheda **Cloud Messaging**.
6. Recuperare l'ID del mittente pertinente dal campo **ID mittente** nella sezione **Firebase Cloud Messaging API (V1)**.
7. Selezionare la scheda **Account di servizio** e fare clic su **Genera nuova chiave privata**.
8. Nella finestra visualizzata, fare clic su **Genera chiave** per generare e scaricare un file di chiave privata.

Firebase Cloud Messaging è ora configurato.

Integrazione con PKI (Public Key Infrastructure)

L'integrazione con l'infrastruttura Public Key Infrastructure (di seguito denominata PKI) ha principalmente l'obiettivo di semplificare l'emissione dei certificati utente di dominio da parte di Administration Server.

L'amministratore può assegnare un certificato di dominio per un utente in Administration Console. A tale scopo, è possibile utilizzare uno dei seguenti metodi:

- Assegnare all'utente uno speciale certificato (personalizzato) da un file nell'Installazione guidata certificato.
- Eseguire l'integrazione con PKI e assegnare a PKI il ruolo di origine dei certificati per un tipo specifico di certificati o per tutti i tipi di certificati.

Le impostazioni dell'integrazione con PKI sono disponibili nell'area di lavoro della cartella **Mobile Device Management** / **Certificati** facendo clic sul collegamento **Integra con infrastruttura a chiave pubblica (PKI)**.

Principio generale di integrazione con PKI per l'emissione dei certificati utente di dominio

In Administration Console fare clic sul collegamento **Integra con infrastruttura a chiave pubblica (PKI)** nell'area di lavoro della cartella **Mobile Device Management** / **Certificati** per specificare un account di dominio che sarà utilizzato da Administration Server per emettere i certificati utente di dominio tramite l'Autorità di certificazione del dominio (di seguito denominato account utilizzato per l'integrazione con PKI).

Tenere presente quanto segue:

- Le impostazioni di integrazione con PKI offrono la possibilità di specificare il modello predefinito per tutti i tipi di certificati. Le regole per l'emissione dei certificati (disponibili nell'area di lavoro della cartella **Mobile Device Management** / **Certificati** facendo clic sul pulsante **Configura regole di emissione certificati**) consentono di specificare un singolo modello per ogni tipo di certificati.
- Un speciale certificato Enrollment Agent (EA) deve essere installato nel dispositivo con Administration Server, nell'archivio di certificati dell'account utilizzato per l'integrazione con PKI. Il certificato Enrollment Agent (EA) viene emesso dall'amministratore dell'Autorità di certificazione del dominio.

L'account utilizzato per l'integrazione con PKI deve soddisfare i seguenti criteri:

- È un utente di dominio.
- È un amministratore locale del dispositivo con Administration Server da cui viene avviata l'integrazione con PKI.
- Ha il diritto di *accesso come servizio*.
- Il dispositivo in cui è installato Administration Server deve essere in esecuzione almeno una volta con questo account per creare un profilo utente permanente.

Server Web di Kaspersky Security Center

Il Server Web di Kaspersky Security Center (di seguito denominato server Web) è un componente di Kaspersky Security Center. Il server Web è progettato per la pubblicazione di pacchetti di installazione indipendenti, pacchetti di installazione indipendenti per dispositivi mobili e file dalla cartella condivisa.

I pacchetti di installazione creati vengono pubblicati automaticamente sul server Web e vengono rimossi dopo il primo download. L'amministratore può inviare il nuovo collegamento all'utente con qualsiasi sistema (ad esempio, tramite e-mail).

Facendo clic su questo collegamento, l'utente può scaricare le informazioni richieste in un dispositivo mobile.

Impostazioni del server Web

Se è necessario ottimizzare il server Web, le relative proprietà consentono di modificare le porte per HTTP (8060) e HTTPS (8061). Oltre a modificare le porte, è possibile sostituire il certificato server per HTTPS e modificare il nome FQDN del server Web per HTTP.

Altre operazioni di routine

Questa sezione fornisce raccomandazioni sul funzionamento di routine di Kaspersky Security Center.

Monitoraggio dei semafori e degli eventi registrati in Administration Console

Administration Console consente di valutare rapidamente lo stato attuale di Kaspersky Security Center e dei dispositivi gestiti controllando indicatori a semaforo. Gli indicatori a semaforo sono visualizzati nell'area di lavoro del nodo **Administration Server**, nella scheda **Monitoraggio**. La scheda fornisce sei riquadri informazioni con indicatori a semaforo ed eventi registrati. L'indicatore a semaforo è una barra verticale colorata a sinistra di un riquadro. Ogni riquadro con un indicatore corrisponde a uno specifico ambito funzionale di Kaspersky Security Center (vedere la tabella seguente).

Ambiti coperti dagli indicatori a semaforo in Administration Console

Nome del riquadro	Ambito dell'indicatore
Distribuzione	Installazione di Network Agent e delle applicazioni di protezione nei dispositivi nella rete di un'organizzazione
Schema di gestione	Struttura dei gruppi di amministrazione. Scansione della rete. Regole di spostamento dei dispositivi
Impostazioni di protezione	Funzionalità dell'applicazione di protezione: stato protezione, scansione malware
Aggiorna	Aggiornamenti e patch
Monitoraggio	Stato protezione
Administration Server	Funzionalità e proprietà di Administration Server

Ogni indicatore a semaforo può assumere cinque colori (vedere la tabella seguente). Il colore di un indicatore dipende dallo stato attuale di Kaspersky Security Center e dagli eventi che sono stati registrati.

Colori degli indicatori a semaforo

Stato	Colore dell'indicatore	Significato del colore dell'indicatore
Informativo	Verde	Non è richiesto l'intervento dell'amministratore.
Avviso	Giallo	È richiesto l'intervento dell'amministratore.
Critico	Rosso	Si sono verificati problemi gravi. È richiesto l'intervento dell'amministratore per risolverli.

Stato	Colore dell'indicatore	Significato del colore dell'indicatore
Informativo	Azzurro	Sono stati registrati eventi che non sono correlati a minacce potenziali o effettive per la sicurezza dei dispositivi gestiti.
Informativo	Grigio	I dettagli degli eventi non sono disponibili o non sono stati ancora recuperati.

L'obiettivo dell'amministratore è quello di tenere attivi gli indicatori a semaforo in tutti i riquadri informazioni nella scheda **Monitoraggio** verde.

I riquadri informazioni mostrano anche gli eventi registrati che interessano i semafori e lo stato di Kaspersky Security Center (vedere la tabella seguente).

Nome, descrizione e colori dei semafori degli eventi registrati

Colore dell'indicatore	Nome visualizzato del tipo di evento	Tipo di evento	Descrizione
Rosso	**Licenza scaduta in %1 dispositivi**	IDS_AK_STATUS_LIC_EXPAIRED	Eventi di questo tipo si verificano alla scadenza della licenza commerciale. Una volta al giorno, Kaspersky Security Center verifica se la licenza nei dispositivi è scaduta. Alla scadenza della licenza commerciale, Kaspersky Security Center fornisce solo le funzionalità di base. Per continuare a utilizzare Kaspersky Security Center, rinnovare la licenza commerciale.
Rosso	**Applicazione di protezione non in esecuzione in: %1 dispositivi**	IDS_AK_STATUS_AV_NOT_RUNNING	Eventi di questo tipo si verificano quando l'applicazione di protezione installata nel dispositivo non è in esecuzione. Verificare che Kaspersky Endpoint Security sia in esecuzione nel dispositivo.
Rosso	**Protezione disabilitata in: %1 dispositivi**	IDS_AK_STATUS_RTP_NOT_RUNNING	Eventi di questo tipo si verificano quando l'applicazione di protezione nel dispositivo è stata disabilitata per un periodo superiore all'intervallo di tempo specificato. Verificare lo stato corrente della protezione in tempo reale nel dispositivo e assicurarsi che tutti i componenti di protezione necessari siano abilitati.
Rosso	**Una vulnerabilità del software è stata rilevata nei dispositivi**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Eventi di questo tipo si verificano quando l'attività *Trova vulnerabilità e aggiornamenti richiesti* ha rilevato vulnerabilità con il livello di criticità specificato nelle applicazioni installate nel dispositivo. Verificare l'elenco degli aggiornamenti disponibili nella sottocartella **Aggiornamenti software** inclusa nella cartella **Gestione applicazioni**. Questa cartella contiene un elenco degli aggiornamenti per le applicazioni Microsoft e di altri fornitori di software recuperati da Administration Server che possono essere distribuiti ai dispositivi. Dopo aver visualizzato le informazioni sugli aggiornamenti disponibili, installarli nel dispositivo.
Rosso	**Eventi critici registrati in Administration Server**	IDS_AK_STATUS_EVENTS_OCCURED	Eventi di questo tipo si verificano quando vengono rilevati eventi critici di Administration Server. Verificare l'elenco degli eventi archiviati in Administration Server, quindi correggere singolarmente gli eventi critici.

Colore dell'indicatore	Nome visualizzato del tipo di evento	Tipo di evento	Descrizione
Rosso	**Sono stati registrati errori negli eventi in Administration Server**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Eventi di questo tipo si verificano quando vengono registrati errori imprevisti sul lato Administration Server. Verificare l'elenco degli eventi archiviati in Administration Server, quindi correggere singolarmente gli errori.
Rosso	**Connessione a %1 dispositivi interrotta**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Eventi di questo tipo si verificano quando si perde la connessione tra Administration Server e il dispositivo. Visualizzare l'elenco dei dispositivi disconnessi e provare a riconnetterli.
Rosso	**%1 dispositivi non si connettono ad Administration Server da molto tempo**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Eventi di questo tipo si verificano quando il dispositivo non viene connesso ad Administration Server nell'intervallo di tempo specificato, perché il dispositivo era spento. Verificare che il dispositivo sia acceso e che Network Agent sia in esecuzione.
Rosso	**Dispositivi con stato diverso da OK: %1**	IDS_AK_STATUS_HOST_NOT_OK	Eventi di questo tipo si verificano quando lo stato *OK* del dispositivo connesso ad Administration Server cambia in *Critico* o *Avviso*. È possibile risolvere il problema utilizzando l'utilità di diagnostica remota di Kaspersky Security Center.
Rosso	**Database non aggiornati in: %1 dispositivi**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Eventi di questo tipo si verificano quando i database anti-virus non sono stati aggiornati nel dispositivo nell'intervallo di tempo specificato. Seguire le istruzioni per aggiornare i database di Kaspersky.
Rosso	**Dispositivi in cui la verifica della disponibilità di aggiornamenti di Windows Update non viene eseguita da molto tempo: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Eventi di questo tipo si verificano quando l'attività *Esegui sincronizzazione di Windows Update* non viene eseguita nell'intervallo di tempo specificato. Seguire le istruzioni per sincronizzare gli aggiornamenti di Windows Update con Administration Server.
Rosso	**È necessario installare %1 plug-in per Kaspersky Security Center**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Eventi di questo tipo si verificano quando è necessario installare plug-in aggiuntivi per le applicazioni Kaspersky. Scaricare e installare i plug-in di gestione richiesti per l'applicazione Kaspersky dal sito Web del servizio di assistenza tecnica di Kaspersky.

Accesso remoto ai dispositivi gestiti

In questa sezione vengono fornite informazioni sull'accesso remoto ai dispositivi gestiti.

Utilizzo dell'opzione "Non eseguire la disconnessione da Administration Server" per garantire connettività continua tra un dispositivo gestito e Administration Server

Se non si utilizzano server push, Kaspersky Security Center non garantisce una connettività continua tra i dispositivi gestiti e Administration Server. I Network Agent nei dispositivi gestiti stabiliscono periodicamente connessioni ed eseguono la sincronizzazione con l'Administration Server. L'intervallo tra queste sessioni di sincronizzazione è definito in un criterio di Network Agent. Se è necessaria una sincronizzazione preventiva, Administration Server (o un punto di distribuzione, se in uso) invia un pacchetto di rete firmato tramite una rete IPv4 o IPv6 alla porta UDP di Network Agent. Il numero di porta predefinito è 15000. Se non è possibile stabilire la connessione tramite UDP tra Administration Server e un dispositivo gestito, la sincronizzazione verrà eseguita alla successiva connessione periodica di Network Agent ad Administration Server entro l'intervallo di sincronizzazione.

Alcune operazioni non possono essere eseguite senza una connessione preventiva tra Network Agent e Administration Server, come l'esecuzione e l'arresto di attività locali, la ricezione di statistiche per un'applicazione gestita o la creazione di un tunnel. Per risolvere il problema, se non si utilizzano server push è possibile utilizzare l'opzione **Non eseguire la disconnessione da Administration Server** per assicurarsi che vi sia connettività continua tra un dispositivo gestito e Administration Server.

Per garantire connettività continua tra un dispositivo gestito e Administration Server:

1. Nella struttura della console selezionare la cartella **Dispositivi gestiti**.
2. Nell'area di lavoro della cartella selezionare il dispositivo gestito con cui si desidera garantire connettività continua.
3. Nel menu di scelta rapida del dispositivo selezionare **Proprietà**.

   Verrà visualizzata la finestra delle proprietà del dispositivo selezionato.
4. Nella sezione **Generale** della finestra visualizzata selezionare l'opzione **Non eseguire la disconnessione da Administration Server**.

Viene stabilita la connettività continua tra il dispositivo gestito e Administration Server.

Il numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata è 300.

Informazioni sul controllo del tempo di connessione tra un dispositivo e Administration Server

Al momento dell'arresto di un dispositivo, Network Agent invia una notifica all'Administration Server di questo evento. In Administration Console il dispositivo è visualizzato come arrestato. Tuttavia, Network Agent non può notificare ad Administration Server tutti gli eventi di questo tipo. Administration Server, pertanto, analizza periodicamente l'attributo **Connesso ad Administration Server** (il valore di questo attributo è visualizzato in Administration Console, nella sezione **Generale** delle proprietà del dispositivo) per ogni dispositivo e lo confronta con l'intervallo di sincronizzazione nelle impostazioni correnti di Network Agent. Se un dispositivo non risponde per più di tre intervalli di sincronizzazione consecutivi, il dispositivo è contrassegnato come arrestato.

Informazioni sulla sincronizzazione forzata

Anche se Kaspersky Security Center sincronizza automaticamente lo stato, le impostazioni, le attività e i criteri per i dispositivi gestiti, in alcuni casi l'amministratore ha l'esigenza di sapere esattamente se la sincronizzazione è stata già eseguita per un determinato dispositivo.

Nel menu di scelta rapida dei dispositivi gestiti in Administration Console, la voce di menu **Tutte le attività** contiene il comando **Forza sincronizzazione**. Quando Kaspersky Security Center 15.1 esegue questo comando, Administration Server tenta di connettersi al dispositivo. Se questo tentativo va a buon fine viene eseguita la sincronizzazione forzata. In caso contrario, la sincronizzazione verrà forzata solo dopo la successiva connessione pianificata tra Network Agent e l'Administration Server.

Informazioni sul tunneling

Kaspersky Security Center consente il tunneling delle connessioni TCP da Administration Console tramite l'Administration Server e quindi tramite Network Agent su una porta specificata in un dispositivo gestito. Il tunneling è progettato per la connessione di un'applicazione client su un dispositivo con Administration Console installato a una porta TCP in un dispositivo gestito, se non è possibile la connessione diretta tra Administration Console e il dispositivo di destinazione.

Il tunneling viene ad esempio utilizzato per le connessioni a un desktop remoto, sia per connettersi a una sessione esistente che per creare una nuova sessione remota.

È anche possibile abilitare il tunneling utilizzando strumenti esterni. L'amministratore può ad esempio eseguire l'utilità putty, il client VNC e altri strumenti in questo modo.

Guida per il dimensionamento

Questa sezione fornisce informazioni sul dimensionamento di Kaspersky Security Center.

Informazioni sulla guida

La Guida per il dimensionamento di Kaspersky Security Center 15.1 (denominato anche Kaspersky Security Center) è destinata ai professionisti che si occupano dell'installazione e dell'amministrazione di Kaspersky Security Center, nonché a quelli che forniscono assistenza tecnica alle organizzazioni che utilizzano Kaspersky Security Center.

Tutti i suggerimenti e i calcoli vengono forniti per le reti in cui Kaspersky Security Center gestisce la protezione dei dispositivi in cui è installato il software Kaspersky, inclusi i dispositivi mobili. Se i dispositivi mobili o altri dispositivi gestiti devono essere considerati separatamente, viene indicato in modo specifico.

Per ottenere e mantenere prestazioni ottimali in diverse condizioni operative, è necessario tenere conto del numero di dispositivi in rete, della topologia della rete e del set di funzionalità di Kaspersky Security Center richiesto.

La presente Guida fornisce le seguenti informazioni:

- Limitazioni di Kaspersky Security Center
- Calcoli per i nodi chiave di Kaspersky Security Center (Administration Server e punti di distribuzione):
  - Requisiti hardware per Administration Server e punti di distribuzione
  - Calcolo del numero e gerarchia degli Administration Server
  - Calcolo del numero e configurazione dei punti di distribuzione
- Configurazione della registrazione degli eventi nel database in base al numero dei dispositivi in rete
- Best practice comuni per l'ottimizzazione delle prestazioni
- Configurazione di attività specifiche mirate alle prestazioni ottimali di Kaspersky Security Center
- Frequenza di traffico (carico di rete) tra Kaspersky Security Center Administration Server e ciascun dispositivo protetto

È consigliabile consultare questa guida nei seguenti casi:

- In caso di pianificazione delle risorse prima dell'installazione di Kaspersky Security Center
- In caso di pianificazione di cambiamenti significativi della portata della rete in cui viene distribuito Kaspersky Security Center
- In caso di passaggio dall'utilizzo di Kaspersky Security Center all'interno di un segmento di rete limitato (un ambiente di test) alla distribuzione su vasta scala di Kaspersky Security Center nella rete aziendale
- In caso di modifiche al set di funzionalità di Kaspersky Security Center utilizzate

Informazioni sulle limitazioni di Kaspersky Security Center

Nella seguente tabella sono riportate le limitazioni della versione corrente di Kaspersky Security Center.

Limitazioni di Kaspersky Security Center

Tipo di limitazione	Valore
Numero massimo di dispositivi gestiti per ogni Administration Server	100.000
Numero massimo di dispositivi con l'opzione **Non eseguire la disconnessione da Administration Server** selezionata	300
Numero massimo di gruppi di amministrazione	10.000
Numero massimo di eventi che è possibile memorizzare	45.000.000
Numero massimo di criteri	2000
Numero massimo di attività	2000
Numero massimo di oggetti Active Directory (unità organizzative, account utente, dispositivi e gruppi di protezione)	1.000.000
Numero massimo di profili in un criterio	100
Numero massimo di Administration Server secondari in un singolo Administration Server primario	500
Numero massimo di Administration Server virtuali	500
Numero massimo di dispositivi a cui può essere applicato un singolo punto di distribuzione (i punti di distribuzione sono applicabili solo ai dispositivi non mobili)	10.000
Numero massimo di dispositivi che possono utilizzare un singolo gateway di connessione	10.000, inclusi i dispositivi mobili
Numero massimo di dispositivi mobili per ogni Administration Server	100000 meno il numero di dispositivi gestiti fissi

Calcoli per gli Administration Server

In questa sezione vengono specificati i requisiti software e hardware per i dispositivi utilizzati come Administration Server. Vengono inoltre forniti suggerimenti per il calcolo del numero e della gerarchia di Administration Server in base alla configurazione della rete dell'organizzazione.

Calcolo delle risorse hardware per Administration Server

Questa sezione contiene i calcoli che forniscono istruzioni sulla pianificazione delle risorse hardware per Administration Server. Viene fornito separatamente un suggerimento sul calcolo dello spazio su disco quando si utilizza la funzionalità Vulnerability e patch management.

Requisiti hardware per il DBMS e l'Administration Server

Nelle seguenti tabelle sono riportati i requisiti hardware minimi consigliati per un DBMS e un Administration Server ottenuti durante i test. Per un elenco completo di sistemi operativi e DBMS supportati fare riferimento all'elenco dei requisiti hardware e software.

Administration Server e DBMS si trovano in dispositivi diversi, la rete include 50.000 dispositivi

Configurazione del dispositivo in cui è installato Administration Server

Hardware	Valore
CPU	4 core, 2500 MHz
RAM	8 GB
Disco rigido	300 GB, RAID consigliato
Scheda di rete	1 Gbit

Configurazione del dispositivo in cui è installato DBMS

Hardware	Valore
CPU	4 core, 2500 MHz
RAM	16 GB
Disco rigido	200 GB, RAID SATA
Scheda di rete	1 Gbit

Administration Server e DBMS si trovano nello stesso dispositivo, la rete include 50.000 dispositivi

Configurazione del dispositivo in cui sono installati Administration Server e DBMS

Hardware	Valore
CPU	8 core, 2500 MHz
RAM	16 GB
Disco rigido	500 GB, RAID SATA
Scheda di rete	1 Gbit

Administration Server e DBMS si trovano in dispositivi diversi, la rete include 100.000 dispositivi

Configurazione del dispositivo in cui è installato Administration Server

Hardware	Valore
CPU	8 core, 2,13 GHz
RAM	8 GB
Disco rigido	1 TB con RAID
Scheda di rete	1 Gbit

Configurazione del dispositivo in cui è installato DBMS

Hardware	Valore
CPU	8 core, 2,53 GHz
RAM	26 GB
Disco rigido	500 GB, RAID SATA
Scheda di rete	1 Gbit

I test sono stati eseguiti con le seguenti impostazioni:

- L'assegnazione automatica dei punti di distribuzione è abilitata in Administration Server oppure i punti di distribuzione vengono assegnati manualmente in base alle tabella consigliata.
- L'attività di backup salva le copie di backup in una risorsa file posizionata in un server dedicato.
- L'intervallo di sincronizzazione per i Network Agent è impostato come specificato nella tabella seguente.

Intervallo di sincronizzazione per i Network Agent

Intervallo di sincronizzazione (minuti)	Numero di dispositivi gestiti
15	10.000
30	20.000
45	30.000
60	40.000
75	50.000
150	100.000

Calcolo dello spazio del database

La quantità approssimativa di spazio che deve essere riservata nel database può essere calcolata utilizzando la seguente formula:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

dove:

- C è il numero dei dispositivi.
- E è il numero di eventi da memorizzare.
- A è il numero totale degli oggetti di Active Directory:
  - Account dispositivo
  - Account utente
  - Account dei gruppi di protezione
  - Unità organizzative di Active Directory

  Se la scansione di Active Directory è disabilitata, A è considerato uguale a zero.
- N è il numero medio di file eseguibili di cui è stato eseguito l'inventario in un dispositivo endpoint.
- F è il numero di dispositivi endpoint nei quali è stato eseguito l'inventario dei file eseguibili.

Se (nelle impostazioni dei criteri di Kaspersky Endpoint Security) si intende abilitare la notifica di Administration Server nelle applicazioni eseguite, è necessaria una quantità aggiuntiva di (0,03 * C) gigabyte per archiviare nel database le informazioni sulle applicazioni eseguite.

Se Administration Server distribuisce gli aggiornamenti di Windows (operando così come server Windows Server Update Services), il database richiederà altri 2,5 GB.

Durante l'esecuzione, nel database è sempre presente una determinata *quantità di spazio non allocato*. Di conseguenza, le dimensioni effettive del file di database (per impostazione predefinita, il file KAV.MDF se si utilizza SQL Server come DBMS) spesso si rivelano circa il doppio della quantità di spazio occupata nel database.

Non è consigliabile limitare in modo esplicito le dimensioni del log delle transazioni (per impostazione predefinita, il file KAV_log. LDF, se si utilizza SQL Server come DBMS). È consigliabile mantenere il valore predefinito del parametro MAXSIZE. Tuttavia, se è necessario limitare la dimensione del file, tenere in considerazione che il valore minimo desiderato tipico del parametro MAXSIZE per KAV_log.LDF è 20480 MB.

Calcolo dello spazio su disco (con e senza l'utilizzo della funzionalità Vulnerability e patch management)

Calcolo dello spazio su disco senza l'utilizzo della funzionalità Vulnerability e patch management

Lo spazio su disco di Administration Server richiesto per la cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit può essere stimato approssimativamente utilizzando la formula:

(724 * C + 0,15 * E + 0,17 * A) KB

dove:

- C è il numero dei dispositivi.
- E è il numero di eventi da memorizzare.
- A è il numero totale degli oggetti di Active Directory:
  - Account dispositivo
  - Account utente
  - Account dei gruppi di protezione
  - Unità organizzative di Active Directory

Se la scansione di Active Directory è disabilitata, A è considerato uguale a zero.

Calcolo dello spazio su disco aggiuntivo con l'utilizzo della funzionalità Vulnerability e patch management

- Aggiornamenti. La cartella condivisa richiede inoltre almeno 4 GB per l'archiviazione degli aggiornamenti.
- Pacchetti di installazione. Se in Administration Server sono archiviati pacchetti di installazione, la cartella condivisa richiederà una quantità aggiuntiva di spazio libero su disco, pari alle dimensioni totali di tutti i pacchetti di installazione disponibili da installare.

- Attività di installazione remota. Se in Administration Server sono presenti attività di installazione remota, sarà richiesta una quantità aggiuntiva di spazio libero su disco (nella cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit), pari alle dimensioni totali di tutti i pacchetti di installazione da installare.

- Patch. Se Administration Server viene utilizzato per l'installazione di patch, sarà richiesta una quantità aggiuntiva di spazio su disco:

  - La cartella delle patch deve disporre di una quantità di spazio su disco pari alle dimensioni totali di tutte le patch scaricate. Per impostazione predefinita, le patch vengono archiviate nella cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles.

    È possibile utilizzare l'utilità klsrvswch per specificare una cartella diversa in cui archiviare le patch. L'utilità klsrvswch si trova nella cartella in cui è installato Administration Server. Il percorso di installazione predefinito: <Disco>:\Programmi (x86)\ Kaspersky Lab\ Kaspersky Security Center.

    Se Administration Server viene utilizzato come server WSUS, è consigliabile allocare almeno 100 GB a questa cartella.

  - La cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit deve disporre di una quantità di spazio su disco pari alle dimensioni totali delle patch a cui fanno riferimento le istanze esistenti delle attività di installazione degli aggiornamenti (patch) e correzione delle vulnerabilità.

Calcolo del numero e configurazione degli Administration Server

Per ridurre il carico sull'Administration Server primario, è possibile assegnare un Administration Server separato a ciascun gruppo di amministrazione. Il numero di Administration Server secondari non può essere superiore a 500 per un singolo Administration Server primario.

È consigliabile creare la configurazione degli Administration Server in base alla configurazione della rete della propria organizzazione.

Suggerimenti per la connessione di macchine virtuali dinamiche a Kaspersky Security Center

Le macchine virtuali dinamiche (denominate anche VM dinamiche) consumano più risorse rispetto alle macchine virtuali statiche.

Per ulteriori informazioni sulle macchine virtuali dinamiche, vedere Supporto delle macchine virtuali dinamiche.

Quando viene connessa una nuova VM dinamica, Kaspersky Security Center crea un'icona per questa VM dinamica in Administration Console e sposta la VM dinamica nel gruppo di amministrazione. Successivamente, la VM dinamica viene aggiunta al database di Administration Server. Administration Server è completamente sincronizzato con Network Agent installato in questa VM dinamica.

Nella rete di un'organizzazione, Network Agent crea i seguenti elenchi di reti per ogni macchina virtuale dinamica:

- Hardware
- Software installato
- Vulnerabilità rilevate
- Eventi ed elenchi di file eseguibili del componente Controllo Applicazioni

Network Agent trasferisce questi elenchi di reti all'Administration Server. La dimensione degli elenchi di rete dipende dai componenti installati nella VM dinamica e può influire sulle prestazioni di Kaspersky Security Center e il sistema di gestione database (DBMS). Si noti che il carico può crescere in modo non lineare.

Dopo che l'utente ha terminato di utilizzare la macchina virtuale dinamica e l'ha spenta, quest'ultima viene quindi rimossa dall'infrastruttura virtuale e le voci relative a questa macchina vengono rimosse dal database di Administration Server.

Tutte queste azioni consumano molte risorse del database di Kaspersky Security Center e Administration Server e possono ridurre le prestazioni di Kaspersky Security Center e DBMS. Si consiglia di connettere fino a 20.000 macchine virtuali dinamiche a Kaspersky Security Center.

È possibile connettere più di 20.000 VM dinamiche a Kaspersky Security Center se le VM dinamiche connesse eseguono operazioni standard (ad esempio, aggiornamenti del database) e consumano non più dell'80% della memoria e del 75-80% dei core disponibili.

La modifica delle impostazioni dei criteri, del software o del sistema operativo sulla VM dinamica può ridurre o aumentare il consumo di risorse. Il consumo dell'80-95% delle risorse è considerato ottimale.

Calcoli per punti di distribuzione e gateway di connessione

Questa sezione fornisce i requisiti hardware per i dispositivi utilizzati come punti di distribuzione insieme ai suggerimenti per il calcolo del numero di punti di distribuzione e di gateway di connessione in base alla configurazione della rete aziendale.

Requisiti per un punto di distribuzione

Per gestire fino a 10.000 dispositivi client, un punto di distribuzione deve soddisfare almeno i seguenti requisiti (è disponibile una configurazione per un'esecuzione di test):

- CPU: Intel® Core™ i7-7700 CPU, 3,60 GHz 4 core.
- RAM: 8 GB.
- Spazio di archiviazione gratuito: 120 GB.

Si sconsiglia di assegnare l'Administration Server come punto di distribuzione, poiché ciò aumenterà il carico sull'Administration Server.

Se in Administration Server è presente un'attività di installazione remota in sospeso, il dispositivo con il punto di distribuzione richiederà inoltre una quantità di spazio disponibile sul disco pari alle dimensioni totali dei pacchetti di installazione da installare.

Se in Administration Server sono presenti una o più istanze in sospeso delle attività di installazione degli aggiornamenti (patch) e di correzione delle vulnerabilità, il dispositivo con il punto di distribuzione richiederà ulteriore spazio disponibile sul disco, una quantità pari al doppio delle dimensioni totali di tutte le patch da installare.

Se si utilizza lo schema in cui i punti di distribuzione ricevono gli aggiornamenti dei database e dei moduli del software applicativo direttamente dai server di aggiornamento Kaspersky, i punti di distribuzione devono essere connessi a Internet.

Calcolo del numero e configurazione dei punti di distribuzione

Più dispositivi client contiene una rete, maggiore è il numero dei punti di distribuzione richiesti. È consigliabile non disabilitare l'assegnazione automatica dei punti di distribuzione. Quando è abilitata l'assegnazione automatica dei punti di distribuzione, Administration Server assegna i punti di distribuzione se il numero dei dispositivi client è ampio e definisce la configurazione.

Utilizzo di punti di distribuzione assegnati in modo esclusivo

Se si prevede di utilizzare alcuni dispositivi specifici come punti di distribuzione (ovvero, server assegnati in modo esclusivo), è possibile scegliere di non utilizzare l'assegnazione automatica dei punti di distribuzione. In questo caso, verificare che i dispositivi a cui assegnare il ruolo di punti di distribuzione dispongano di un volume sufficiente di spazio libero su disco, che non vengano arrestati regolarmente e che la modalità di sospensione sia disabilitata.

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Numero di punti di distribuzione assegnati in modo esclusivo in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–100	1
Più di 100	Accettabile: (N/10.000 + 1), consigliato: (N/5.000 + 2), dove N è il numero di dispositivi nella rete

Utilizzo di dispositivi client standard (workstation) come punti di distribuzione

Se si prevede di utilizzare dispositivi client standard (ovvero, workstation) come punti di distribuzione, è consigliabile assegnare i punti di distribuzione come indicato nelle tabelle seguenti per evitare un carico eccessivo sui canali di comunicazione e su Administration Server:

Numero di workstation che operano come punti di distribuzione in una rete che contiene un solo segmento di rete, in base al numero di dispositivi di rete

Numero di dispositivi client nel segmento di rete	Numero di punti di distribuzione
Minore di 300	0 (non assegnare punti di distribuzione)
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Numero di workstation che operano come punti di distribuzione in una rete che contiene più segmenti di rete, in base al numero di dispositivi di rete

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
Minore di 10	0 (non assegnare punti di distribuzione)
10–30	1

Numero di dispositivi client per segmento di rete	Numero di punti di distribuzione
31–300	2
Più di 300	(N/300 + 1), dove N è il numero dei dispositivi nella rete; devono essere presenti almeno 3 punti di distribuzione

Se un punto di distribuzione viene arrestato (o non è disponibile per altri motivi), i dispositivi gestiti nel relativo ambito possono accedere ad Administration Server per gli aggiornamenti.

Calcolo del numero di gateway di connessione

Se si prevede di utilizzare un gateway di connessione, è consigliabile specificare un dispositivo specifico per questa funzione.

Un gateway di connessione può coprire un massimo di 10.000 dispositivi gestiti, inclusi i dispositivi mobili.

Registrazione delle informazioni sugli eventi per le attività e i criteri

Questa sezione contiene i calcoli associati all'archiviazione degli eventi nel database di Administration Server e offre suggerimenti su come ridurre al minimo il numero di eventi, riducendo quindi il carico su Administration Server.

Per impostazione predefinita, le proprietà di ogni attività e criterio consentono l'archiviazione di tutti gli eventi relativi all'esecuzione delle attività e all'applicazione dei criteri.

Tuttavia, se un'attività viene eseguita con una frequenza elevata (ad esempio più di una volta a settimana) e su un ampio numero di dispositivi (ad esempio più di 10.000), il numero di eventi può rivelarsi troppo ampio e gli eventi possono riempire eccessivamente il database. In questo caso è consigliabile selezionare una delle due opzioni nelle impostazioni dell'attività:

- **Salva eventi correlati all'avanzamento dell'attività**. In questo caso il database riceve solo le informazioni sull'avvio, sull'andamento e sul completamento dell'attività (completa, con avviso o con errore) da ciascun dispositivo in cui viene eseguita l'attività.

- **Salva solo i risultati dell'esecuzione dell'attività**. In questo caso il database riceve solo le informazioni sul completamento delle attività (completa, con avviso o con errore) da ciascun dispositivo in cui viene eseguita l'attività.

Se è stato definito un criterio per un ampio numero di dispositivi (ad esempio più di 10.000), il numero di eventi può anche rivelarsi troppo ampio e gli eventi possono riempire eccessivamente il database. In questo caso è consigliabile scegliere solo gli eventi più critici nelle impostazioni del criterio e abilitare la relativa registrazione. È consigliabile disabilitare la registrazione di tutti gli altri eventi.

In tal modo si riduce il numero di eventi nel database, si aumenta la velocità di esecuzione degli scenari associati all'analisi della tabella degli eventi nel database e si limita il rischio che gli eventi critici vengano sovrascritti da un ampio numero di eventi.

È anche possibile ridurre il periodo di archiviazione per gli eventi associati a un'attività o a un criterio. Il periodo predefinito è di 7 giorni per gli eventi correlati alle attività e di 30 giorni per gli eventi correlati ai criteri. Quando si modifica il periodo di archiviazione di un evento è opportuno prendere in considerazione le procedure operative in atto nell'organizzazione e la quantità di tempo che l'amministratore di sistema può dedicare all'analisi di ciascun evento.

È consigliabile modificare le impostazioni di archiviazione degli eventi in uno dei seguenti casi:

- Gli eventi riguardanti modifiche degli stati intermedi delle attività di gruppo e gli eventi correlati all'applicazione dei criteri occupano un'ampia quota del totale degli eventi nel database di Kaspersky Security Center.
- Il registro eventi Kaspersky inizia a mostrare le voci relative alla rimozione automatica degli eventi quando viene superato il limite stabilito sul numero totale di eventi archiviati nel database.

Scegliere le opzioni di registrazione degli eventi partendo dal presupposto che il numero ottimale di eventi che derivano da un singolo dispositivo in un giorno non deve essere superiore a 20. È possibile aumentare leggermente questo limite, se necessario, ma solo se il numero di dispositivi nella rete è relativamente piccolo (inferiore a 10.000).

Considerazioni specifiche e impostazioni ottimali di determinate attività

Determinate attività sono soggette a considerazioni specifiche relative al numero di dispositivi di rete. Questa sezione offre suggerimenti sulla configurazione ottimale delle impostazioni per tali attività.

Device discovery, attività di backup dei dati, attività di manutenzione di Administration Server e attività di gruppo per aggiornare Kaspersky Endpoint Security fanno parte della funzionalità di base di Kaspersky Security Center.

Frequenza della device discovery

Non è consigliabile aumentare la frequenza predefinita della device discovery poiché ciò può creare un carico eccessivo nei controller di dominio. È invece consigliabile pianificare il polling con la frequenza minima consentita dalle esigenze dell'organizzazione. Nella tabella di seguito vengono forniti i suggerimenti per il calcolo della pianificazione ottimale.

Pianificazione della device discovery

Numero di dispositivi nella rete	Frequenza consigliata per la device discovery
Minore di 10.000	Frequenza predefinita o inferiore
10.000 o superiore	Una volta al giorno o inferiore

Attività di backup dei dati di Administration Server e attività di manutenzione di Administration Server

Administration Server smette di funzionare quando sono in esecuzione le seguenti attività:

- Backup dei dati di Administration Server
- Manutenzione di Administration Server

Quando queste attività sono in esecuzione, il database non può ricevere alcun dato.

Potrebbe essere necessario ripianificare queste attività in modo che non vengano eseguite contemporaneamente ad altre attività di Administration Server.

Attività di gruppo per l'aggiornamento di Kaspersky Endpoint Security

Se Administration Server opera come sorgente degli aggiornamenti, l'opzione di pianificazione consigliata per le attività di aggiornamento di gruppo di Kaspersky Endpoint Security 10 e versioni successive è **Quando vengono scaricati nuovi aggiornamenti nell'archivio** con la casella di controllo **Usa automaticamente il ritardo casuale per l'avvio delle attività** selezionata.

Se si crea un'attività locale di download degli aggiornamenti dai server Kaspersky nell'archivio in ogni punto di distribuzione, la pianificazione periodica è consigliata per l'attività di aggiornamento di gruppo di Kaspersky Endpoint Security. In questo caso il valore del periodo con impostazione casuale deve essere di un'ora.

Attività di inventario

È possibile ridurre il carico sul database mentre si ottengono informazioni sui file eseguibili. A tale scopo, si consiglia di eseguire un'attività di inventario per Kaspersky Endpoint Security sui dispositivi di riferimento in cui è installato un set standard di software.

Il numero di file eseguibili ricevuti da Administration Server da un singolo dispositivo non può essere superiore a 150.000. Quando Kaspersky Security Center raggiunge questo limite, non può ricevere nuovi file.

In genere, il numero di file in un dispositivo client comune non può essere superiore a 60.000. Il numero di file eseguibili in un file server può essere maggiore e può addirittura superare la soglia di 150.000.

Le misurazioni di prova hanno dimostrato che l'attività dell'inventario dispone dei seguenti risultati in un dispositivo che esegue il sistema operativo Windows 7 in cui è installato Kaspersky Endpoint Security 11 e nessun'applicazione di terze parti:

- Con le caselle di controllo **Inventario dei moduli DLL** e **Inventario dei file di script** deselezionate: circa 3000 file.
- Con le caselle di controllo **Inventario dei moduli DLL** e **Inventario dei file di script** selezionate: da 10.000 a 20.000 file, a seconda del numero di service pack del sistema operativo installati.
- Con solo la casella di controllo **Inventario dei file di script** selezionata: circa 10.000 file.

Dettagli del carico di rete trasmesso fra Administration Server e dispositivi protetti

Questa sezione fornisce i risultati delle misurazioni di prova del traffico di rete con una descrizione delle condizioni di esecuzione delle misurazioni. È possibile fare riferimento a queste informazioni quando si pianifica l'infrastruttura di rete e la capacità di throughput dei canali di rete all'interno dell'organizzazione (o tra Administration Server e un'altra organizzazione con i dispositivi da proteggere). Conoscendo la capacità di throughput della rete, è inoltre possibile stimare approssimativamente il tempo richiesto dalle diverse operazioni di trasmissione dei dati.

Consumo del traffico in diversi scenari

La tabella di seguito consente di visualizzare i risultati dei test di misurazione condotti sul traffico tra Administration Server e un dispositivo gestito in scenari diversi.

Per impostazione predefinita, i dispositivi vengono sincronizzati con Administration Server ogni 15 minuti o con un intervallo più lungo. Tuttavia, se si modificano le impostazioni di un criterio o di un'attività in Administration Server, si verifica una sincronizzazione anticipata nei dispositivi a cui è applicabile il criterio (o l'attività), pertanto le nuove impostazioni vengono trasmesse ai dispositivi.

Frequenza di traffico tra Administration Server e un dispositivo gestito

Scenario	Traffico da Administration Server a ciascun dispositivo gestito	Traffico da ciascun dispositivo gestito ad Administration Server
Installazione di Kaspersky Endpoint Security 11.7 for Windows con database aggiornati	390 MB	3,3 MB
Installazione di Network Agent	75 MB	397 KB
Installazione simultanea di Network Agent e Kaspersky Endpoint Security 11.7 for Windows	459 MB	3.6 MB
Aggiornamento iniziale dei database anti-virus senza aggiornare i database nel pacchetto (se la partecipazione a Kaspersky Security Network è disabilitata)	113 MB	1,8 MB
Aggiornamento giornaliero dei database anti-virus (se la partecipazione a Kaspersky Security Network è abilitata)	22 MB	373 MB
Sincronizzazione iniziale prima dell'aggiornamento dei database in un dispositivo (trasferimento di criteri e attività)	382 KB	446 KB
Sincronizzazione iniziale dopo l'aggiornamento dei database in un dispositivo	20 KB	157 KB

Scenario	Traffico da Administration Server a ciascun dispositivo gestito	Traffico da ciascun dispositivo gestito ad Administration Server
Sincronizzazione senza modifiche in Administration Server (in base a una pianificazione)	18 KB	23 KB
Sincronizzazione quando una singola impostazione in un criterio di gruppo viene modificata (non appena l'impostazione viene modificata)	19 KB	20 KB
Sincronizzazione quando una singola impostazione in un'attività di gruppo viene modificata (non appena l'impostazione viene modificata)	14 KB	11 KB
Sincronizzazione forzata	110 KB	109 KB
Evento **Virus rilevato** (1 virus)	44 KB	50 KB
Evento **Virus rilevato** (10 virus)	58 KB	77 KB
Traffico occasionale dopo l'abilitazione dell'elenco Registro delle applicazioni	fino a 10 KB	fino a 12 KB
Traffico giornaliero quando è abilitato l'elenco Registro delle applicazioni	fino a 840 KB	fino a 1 MB

Utilizzo del traffico medio nell'arco di 24 ore

L'utilizzo medio del traffico tra Administration Server e un dispositivo gestito nell'arco di 24 ore è il seguente:

- Il traffico da Administration Server al dispositivo gestito è di 840 KB.
- Il traffico dal dispositivo gestito ad Administration Server è di 1 MB.

Il traffico è stato calcolato nell'ambito delle seguenti condizioni:

- Nel dispositivo gestito erano installati Network Agent e Kaspersky Endpoint Security 11.6 for Windows.
- Al dispositivo non era assegnato un punto di distribuzione.
- Vulnerability e patch management non era abilitata.
- La frequenza di sincronizzazione con Administration Server era di 15 minuti.

Contatta Assistenza tecnica

Questa sezione descrive i modi e le condizioni per ottenere assistenza tecnica.

Come ottenere assistenza tecnica

Se non è possibile trovare una soluzione per il proprio problema nella documentazione di Kaspersky Security Center o in una delle fonti di informazioni su Kaspersky Security Center, contattare il Servizio di assistenza tecnica Kaspersky. Gli specialisti del Servizio di assistenza tecnica risponderanno a tutte le domande relative all'installazione e all'utilizzo di Kaspersky Security Center.

> Kaspersky garantisce il supporto di Kaspersky Security Center durante il ciclo di vita (vedere la pagina del ciclo di vita di supporto dell'applicazione). Prima di contattare il Servizio di assistenza tecnica, consultare le regole dell'assistenza.

È possibile contattare il Servizio di assistenza tecnica in uno dei seguenti modi:

- Visitando il sito Web del Servizio di assistenza tecnica
- Inviando una richiesta al Servizio di assistenza tecnica dal portale Kaspersky CompanyAccount

Assistenza tecnica tramite Kaspersky CompanyAccount

Kaspersky CompanyAccount è un portale per le aziende che utilizzano le applicazioni Kaspersky. Il portale Kaspersky CompanyAccount è progettato per facilitare l'interazione tra gli utenti e gli esperti di Kaspersky tramite richieste online. È possibile utilizzare Kaspersky CompanyAccount per tenere traccia dello stato delle proprie richieste online e visualizzarne la cronologia.

È possibile registrare tutti i dipendenti dell'organizzazione in un singolo account su Kaspersky CompanyAccount. Un singolo account consente di gestire in modo centralizzato le richieste online inviate a Kaspersky dai dipendenti registrati e di gestire i privilegi dei dipendenti tramite Kaspersky CompanyAccount.

Il portale Kaspersky CompanyAccount è disponibile nelle seguenti lingue:

- Inglese
- Spagnolo
- Italiano
- Tedesco
- Polacco
- Portoghese

- Russo
- Francese
- Giapponese

Per ulteriori informazioni su Kaspersky CompanyAccount, visitare il sito Web del Servizio di assistenza tecnica.

Recupero dei file di dump di Administration Server

I file di dump di Administration Server contengono tutte le informazioni sui processi di Administration Server in un determinato momento. I file di dump di Administration Server sono archiviati nella cartella %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps. I file di dump vengono archiviati finché Kaspersky Security Center è in uso e vengono eliminati definitivamente quando viene rimosso. I file di dump non vengono trasferiti automaticamente a Kaspersky.

In caso di arresto anomalo di Administration Server, è possibile contattare l'Assistenza tecnica di Kaspersky. Uno specialista dell'Assistenza tecnica può richiedere di inviare i file di dump di Administration Server per ulteriori analisi a Kaspersky.

I file di dump possono contenere dati personali. Si consiglia di proteggere le informazioni dall'accesso non autorizzato prima di inviarle a Kaspersky.

Fonti di informazioni sull'applicazione

Pagina di Kaspersky Security Center nel sito Web di Kaspersky

Nella pagina di Kaspersky Security Center nel sito Web di Kaspersky sono disponibili informazioni generali sull'applicazione e le relative funzionalità e caratteristiche.

Pagina di Kaspersky Security Center nella Knowledge Base

La *Knowledge Base* è una sezione del sito Web del Servizio di assistenza tecnica di Kaspersky.

Nella pagina di Kaspersky Security Center nella Knowledge Base è possibile leggere articoli che forniscono informazioni utili, raccomandazioni e risposte alle domande frequenti su come acquistare, installare e utilizzare l'applicazione.

Gli articoli nella Knowledge Base possono fornire risposte a domande relative sia a Kaspersky Security Center che ad altre applicazioni Kaspersky. Gli articoli nella Knowledge Base possono anche contenere notizie dal Servizio di assistenza tecnica.

Discutere delle applicazioni Kaspersky con la community

Se la domanda non richiede una risposta immediata, è possibile sottoporla agli esperti di Kaspersky e ad altri utenti nel nostro Forum.

Nel Forum, è possibile visualizzare gli argomenti di discussione, pubblicare i propri commenti e creare nuovi argomenti di discussione.

> Per accedere alle risorse del sito Web, è necessaria una connessione a Internet.

Se non è possibile trovare una soluzione al problema, contattare il Servizio di assistenza tecnica.

Glossario

Administration Console

Un componente di Kaspersky Security Center basato su Windows (denominato anche Administration Console basata su MMC). Questo componente offre un'interfaccia utente per i servizi di amministrazione di Administration Server e Network Agent.

Administration Server

Un componente di Kaspersky Security Center che archivia in modo centralizzato le informazioni su tutte le applicazioni Kaspersky installate nella rete aziendale. È inoltre possibile utilizzarlo per la gestione di tali applicazioni.

Administration Server principale

Per Administration Server principale si intende l'Administration Server che è stato specificato durante l'installazione di Network Agent. L'Administration Server principale può essere utilizzato nelle impostazioni dei profili di connessione di Network Agent.

Administration Server virtuale

Componente di Kaspersky Security Center progettato per la gestione del sistema di protezione della rete di un'organizzazione client.

Un Administration Server virtuale è un particolare tipo di Administration Server secondario e presenta le seguenti limitazioni rispetto a un Administration Server fisico:

- Un Administration Server virtuale può essere creato solo in un Administration Server primario.
- L'Administration Server virtuale utilizza il database dell'Administration Server primario durante il relativo funzionamento. Le attività di backup e ripristino dei dati, nonché le attività di scansione e download degli aggiornamenti, non sono supportate in un Administration Server virtuale.
- Un server virtuale non supporta la creazione di Administration Server secondari (inclusi server virtuali).

Agente di Autenticazione

Interfaccia che consente di completare l'autenticazione per l'accesso ai dischi rigidi criptati e il caricamento del sistema operativo dopo il criptaggio del disco rigido avviabile.

Aggiorna

Procedura di sostituzione o aggiunta di nuovi file (database o moduli dell'applicazione) recuperati dai server degli aggiornamenti di Kaspersky.

Aggiornamento disponibile

Un set di aggiornamenti per i moduli dell'applicazione Kaspersky, inclusi gli aggiornamenti critici accumulati in un determinato periodo di tempo e modifiche all'architettura dell'applicazione.

Amazon Machine Image (AMI)

Modello contenente la configurazione software necessaria per eseguire la macchina virtuale. È possibile creare più istanze in base a una singola AMI.

Ambiente cloud

Macchine virtuali e altre risorse virtuali basate su una piattaforma cloud e combinate in reti.

Amministratore client

Membro dello staff di un'organizzazione client responsabile del monitoraggio dello stato della protezione anti-virus.

Amministratore del provider di servizi

Membro dello staff di un provider di servizi di protezione anti-virus. Questo amministratore esegue i processi di installazione e manutenzione per i sistemi di protezione anti-virus basati sui prodotti Kaspersky, oltre a fornire assistenza tecnica ai clienti.

Amministratore di Kaspersky Security Center

La persona che gestisce le operazioni dell'applicazione tramite il sistema centralizzato di amministrazione remota Kaspersky Security Center.

API (Application Programming Interface) AWS

L'API della piattaforma AWS utilizzata da Kaspersky Security Center. In particolare, gli strumenti API AWS vengono utilizzati per il polling dei segmenti cloud e l'installazione di Network Agent nelle istanze.

Applicazione incompatibile

Un'applicazione anti-virus di uno sviluppatore di terze parti o un'applicazione Kaspersky che non supporta la gestione tramite Kaspersky Security Center.

Archivio eventi

Una parte del database di Administration Server dedicato all'archiviazione delle informazioni sugli eventi che si verificano in Kaspersky Security Center.

Attacco MITM

Man in The Middle. Un attacco all'infrastruttura IT di un'organizzazione in cui un hacker dirotta il collegamento di comunicazione tra due punti di accesso, lo inoltra e modifica la connessione tra questi punti di accesso, se necessario.

Attività

Le funzioni eseguite dall'applicazione Kaspersky sono implementate come attività, ad esempio Protezione in tempo reale, Scansione completa del computer e Aggiornamento database.

Attività di gruppo

Un'attività definita per un gruppo di amministrazione ed eseguita in tutti i dispositivi client inclusi nel gruppo di amministrazione.

Attività locale

Attività definita e in esecuzione in un singolo computer client.

Attività per dispositivi specifici

Attività assegnata a un set di dispositivi client appartenenti a gruppi di amministrazione arbitrari ed eseguita su tali dispositivi.

Backup dei dati di Administration Server

Copia dei dati di Administration Server per il backup e il successivo ripristino eseguita tramite l'utilità di backup. L'utilità consente di salvare:

- Database di Administration Server (criteri, attività, impostazioni delle applicazioni, eventi salvati in Administration Server)
- Informazioni sulla configurazione della struttura dei gruppi di amministrazione e dei dispositivi client
- Archivio dei file di installazione per l'installazione remota delle applicazioni (contenuto delle cartelle: Pacchetti, Disinstallazione e Aggiornamenti)
- Certificato di Administration Server

Cartella di backup

Speciale cartella per la memorizzazione delle copie dei dati di Administration Server create tramite l'utilità di backup.

Certificato condiviso

Certificato che consente di identificare il dispositivo mobile dell'utente.

Certificato di Administration Server

Il certificato utilizzato da Administration Server per i seguenti scopi:

- Autenticazione di Administration Server durante la connessione ad Administration Console basato su MMC o Kaspersky Security Center Web Console
- Interazione sicura tra Administration Server e Network Agent nei dispositivi gestiti
- Autenticazione degli Administration Server durante la connessione di un Administration Server primario a un Administration Server secondario

Il certificato viene creato automaticamente quando si installa Administration Server e quindi archiviato in Administration Server.

Chiave attiva

Chiave attualmente utilizzata dall'applicazione.

Chiave di accesso AWS IAM

Una combinazione che comprende l'ID della chiave (con un aspetto simile a "AKIAIOSFODNN7EXAMPLE") e la chiave segreta (con un aspetto simile a "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Questa coppia appartiene all'utente IAM e viene utilizzata per ottenere l'accesso ai servizi AWS.

Chiave di licenza aggiuntiva (o di riserva)

Una chiave che convalida il diritto di utilizzo dell'applicazione, ma non è attualmente utilizzata.

Client di Administration Server (dispositivo client)

Dispositivo, server o workstation in cui è installato Network Agent e sono in esecuzione le applicazioni Kaspersky gestite.

Cloud Discovery

Cloud Discovery è un componente della soluzione Cloud Access Security Broker (CASB) che protegge l'infrastruttura cloud di un'organizzazione. Cloud Discovery gestisce l'accesso degli utenti ai servizi cloud. I servizi cloud includono, ad esempio, Microsoft Teams, Salesforce e Microsoft Office 365. I servizi cloud sono raggruppati in categorie, ad esempio *Scambio dati*, *Messenger*, *E-mail*.

Console di gestione AWS

Interfaccia Web per la visualizzazione e la gestione delle risorse AWS. La console di gestione AWS è disponibile sul Web all'indirizzo https://aws.amazon.com/it/console/

Criterio

Un criterio determina le impostazioni di un'applicazione e gestisce la capacità di configurare tale applicazione nei computer all'interno di un gruppo di amministrazione. Per ogni applicazione è necessario creare un criterio individuale. È possibile creare più criteri per le applicazioni installate nei computer di ciascun gruppo di amministrazione, ma a ogni applicazione è possibile applicare un solo criterio per volta all'interno di un gruppo di amministrazione.

Database anti-virus

Database che contengono informazioni sulle minacce per la protezione del computer note a Kaspersky al momento del rilascio dei database anti-virus. Le voci contenute nei database anti-virus consentono il rilevamento del codice dannoso negli oggetti esaminati. I database anti-virus sono creati dagli specialisti di Kaspersky e vengono aggiornati ogni ora.

Diritti di amministratore

Livello di diritti e privilegi dell'utente necessari per l'amministrazione di oggetti Exchange all'interno di un'organizzazione Exchange.

Dispositivi gestiti

Dispositivi della rete aziendale inclusi in un gruppo di amministrazione.

Dispositivo di protezione UEFI

Dispositivo con soluzione Kaspersky o applicazione per UEFI integrata a livello di BIOS. La protezione integrata garantisce la sicurezza del dispositivo fin dall'avvio del sistema, mentre la protezione nei dispositivi senza software integrato inizia solo dopo l'avvio dell'applicazione di protezione.

Dispositivo KES

Un dispositivo mobile connesso a Kaspersky Security Center Administration Server e gestito tramite l'app Kaspersky Endpoint Security for Android.

Dispositivo MDM iOS

Un dispositivo mobile connesso al server MDM iOS tramite il protocollo MDM iOS. I dispositivi con sistema operativo iOS possono essere connessi e gestiti tramite il protocollo MDM iOS.

Dominio di trasmissione

Un'area logica di una rete in cui tutti i nodi possono scambiare dati utilizzando un canale di trasmissione al livello OSI (Open Systems Interconnection Basic Reference Model).

Epidemia di virus

Una serie di tentativi intenzionali di infettare un dispositivo con un virus.

File chiave

Un file nel formato xxxxxxxx.key che consente l'utilizzo di un'applicazione Kaspersky in base ai termini della licenza commerciale o di prova.

Finestra Kaspersky Security Network (KSN)

Un'infrastruttura di servizi cloud che consente di accedere al database di Kaspersky, con informazioni sempre aggiornate sulla reputazione di file, risorse Web e software. Kaspersky Security Network assicura una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora l'efficacia di alcuni componenti della protezione e riduce la probabilità di falsi positivi.

Gateway di connessione

Un *gateway di connessione* è un Network Agent che funziona in modalità speciale. Un gateway di connessione accetta le connessioni da altri Network Agent e le trasmette ad Administration Server tramite la propria connessione con il server. A differenza di un normale Network Agent, un gateway di connessione attende le connessioni da Administration Server anziché stabilire connessioni ad Administration Server.

Gestione centralizzata delle applicazioni

Gestione remota delle applicazioni tramite i servizi di amministrazione forniti da Kaspersky Security Center.

Gestione diretta delle applicazioni

Gestione applicazioni tramite un'interfaccia locale.

Gruppo di amministrazione

Un set di dispositivi raggruppati in base alla funzione e alle applicazioni Kaspersky installate. I dispositivi sono raggruppati come una singola entità per semplificare la gestione. Un gruppo può includere altri gruppi. È possibile creare criteri di gruppo e attività di gruppo per ogni applicazione installata nel gruppo.

Gruppo di applicazioni concesse in licenza

Gruppo di applicazioni creato in base ai criteri impostati dall'amministratore (ad esempio, per produttore), per cui vengono registrate statistiche sulle installazioni nei dispositivi client.

Guida all'hardening

Una serie di suggerimenti e caratteristiche per la configurazione di Kaspersky Security Center e dei suoi componenti, intesi a ridurre i rischi di compromissione.

HTTPS

Protocollo sicuro per il trasferimento dei dati tramite criptaggio tra un browser e un server Web. HTTPS viene utilizzato per ottenere l'accesso a informazioni con restrizioni, quali dati aziendali o finanziari.

IAM (Identity and Access Management)

Il servizio AWS che consente la gestione dell'accesso degli utenti ad altri servizi e risorse AWS.

Impostazioni attività

Impostazioni dell'applicazione specifiche per ogni tipo di attività.

Impostazioni del programma

Impostazioni dell'applicazione comuni a tutti i tipi di attività e che determinano il funzionamento generale dell'applicazione, ad esempio: impostazioni relative alle prestazioni dell'applicazione, impostazioni dei rapporti e impostazioni di backup.

Installazione forzata

Metodo per l'installazione remota delle applicazioni Kaspersky che consente di installare il software in dispositivi client specifici. Per la corretta esecuzione dell'installazione forzata, l'account utilizzato per l'attività deve disporre di diritti sufficienti per l'avvio remoto delle applicazioni nei dispositivi client. Questo metodo è consigliato per l'installazione delle applicazioni nei dispositivi che eseguono i sistemi operativi Microsoft Windows e supportano questa funzionalità.

Installazione locale

Installazione di un'applicazione di protezione in un dispositivo di una rete aziendale che presuppone l'avvio manuale dell'installazione dal pacchetto di distribuzione dell'applicazione di protezione o l'avvio manuale di un pacchetto di installazione pubblicato che è stato scaricato preventivamente nel dispositivo.

Installazione manuale

Installazione di un'applicazione di protezione in un dispositivo della rete aziendale dal pacchetto di distribuzione. L'installazione manuale richiede il coinvolgimento di un amministratore o di un altro specialista IT. In genere l'installazione manuale viene eseguita se l'installazione remota è stata completata con un errore.

Installazione remota

Installazione delle applicazioni Kaspersky utilizzando i servizi offerti da Kaspersky Security Center.

Istanza Amazon EC2

Una macchina virtuale creata in base a un'immagine AMI utilizzando Amazon Web Services.

JavaScript

Linguaggio di programmazione che estende le prestazioni delle pagine Web. Le pagine Web create tramite JavaScript possono eseguire funzioni (ad esempio, modificare la visualizzazione di elementi di interfaccia o aprire ulteriori finestre) senza aggiornare la pagina Web con nuovi dati dal server Web. Per visualizzare le pagine create utilizzando JavaScript, abilitare il supporto per JavaScript nella configurazione del browser.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network è una soluzione che consente agli utenti dei dispositivi in cui sono installate le applicazioni Kaspersky di accedere ai database di reputazione di Kaspersky Security Network e ad altri dati statistici senza inviare dati dai propri dispositivi a Kaspersky Security Network. Kaspersky Private Security Network è progettato per i clienti aziendali che non sono in grado di partecipare al programma Kaspersky Security Network per uno dei seguenti motivi:

- I dispositivi non sono connessi a Internet.
- La trasmissione dei dati all'esterno del paese o della rete LAN aziendale è vietata dalla legge o dai criteri di protezione aziendali.

Kaspersky Security Center System Health Validator (SHV)

Un componente Kaspersky Security Center utilizzato per la verifica della possibilità di utilizzare il sistema operativo in caso siano in esecuzione contemporaneamente Kaspersky Security Center e Microsoft NAP.

Lightweight Nagent (LWNGT)

Un protocollo per l'interazione con Kaspersky Endpoint Security sui dispositivi mobili. Il protocollo LWNGT (chiamato anche protocollo Mobile) funziona come Network Agent senza dover effettivamente installare il programma di installazione di Network Agent sui dispositivi mobili.

Livello di criticità di un evento

Una proprietà di un evento verificatosi durante l'esecuzione di un'applicazione Kaspersky. Esistono i seguenti livelli di criticità:

- Evento critico
- Errore funzionale
- Avviso
- Informazioni

Eventi dello stesso tipo possono avere diversi livelli di criticità, a seconda della situazione in cui si è verificato l'evento.

Livello di importanza patch

Attributo della patch. Esistono cinque livelli di importanza per le patch di Microsoft e di terze parti:

- Critico
- Alto
- Medio
- Basso
- Sconosciuto

Il livello di importanza di una patch di Microsoft o di terze parti è determinato in base al livello di criticità meno favorevole tra le vulnerabilità che le patch dovrebbero correggere.

Negozio applicazioni

Componente di Kaspersky Security Center. Il negozio applicazioni viene utilizzato per installare le applicazioni nei dispositivi Android di proprietà degli utenti. Il negozio applicazioni consente di pubblicare i file APK delle applicazioni e i collegamenti alle applicazioni in Google Play.

Network Agent

Un componente di Kaspersky Security Center che consente l'interazione tra Administration Server e le applicazioni Kaspersky installate in un nodo di rete specifico (workstation o server). Questo componente è comune a tutte le applicazioni dell'azienda per Microsoft® Windows®. Esistono versioni distinte di Network Agent per le applicazioni Kaspersky sviluppate per i sistemi operativi Unix e macOS.

Network Location Awareness (NLA)

Servizio Windows che aiuta un sistema operativo a identificare la rete corrente. NLA rileva le modifiche alla rete e regola la configurazione di protezione del dispositivo.

Operatore di Kaspersky Security Center

Utente che monitora lo stato e l'esecuzione di un sistema di protezione gestito tramite Kaspersky Security Center.

Pacchetto di installazione

Un set di file creati per l'installazione remota di un'applicazione Kaspersky tramite il sistema di amministrazione remota Kaspersky Security Center. Il pacchetto di installazione contiene numerose impostazioni necessarie per installare l'applicazione e renderla operativa subito dopo l'installazione. Le impostazioni corrispondono alle impostazioni predefinite dell'applicazione. Il pacchetto di installazione viene creato utilizzando i file con le estensioni kpd e kud inclusi nel kit di distribuzione dell'applicazione.

Periodo licenza

Il periodo di tempo durante il quale l'utente ha accesso alle funzionalità dell'applicazione e dispone dei diritti necessari per utilizzare i servizi aggiuntivi. I servizi che possono essere utilizzati dipendono dal tipo di licenza.

Plug-in di gestione

Componente specializzato che fornisce l'interfaccia per la gestione applicazioni tramite Administration Console. Ogni applicazione dispone del proprio plug-in. È incluso in tutte le applicazioni Kaspersky che possono essere gestite utilizzando Kaspersky Security Center.

Profilo di configurazione

Criterio che contiene un insieme di impostazioni e limitazioni per un dispositivo mobile MDM iOS.

Profilo di provisioning

Insieme di impostazioni per l'esecuzione delle applicazioni nei dispositivi mobili iOS. Un profilo di provisioning contiene le informazioni sulla licenza ed è collegato a una specifica applicazione.

Profilo MDM iOS

Raccolta di impostazioni per la connessione di dispositivi mobili iOS ad Administration Server. Una volta che l'utente installa un profilo MDM iOS in un dispositivo mobile, questo si connette ad Administration Server.

Proprietario dispositivo

Il proprietario dispositivo è un utente che l'amministratore può contattare quando si rende necessario eseguire determinate operazioni con un dispositivo client.

Protezione anti-virus della rete

Set di misure tecniche e organizzative che riducono il rischio di penetrazione di virus e spam nella rete di un'organizzazione, oltre a impedire attacchi di rete, phishing e altre minacce. La sicurezza di rete aumenta quando si utilizzano applicazioni e servizi di protezione e quando si applicano e si rispettano i criteri di protezione dei dati aziendali.

Provider di servizi di protezione anti-virus

Organizzazione che fornisce a un'organizzazione client servizi di protezione anti-virus basati sulle soluzioni Kaspersky.

Punto di distribuzione

Computer in cui è installato Network Agent e che viene utilizzato per la distribuzione di aggiornamenti, l'installazione remota di applicazioni, l'acquisizione di informazioni sui computer in un gruppo di amministrazione e/o la trasmissione in un dominio. I punti di distribuzione hanno l'obiettivo di ridurre il carico sull'Administration Server durante la distribuzione degli aggiornamenti e di ottimizzare il traffico di rete. I punti di distribuzione possono essere assegnati automaticamente dall'Administration Server o manualmente dall'amministratore. Il punto di distribuzione era precedentemente noto come Update Agent.

Rete perimetrale (DMZ)

La rete perimetrale è un segmento di una rete locale in cui sono contenuti i server che risponde alle richieste del Web globale. Per garantire la protezione della rete locale di un'organizzazione, l'accesso alla LAN dalla rete perimetrale è protetto tramite firewall.

Ripristino

Riposizionamento dell'oggetto originale dalle cartelle Quarantena o Backup nella cartella originale in cui era memorizzato prima di essere messo in quarantena, disinfettato o eliminato, oppure in una cartella definita dall'utente.

Ripristino dei dati di Administration Server

Ripristino dei dati di Administration Server dalle informazioni salvate in Backup tramite l'utilità di backup. L'utilità consente di ripristinare:

- Database di Administration Server (criteri, attività, impostazioni delle applicazioni, eventi salvati in Administration Server)
- Informazioni sulla configurazione della struttura dei gruppi di amministrazione e dei dispositivi client
- Archivio dei file di installazione per l'installazione remota delle applicazioni (contenuto delle cartelle: Pacchetti, Disinstallazione e Aggiornamenti)
- Certificato di Administration Server

Ruolo IAM

Set di diritti per effettuare le richieste ai servizi basati su AWS. I ruoli IAM non sono associati a un utente o a un gruppo specifico; forniscono diritti di accesso senza le chiavi di accesso AWS IAM. È possibile assegnare un ruolo IAM agli utenti IAM, alle istanze EC2 e ai servizi o alle applicazioni basate su AWS.

Server degli aggiornamenti Kaspersky

I server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti per i database e i moduli delle applicazioni.

Server per dispositivi mobili

Componente di Kaspersky Security Center che fornisce l'accesso ai dispositivi mobili e consente di gestirli tramite Administration Console.

Server per dispositivi mobili MDM iOS

Componente di Kaspersky Security Center installato in un dispositivo client e che consente la connessione dei dispositivi mobili iOS ad Administration Server e la gestione dei dispositivi mobili iOS tramite Apple Push Notifications (APNs).

Server Web di Kaspersky Security Center

Componente di Kaspersky Security Center installato insieme ad Administration Server. Il server Web è progettato per la trasmissione tramite una rete di pacchetti di installazione indipendenti, profili MDM iOS e file da una cartella condivisa.

Soglia di attività virus

Numero massimo di eventi del tipo specificato consentiti in un determinato periodo di tempo; il superamento di questo numero viene interpretato come un aumento dell'attività dei virus e una minaccia di un attacco di un virus. Questa funzionalità è importante quando si verificano epidemie di virus, dal momento che consente agli amministratori di rispondere tempestivamente alle minacce associate agli attacchi dei virus.

SSL

Protocollo di criptaggio dei dati utilizzato per Internet e le reti locali. Secure Sockets Layer (SSL) viene utilizzato nelle applicazioni Web per creare una connessione protetta tra un client e un server.

Stato della protezione della rete

Stato della protezione corrente, che definisce la sicurezza dei dispositivi della rete aziendale. Lo stato della protezione della rete include fattori come le applicazioni di protezione installate, l'utilizzo delle chiavi di licenza e il numero e i tipi di minacce rilevate.

Stato protezione

Stato corrente della protezione, che riflette il livello di protezione del computer.

Upgrade di Kaspersky Security Center

Procedura di installazione di una versione più recente di Kaspersky Security Center in un dispositivo in cui è installata una versione precedente di questa applicazione.

Utente IAM

L'utente dei servizi AWS. Un utente IAM può disporre dei diritti per eseguire il polling dei segmenti cloud.

Utenti interni

Gli account degli utenti interni vengono utilizzati per operare con gli Administration Server virtuali. Kaspersky Security Center concede agli utenti interni dell'applicazione diritti equivalenti a quelli degli utenti reali.

Gli account degli utenti interni vengono creati e utilizzati solo in Kaspersky Security Center. Nessun dato relativo agli utenti interni viene trasferito al sistema operativo. Kaspersky Security Center esegue l'autenticazione degli utenti interni.

Vulnerabilità

Una vulnerabilità di un sistema operativo o un'applicazione che può essere utilizzata dagli sviluppatori di malware per penetrare nel sistema operativo o nell'applicazione e violarne l'integrità. La presenza di un numero elevato di vulnerabilità rende un sistema operativo inaffidabile, dal momento che i virus penetrati possono causare interruzioni del sistema operativo stesso e delle applicazioni installate.

Windows Server Update Services (WSUS)

Applicazione utilizzata per la distribuzione degli aggiornamenti per le applicazioni Microsoft ai computer degli utenti nella rete di un'organizzazione.

Workstation dell'amministratore

Un dispositivo in cui è installato Administration Console o utilizzato per aprire Kaspersky Security Center Web Console. Questo componente fornisce un'interfaccia di gestione per Kaspersky Security Center.

La workstation dell'amministratore viene utilizzata per configurare e gestire la parte server di Kaspersky Security Center. Utilizzando la workstation dell'amministratore, l'amministratore crea e gestisce un sistema centralizzato della protezione anti-virus per la rete LAN aziendale basato sulle applicazioni Kaspersky.

Informazioni sul codice di terze parti

Le informazioni sul codice di terze parti sono contenute nel file denominato legal_notices.txt, disponibile nella cartella di installazione dell'applicazione.

Note relative ai marchi registrati

I marchi registrati e i marchi di servizi sono di proprietà dei rispettivi titolari.

Adobe, Acrobat, Flash, Shockwave e PostScript sono marchi o marchi registrati di Adobe negli Stati Uniti e/o in altri paesi.

AMD e AMD64 sono marchi o marchi registrati di Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace sono marchi registrati di Amazon.com, Inc. o delle relative consociate.

Apache è un marchio o un marchio registrato di Apache Software Foundation negli Stati Uniti e in altri paesi.

Apple, AirPlay, AirDrop, AirPrint, App Store, Apple Configurator, AppleScript, FaceTime, FileVault, iBook, iBooks, iCloud, iPad, iPhone, iTunes, Leopard, macOS, Mac, Mac OS, OS X, Safari, Snow Leopard, Tiger, QuickTime e Touch ID sono marchi di Apple Inc.

Arm è un marchio registrato di Arm Limited (o delle sue filiali) negli Stati Uniti e/o altrove.

La parola, il marchio e i logo Bluetooth sono di proprietà di Bluetooth SIG, Inc.

Ubuntu, LTS sono marchi registrati di Canonical Ltd.

Cisco Systems, Cisco, Cisco Jabber, IOS sono marchi o marchi registrati di Cisco Systems, Inc. e/o delle relative consociate negli Stati Uniti e in altri paesi.

Citrix, XenServer sono marchi registrati o marchi di Cloud Software Group, Inc. e/o delle sue consociate negli Stati Uniti e/o in altri paesi.

Corel è un marchio o un marchio registrato di Corel Corporation e/o delle relative filiali in Canada, negli Stati Uniti e/o in altri paesi.

Cloudflare, il logo Cloudflare e Cloudflare Workers sono marchi e/o marchi registrati di Cloudflare, Inc. negli Stati Uniti e in altre giurisdizioni.

Dropbox è un marchio di Dropbox, Inc.

Radmin è un marchio registrato di Famatech.

Firebird è un marchio registrato di Firebird Foundation.

Foxit è un marchio registrato di Foxit Corporation.

FreeBSD è un marchio registrato di The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS e YouTube sono marchi di Google LLC.

EulerOS, FusionCompute, FusionSphere sono marchi di Huawei Technologies Co., Ltd.

Intel, Core, Xeon sono marchi registrati di Intel Corporation o delle sue affiliate.

IBM, QRadar sono marchi di International Business Machines Corporation, registrati presso diverse giurisdizioni a livello mondiale.

Node.js è un marchio di Joyent, Inc.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti e in altri paesi.

Logitech è un marchio o un marchio registrato di Logitech negli Stati Uniti e in altri paesi.

Microsoft, Active Directory, ActiveSync, BitLocker, Excel, Forefront, Internet Explorer, InfoPath, Hyper-V, Microsoft Edge, MultiPoint, MS-DOS, Office 365, PowerShell, PowerPoint, SharePoint, SQL Server, OneNote, Outlook, Skype, Tahoma, Visio, Win32, Windows, Windows PowerShell, Windows Media, Windows Mobile, Windows Server, Windows Phone, Windows Vista e Windows Azure sono marchi del gruppo di società Microsoft.

CVE è un marchio registrato di The MITRE Corporation.

Mozilla, Firefox, Thunderbird sono marchi di Mozilla Foundation negli Stati Uniti e in altri paesi.

Novell è un marchio registrato di Novell Enterprises Inc. negli Stati Uniti e in altri paesi.

NetWare è un marchio registrato di Novell Inc. negli Stati Uniti e in altri paesi.

OpenVPN è un marchio registrato di OpenVPN, Inc.

OpenSSL è un marchio di proprietà di OpenSSL Software Foundation.

Oracle, Java, JavaScript e TouchDown sono marchi registrati di Oracle e/o delle relative consociate.

Parallels, il logo Parallels e Coherence sono marchi o marchi registrati di Parallels International GmbH.

Chef è un marchio o un marchio registrato di Progress Software Corporation e/o di una delle relative consociate o filiali negli Stati Uniti e/o in altri paesi.

Puppet è un marchio o un marchio registrato di Puppet, Inc.

Python è un marchio o un marchio registrato di Python Software Foundation.

Red Hat, Fedora e Red Hat Enterprise Linux sono marchi o marchi registrati di Red Hat, Inc. o delle relative consociate negli Stati Uniti e in altri paesi.

Ansible è un marchio registrato di Red Hat. Inc. negli Stati Uniti e in altri paesi.

CentOS è un marchio o un marchio registrato di Red Hat, Inc. o delle relative consociate negli Stati Uniti e in altri paesi.

Il marchio BlackBerry è di proprietà di Research In Motion Limited ed è registrato negli Stati Uniti e potrebbe essere registrato o in attesa di registrazione in altri paesi.

Rocky Linux è un marchio registrato di The Rocky Enterprise Software Foundation.

SAMSUNG è un marchio di SAMSUNG negli Stati Uniti e in altri paesi.

Debian è un marchio registrato di Software in the Public Interest, Inc.

Splunk, SPL sono marchi e marchi registrati di Splunk Inc. negli Stati Uniti e in altri paesi.

SUSE è un marchio registrato di SUSE LLC negli Stati Uniti e in altri paesi.

Symbian è un marchio registrato di proprietà di Symbian Foundation Ltd.

OpenAPI è un marchio di Linux Foundation.

UNIX è un marchio registrato negli Stati Uniti e in altri paesi, concesso in licenza in esclusiva tramite X/Open Company Limited.

Zabbix è un marchio registrato di Zabbix SIA.

Problemi noti

Kaspersky Security Center Web Console presenta una serie di limitazioni non critiche per il funzionamento dell'applicazione:

- La console visualizza la sottosezione **Avvisi** nella sezione **Monitoraggio e generazione dei rapporti** del menu principale solo se è stata aggiunta una chiave di licenza per EDR Optimum all'archivio di Administration Server immettendo il codice di attivazione.

- Per garantire la potenza del criptaggio, il certificato di Administration Server deve essere firmato utilizzando SHA-2 e avere una chiave di lunghezza minima 2048. Se è necessario riemettere il certificato, fare riferimento alla Knowledge Base di Kaspersky Security Center.

- Se si crea un'attività con le impostazioni di pianificazione **Every N days** e **By days of week** in Kaspersky Security Center 15.1 Web Console e quindi si apre l'attività nelle versioni precedenti di Kaspersky Security Center Web Console o Kaspersky Security Center Administration Console (ad esempio, quando l'attività viene applicata anche agli Administration Server secondari, che possono essere sia basati su Linux che su Windows), le impostazioni di pianificazione potrebbero essere visualizzate in modo errato o si potrebbe verificare un errore.

- Quando si configura l'esportazione nei sistemi SIEM in Kaspersky Security Center Web Console e si seleziona il protocollo UDP, viene restituito un errore dopo aver fatto clic sul pulsante **Controlla connessione**, poiché UDP non stabilisce una connessione e la distribuzione dei dati non può essere garantita.

- Quando si esegue un'attività per rimuovere Network Agent da un dispositivo basato sull'architettura Arm in cui viene eseguito Astra Linux Special Edition RUSB.10015-01 (aggiornamento operativo 1.7), Network Agent viene rimosso, ma lo stato dell'attività per l'avanzamento corrente nell'elenco delle attività è bloccato.

- La finestra delle proprietà del criterio di Kaspersky Device Management for iOS contiene ancora la sezione **Impostazioni dei dispositivi EAS**, anche se Exchange ActiveSync non è più supportato.

- La connessione a KSN tramite HTTPS non riesce se Kaspersky Security Center è installato in un dispositivo con simboli cirillici nel nome del dispositivo e il proxy KSN è abilitato in Administration Server.

- Quando si tenta di modificare le proprietà di un account utente per cui è abilitata l'opzione **Richiedi l'autenticazione per controllare l'autorizzazione di modifica degli account utente** e quindi si fa clic su **Annulla** nella finestra **Protezione account**, si verifica un errore imprevisto.

- Se si modifica l'ora o il fuso orario nel dispositivo, è necessario riavviare il servizio Kaspersky Security Center Web Console.

- Se viene utilizzato un proxy nel dispositivo e le variabili di ambiente proxy sono impostate, il programma di installazione di Kaspersky Security Center Web Console potrebbe bloccarsi.

- Quando si importa l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* o *Aggiorna verifica*, l'opzione **Selezionare i dispositivi a cui assegnare l'attività** è abilitata. Queste attività non possono essere assegnate a una selezione di dispositivi o a dispositivi specifici. Se si assegna l'attività *Scarica aggiornamenti negli archivi dei punti di distribuzione* o *Aggiorna verifica* a dispositivi specifici, l'attività verrà importata in modo errato.

- Se si esegue il polling di Active Directory utilizzando un punto di distribuzione Linux con Network Agent versione 15 installato, è possibile eseguire il polling solo dei domini di Active Directory per i quali si specificano l'indirizzo e le credenziali dell'utente. Il polling del dominio Active Directory corrente e della foresta di domini Active Directory non è disponibile.

- I dispositivi client potrebbero non essere trovati dopo aver eseguito il polling di rete di Windows.

- Nella procedura guidata **Aggiungi Administration Server secondario**, se si specifica un account con la verifica in due passaggi abilitata per l'autenticazione sul futuro server secondario, la procedura guidata termina con un errore. Per risolvere questo problema, specificare un account per il quale la verifica in due passaggi è disabilitata o creare la gerarchia dal futuro server secondario.

- Durante l'accesso a Kaspersky Security Center Web Console, se si utilizza l'autenticazione del dominio e si specifica un Administration Server virtuale a cui connettersi, viene effettuata la disconnessione e quindi viene tentato l'accesso all'Administration Server principale. Kaspersky Security Center Web Console si connette all'Administration Server virtuale. Per connettersi all'Administration Server primario, riaprire il browser.

- Il polling di rete Windows rapido/completo restituisce un risultato vuoto.

- Se si installa Kaspersky Security Center Web Console con Identity and Access Manager e si cambia l'Administration Server per Kaspersky Security Center Web Console, Identity and Access Manager non ottiene le informazioni sul nuovo Administration Server.

- Un dispositivo gestito che dispone di più schede di rete invia all'Administration Server informazioni sull'indirizzo MAC della scheda di rete che non sono quelle utilizzate per la connessione all'Administration Server.

- La connessione di prova a SIEM fallisce quando viene selezionato il formato dati CEF.

- L'autenticazione NTLM non funziona per gli account utente all'interno del gruppo Utenti protetti.