kaspersky

Kaspersky Security Center 14.2 Windows

© 2025 AO Kaspersky Lab

Índice

Ajuda do Kaspersky Security Center 14.2

O que há de novo

Kaspersky Security Center 14.2

- Conceitos básicos
  - Servidor de Administração
  - Hierarquia de Servidores de Administração
  - Servidor de Administração virtual
  - Servidor de dispositivos móveis
  - Servidor Web
  - Agente de Rede
  - Grupos de administração
  - Dispositivo gerenciado
  - Dispositivo não atribuído
  - Estação de trabalho do administrador
  - Plugin de gerenciamento
  - Plug-in da Web de gerenciamento
  - Políticas
  - Perfis da política
  - Tarefas
  - Escopo da tarefa
  - Como as configurações do aplicativo local se relacionam com as políticas
  - Ponto de distribuição
  - Gateway de conexão
- Sobre o Kaspersky Security Center
  - Requisitos de hardware e software
    - Requisitos do Servidor de Administração
    - Requisitos do Web Console
    - Requisitos de servidores móveis
    - Requisitos do Console de Administração
    - Requisitos do Agente de Rede
  - Aplicativos e soluções da Kaspersky compatíveis
  - Licenças e recursos do Kaspersky Security Center 14.2
  - Sobre a compatibilidade do Servidor de Administração e Kaspersky Security Center Web Console
  - Comparativo do Kaspersky Security Center: baseado em Windows X baseado em Linux
  - Sobre o Kaspersky Security Center Cloud Console
- Arquitetura
- Cenário principal de implementação
- Portas usadas pelo Kaspersky Security Center
- Certificados para trabalhar com o Kaspersky Security Center
  - Sobre os certificados do Kaspersky Security Center
  - Sobre o certificado do Servidor de Administração
  - Requisitos para certificados personalizados usados no Kaspersky Security Center
  - Cenário: especificação do certificado personalizado do Servidor de Administração

- Substituição do certificado do Servidor de Administração usando o utilitário klsetsrvcert
- Conexão dos Agentes de Rede ao Servidor de Administração usando o utilitário klmover
- Reemissão do certificado do Servidor Web

Esquemas para o tráfego de dados e uso de porta

- Servidor de Administração e dispositivos gerenciados dentro de uma rede de área local
- Servidor de Administração principal dentro da rede de área local e dois Servidores de Administração secundários
- Servidor de Administração na LAN, dispositivos gerenciados na Internet, proxy reverso em uso
- Servidor de Administração dentro da LAN, dispositivos gerenciados na Internet, e o gateway de conexão em uso
- Servidor de Administração dentro do DMZ, dispositivos gerenciados na Internet
- Interação dos componentes e aplicativos de segurança do Kaspersky Security Center: mais informações
  - Convenções usadas em esquemas de interação
  - Servidor de Administração e DBMS
  - Servidor de Administração e Console de Administração
  - Servidor de Administração e dispositivo cliente: Gerenciar o aplicativo de segurança
  - Atualizar o software em um dispositivo cliente através de uma ponto de distribuição
  - Hierarquia de Servidores de Administração: Servidor de Administração principal e Servidor de Administração secundário
  - Hierarquia de Servidores de Administração com um Servidor de Administração secundário na DMZ
  - Servidor de Administração, um gateway de conexão em um segmento da rede e um dispositivo cliente
  - Servidor de Administração e dois dispositivos na DMZ: um gateway de conexão e um dispositivo cliente
  - Servidor de Administração e Kaspersky Security Center Web Console
  - Ativar e gerenciar o aplicativo de segurança em um dispositivo móvel

Implementação de melhores práticas

- Guia de Proteção
  - Implementação do Servidor de Administração
  - Segurança de conexão
  - Contas e autenticação
  - Gerenciamento da proteção do Servidor de Administração
  - Gerenciamento de proteção dos dispositivos cliente
  - Configuração da proteção para aplicativos gerenciados
  - Manutenção do Servidor de Administração
  - Transferência de eventos para sistemas de terceiros
- Preparação para implementação
  - Planejar a implementação do Kaspersky Security Center
    - Esquemas típicos para implementação do sistema de proteção
    - Sobre o planejamento da implementação do Kaspersky Security Center em uma rede da organização
    - Selecionar uma estrutura para a proteção de uma empresa
    - Configurações padrão do Kaspersky Security Center
      - Configuração padrão: escritório único
      - Configuração padrão: Alguns escritórios de larga escala executam por si seus próprios administradores
      - Configuração padrão: múltiplos pequenos escritórios remotos
    - Selecionar um DBMS
    - Configuração do servidor MariaDB x64 para uso com o Kaspersky Security Center 14.2
    - Configurando o servidor MySQL x64 para uso com o Kaspersky Security Center 14.2
    - Configurar o servidor PostgreSQL ou Postgres Pro para uso com o Kaspersky Security Center 14.2
    - Gerenciar dispositivos móveis com o Kaspersky Endpoint Security for Android
    - Fornecer acesso à Internet ao Servidor de Administração
      - Acesso à Internet: Servidor de Administração em uma rede local

Acesso à Internet: Servidor de Administração em DMZ
Acesso à Internet: Agente de Rede como um gateway de conexão no DMZ
Sobre os pontos de distribuição
Aumento do limite de descritores de arquivo para o serviço klnagent
Calcular o número e a configuração de pontos de distribuição
Hierarquia de Servidores de Administração
Servidores de Administração virtual
Informações sobre as limitações do Kaspersky Security Center
Carga de rede
Implementação inicial da proteção antivírus
Atualização inicial dos bancos de dados antivírus
Sincronização de um cliente com o Servidor de Administração
Atualização adicional dos bancos de dados antivírus
Processamento de eventos clientes pelo Servidor de Administração
Tráfego durante 24 horas
Preparar para o gerenciamento do dispositivo móvel
Servidor de dispositivos móveis Exchange
Como implementar um Servidor de dispositivos móveis Exchange
Direitos necessários para a implementação de um Servidor de dispositivos móveis Exchange
Conta para o serviço Exchange ActiveSync
Servidor MDM do iOS
Configuração padrão: Kaspersky Device Management for iOS no DMZ
Configuração padrão: Servidor de MDM do iOS na rede local de uma organização
Gerenciar dispositivos móveis com o Kaspersky Endpoint Security for Android
Informações sobre o desempenho do Servidor de Administração
Limitações na conexão a um Servidor de Administração
Resultados do teste de desempenho do Servidor de Administração
Resultados do teste de desempenho do Servidor proxy da KSN
Configurações de rede para interação com serviços externos
Implementar o Agente de Rede e o aplicativo de segurança
Implementação inicial
Configurar os instaladores
Pacotes de instalação
Propriedades MSI e arquivos de transformação
Implementação com ferramentas de terceiros para a instalação remota de aplicativos
Sobre as tarefas de instalação remotas no Kaspersky Security Center
Implementação ao capturar e copiar a imagem de um dispositivo
Cópia incorreta de uma imagem do disco rígido
Implementar usando políticas de grupo do Microsoft Windows
Implementação forçada através da tarefa de instalação remota do Kaspersky Security Center
Executar pacotes independentes criados pelo Kaspersky Security Center
Opções para a instalação manual de aplicativos
Como criar um arquivo MST
Instalação remota de aplicativos em dispositivos com o Agente de Rede instalado
O gerenciamento do dispositivo reinicia na tarefa de instalação remota
Adequabilidade da atualização dos bancos de dados em um pacote de instalação de um aplicativo de segurança

Usar as ferramentas da instalação remota de aplicativos no Kaspersky Security Center para executar arquivos executáveis relevantes em dispositivos gerenciados
Monitorar a implementação
Configurar os instaladores
Informações gerais
Instalação em modo silencioso (com um arquivo de resposta)
Instalação do Agente de Rede no modo silencioso (sem um arquivo de resposta)
Configuração de instalação parcial através de setup.exe
Parâmetros de instalação do Servidor de Administração
Parâmetros de instalação do Agente de Rede
Infraestrutura virtual
Dicas sobre como reduzir a carga em máquinas virtuais
Suporte de máquinas virtuais dinâmicas
Suporte para copiar máquinas virtuais
O suporte do sistema de arquivos reverte para dispositivos com o Agente de Rede
Instalação local de aplicativos
Instalação local do Agente de Rede
Instalar o Agente de Rede em modo silencioso
Instalar o Agente de Rede para Linux no modo silencioso (com um arquivo de resposta)
Instalação do Agente de Rede para Linux no modo interativo
Preparar um dispositivo executando o Astra Linux no modo de ambiente de software fechado para a instalação do Agente de Rede
Instalação local do plugin de gerenciamento de aplicativos
Instalando aplicativos no modo silencioso
Instalação de aplicativos usando pacotes independentes
Configurações do pacote de instalação do Agente de Rede
Visualizar a Política de Privacidade
Implementar sistemas de gerenciamento de dispositivos móveis
Implementar um sistema para gerenciamento através do protocolo Exchange ActiveSync
Instalação de um Servidor de dispositivos móveis para Exchange ActiveSync
Conectar dispositivos móveis a um Servidor de dispositivos móveis Exchange
Configurar o servidor da Web dos Serviços de informações da Internet
Instalação local de um Servidor de dispositivos móveis Exchange
Instalação remota de um Servidor de dispositivos móveis do Microsoft Exchange
Implementar um sistema para gerenciamento através do protocolo MDM do iOS
Instalando o Servidor de MDM do iOS
Instalando o Servidor de MDM do iOS no modo silencioso
Cenários de implementação do Servidor de MDM do iOS
Esquema de implementação simplificada
Esquema de implementação envolvendo a delegação de restrição Kerberos (KCD)
Recebimento de um certificado de APNs
Renovação de um certificado de APNs
Configurando um certificado de reserva de servidor MDM iOS
Instalação de um certificado de APNs em um Servidor de MDM do iOS
Configurar o acesso ao serviço Apple Push Notification
Emissão e instalação de um certificado compartilhado em um dispositivo móvel
Adicionar um dispositivo KES na lista de dispositivos gerenciados

Conectar dispositivos KES ao Servidor de Administração
Conexão direta de dispositivos ao Servidor de Administração
Esquema para conectar dispositivos KES ao servidor envolvendo a delegação de restrição Kerberos (KCD)
Usar o Firebase Cloud Messaging
Integração com a infraestrutura de chaves públicas
Servidor Web do Kaspersky Security Center
Instalação do Kaspersky Security Center
Preparar para instalar
Contas para trabalhar com o DBMS
Configurando contas para uso com SQL Server (autenticação do Windows)
Configurar contas para uso com SQL Server (autenticação do SQL Server)
Configuração de contas para uso com MySQL e MariaDB
Mover dados de um espaço de tabela compartilhado para um espaço de tabela individual nos DBMSs MySQL e MariaDB
Configurar contas para uso com PostgreSQL e Postgres Pro
Cenário: Autenticação do Microsoft SQL Server
Recomendações sobre a instalação do Servidor de Administração
Criar contas para os serviços do Servidor de Administração em um cluster para falhas
Definir uma pasta compartilhada
Instalação remota com as ferramentas do Servidor de Administração através das políticas de grupo do Active Directory
Instalação remota através da entrega do caminho UNC a um pacote independente
Atualizar da partir da pasta compartilhada do Servidor de Administração
Imagens de instalação de sistemas operacionais
Especificar o endereço do Servidor de Administração
Instalação padrão
Etapa 1. Leitura do Contrato de Licença e da Política de Privacidade
Etapa 2. Seleção do método de instalação
Etapa 3. Instalar o Kaspersky Security Center Web Console
Etapa 4. Selecionando o tamanho da rede
Etapa 5. Seleção do banco de dados
Etapa 6. Configuração do servidor SQL
Etapa 7. Seleção do modo de autenticação
Etapa 8. Descompactação e instalação dos arquivos no disco rígido
Instalação personalizada
Etapa 1. Leitura do Contrato de Licença e da Política de Privacidade
Etapa 2. Seleção do método de instalação
Etapa 3. Seleção dos componentes a serem instalados
Etapa 4. Instalar o Kaspersky Security Center Web Console
Etapa 5. Selecionando o tamanho da rede
Etapa 6. Seleção do banco de dados
Etapa 7. Configuração do servidor SQL
Etapa 8. Seleção do modo de autenticação
Etapa 9. Selecionar a conta para iniciar o Servidor de Administração
Etapa 10. Selecionar a conta para a execução dos serviços do Kaspersky Security Center
Etapa 11. Seleção de uma pasta compartilhada
Etapa 12. Configuração de conexão ao Servidor de Administração
Etapa 13. Definição do endereço do Servidor de Administração
Etapa 14. Endereço do Servidor de Administração para conexão de dispositivos móveis

Etapa 15. Seleção dos plugins de gerenciamento de aplicativos
Etapa 16. Descompactação e instalação dos arquivos no disco rígido
Implementação do cluster de failover do Kaspersky Security Center
Cenário: implantação de um cluster de failover do Kaspersky Security Center
Sobre o cluster de failover do Kaspersky Security Center
Preparando um servidor de arquivos para um cluster de failover do Kaspersky Security Center
Preparando nós para um cluster de failover do Kaspersky Security Center
Instalando o Kaspersky Security Center nos nós do cluster de failover do Kaspersky Security Center
Iniciando e interrompendo nós de cluster manualmente
Instalação do Servidor de Administração em um cluster de failover da Microsoft
Etapa 1. Leitura do Contrato de Licença e da Política de Privacidade
Etapa 2. Selecionando o tipo de instalação em um cluster
Etapa 3. Especificando o nome do Servidor de Administração virtual
Etapa 4. Especificando os detalhes da rede do Servidor de Administração virtual
Etapa 5. Especificando um grupo de cluster
Etapa 6. Selecionando um armazenamento de dados de cluster
Etapa 7. Especificando uma conta para instalação remota
Etapa 8. Seleção dos componentes a serem instalados
Etapa 9. Selecionando o tamanho da rede
Etapa 10. Seleção do banco de dados
Etapa 11. Configuração do servidor SQL
Etapa 12. Seleção do modo de autenticação
Etapa 13. Selecionar a conta para iniciar o Servidor de Administração
Etapa 14. Selecionar a conta para a execução dos serviços do Kaspersky Security Center
Etapa 15. Seleção de uma pasta compartilhada
Etapa 16. Configuração de conexão ao Servidor de Administração
Etapa 17. Definição do endereço do Servidor de Administração
Etapa 18. Endereço do Servidor de Administração para conexão de dispositivos móveis
Etapa 19. Descompactação e instalação dos arquivos no disco rígido
Instalar o Servidor de Administração no modo silencioso
Instalação do Console de Administração na estação de trabalho do administrador
Alterações no sistema após a instalação do Kaspersky Security Center
Removendo o aplicativo
Sobre atualizar o Kaspersky Security Center
Cenário: atualização do Kaspersky Security Center e de aplicativos de segurança gerenciados
Atualização do Kaspersky Security Center a partir de uma versão anterior
Atualização do Kaspersky Security Center a partir de nós do cluster de failover do Kaspersky Security Center
Configuração inicial do Kaspersky Security Center
Guia de Proteção
Assistente de Início Rápido do Servidor de Administração
Sobre o Assistente de Início Rápido
Iniciar o Assistente de início rápido do Servidor de Administração
Etapa 1. Configurar um servidor proxy
Etapa 2. Selecionando o método de ativação do aplicativo
Etapa 3. Seleção das áreas de proteção e sistemas operacionais
Etapa 4. Selecionar os plugins para os aplicativos gerenciados
Etapa 5. Baixando os pacote de distribuição e criando pacotes de instalação

Etapa 6. Configurando o uso da Kaspersky Security Network
Etapa 7. Configurar notificações por e-mail
Etapa 8. Configurar o Gerenciamento de atualizações
Etapa 9. Criar uma configuração da proteção inicial
Etapa 10. Conectar dispositivos móveis
Etapa 11. Baixar atualizações
Etapa 12. Localização dos dispositivos
Etapa 13. Fechar o Assistente de início rápido
Configurar a conexão do Console de Administração ao Servidor de Administração
Definição das configurações de acesso à Internet para o Servidor de Administração
Conectando dispositivos fora do escritório
Cenário: Conectando dispositivos externos por meio de um gateway de conexão
Cenário: conectando dispositivos ausentes do escritório por meio de um Servidor de Administração secundário na DMZ
Sobre a conexão de dispositivos externos
Conexão de dispositivos de desktop externos com o Servidor de Administração
Sobre a configuração de perfis de conexão para usuários ausentes
Criando um perfil de conexão para usuários ausentes
Sobre a mudança do Agente de Rede para outro servidor de Administração
Criar uma regra de troca do Agente de Rede por localização da rede
Criptografar comunicação com TLS
Notificações de eventos
Configurar a notificação de evento
Testar as notificações
Notificações de evento exibidas executando um arquivo executável
Configurar interface
Localizar dispositivos na rede
Cenário: Localizar dispositivos na rede
Dispositivos não atribuídos
Localização dos dispositivos
Sondagem da rede do Windows
Sondagem do Active Directory
Sondagem do conjunto de IPs
Sondagem Zeroconf
Trabalhar com domínios do Windows. Visualização e alteração das configurações de domínio
Configuração de regras de retenção para dispositivos não atribuídos
Trabalhar com conjuntos de IPs
Criação de um conjunto de IPs
Visualização e alteração de configurações de conjuntos de IPs
Trabalhar com os grupos do Active Directory. Visualização e modificação de configurações de grupo
Criar regras para migrar dispositivos automaticamente para grupos de administração
Usar o modo dinâmico VDI nos dispositivos cliente
Ativar o modo dinâmico VDI nas propriedades de um pacote de instalação para o Agente de Rede
Pesquisar por dispositivos que fazem parte da VDI
Mover os dispositivos da VDI para um grupo de administração
Inventário de equipamentos
Adição de informações dobre novos dispositivos
Configuração de critérios usados para definir dispositivos corporativos

Configurar campos personalizados
Licenciamento
Eventos do limite do licenciamento excedidos
Sobre o licenciamento
Sobre a licença
Sobre o Contrato de Licença do Usuário Final
Sobre o certificado de licença
Sobre a chave de licença
Sobre o arquivo de chave
Sobre a assinatura
Sobre o código de ativação
Revogando o consentimento com um Contrato de Licença do Usuário Final
Sobre a coleta de dados
Opções de licença do Kaspersky Security Center
Recursos de Licenças do Kaspersky Security Center e aplicativos gerenciados
Aplicativos da Kaspersky. Implementação centralizada
Substituição de aplicativos de segurança de terceiros
Instalação de aplicativos usando a tarefa de instalação remota
Instalar um aplicativo nos dispositivos selecionados
Instalação de um aplicativo em dispositivos cliente em um grupo de administração
Instalar um aplicativo usando as políticas de grupo do Active Directory
Instalando aplicativos nos Servidores de Administração secundários
Instalação de aplicativos usando o Assistente de instalação remota
Exibir um relatório de implementação da proteção
Como trabalhar com os plug-ins de gerenciamento
Remoção remota de aplicativos
Remoção remota de um aplicativo de um dispositivo cliente do grupo de administração
Remoção remota de um aplicativo de dispositivos selecionados
Trabalho com pacotes de instalação
Criação de um pacote de instalação
Criação do pacote de instalação independente
Criar pacotes de instalação personalizados
Exibir e editar as propriedades de pacotes de instalação personalizada
Obtenção do pacote de instalação do agente de rede a partir do kit de distribuição do Kaspersky Security Center
Distribuindo pacotes de instalação para Servidores de Administração secundários
Distribuir os pacotes de instalação através de pontos de distribuição
Transferência de resultados da instalação do aplicativo para o Kaspersky Security Center
Definindo o endereço do servidor proxy da KSN para pacotes de instalação
Obtenção de versões atualizadas de aplicativos
Preparação de um dispositivo Windows para instalação remota
Preparar um dispositivo Linux e instalar o Agente de Rede em um dispositivo Linux remotamente
Preparo de um dispositivo executando o SUSE Linux Enterprise Server 15 para instalação do agente de rede
Preparar um dispositivo macOS para a instalação remota do Agente de Rede
Aplicativos Kaspersky: licenciamento e ativação
Licenciamento de aplicativos gerenciados
Visualizando de informações sobre chaves de licença em uso
Adição de uma chave de licença ao repositório do Servidor de Administração

Adição de uma chave de licença do Servidor de Administração
Remover uma chave de licença do Servidor de Administração
Implementando uma chave de licença para dispositivos clientes
Distribuição automática de uma chave de licença
Criação e visualização de um relatório de uso da chave de licença
Visualizando informações sobre as chaves de licença do aplicativo
Exportação de um arquivo de chave de licença
Configuração da proteção da rede
Cenário: Configurar a proteção da rede
Configuração e propagação de políticas: abordagem centrada no dispositivo
Sobre as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário
Configuração manual da política do Kaspersky Endpoint Security
Configurar a política na seção Proteção Avançada Contra Ameaças
Configurar a política na seção Proteção Essencial Contra Ameaças
Configurar a política na seção Configurações Gerais
Configurando a política na seção Configuração de eventos
Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security
Configuração manual da tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security
Agendar a tarefa Encontrar vulnerabilidades e atualizações necessárias
Configuração manual da tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades
Configuração do número máximo de eventos no repositório de eventos
Definindo o período máximo de armazenamento para as informações sobre vulnerabilidades corrigidas
Tarefas de gerenciamento
Criar uma tarefa
Criação de uma tarefa do Servidor de Administração
Criar uma tarefa para dispositivos específicos
Criação de uma tarefa local
Exibição de uma tarefa de grupo herdada no espaço de trabalho de um grupo hospedado
Ativar automaticamente os dispositivos antes de iniciar uma tarefa
Desativar automaticamente um dispositivo após a conclusão de uma tarefa
Limitação do tempo de execução de tarefas
Exportação de tarefa
Importação de uma tarefa
Conversão de tarefas
Início e interrupção manual de uma tarefa
Pausa e continuação manual de uma tarefa
Monitoramento de execução de tarefa
Visualização de resultados da execução de tarefas armazenados no Servidor de Administração
Configuração da filtragem de informações sobre resultados da execução de tarefas
Modificar uma tarefa. Reverter modificações
Comparar tarefas
Contas para iniciar tarefas
Exportar histórico de execução de tarefas
Assistente para Alterar a Senha das Tarefas
Etapa 1. Especificar as credenciais
Etapa 2. Selecionar uma ação a ser executada
Etapa 3. Visualizar os resultados

Criar uma hierarquia de grupos de administração subordinados a um Servidor de Administração virtual
Políticas e perfis da política
Hierarquia de políticas, usando perfis de política
Hierarquia de políticas
Perfis da política
Herança de configurações da política
Gerenciamento de políticas
Criação de uma política
Exibição de política herdada em um subgrupo
Ativação de uma política
Ativação automática de uma política no evento Ataque de vírus
Aplicar uma política de ausência do escritório
Modificando uma política. Reverter modificações
Visualizar o gráfico de status de distribuição da política
Comparar políticas
Exclusão de uma política
Cópia de uma política
Exportação de uma política
Importação de uma política
Converter políticas
Gerenciando perfis de política
Gerenciando perfis de política
Criar um perfil da política
Modificar um perfil da política
Excluir um perfil de política
Criar uma regra de ativação do perfil da política
Regras de migração de dispositivos
Clonar as regras para migrar dispositivos
Categorização de software
Prerrequisitos para instalar aplicativos em dispositivos de uma organização cliente
Exibir e editar as configurações do aplicativo local
Atualizar Kaspersky Security Center e os aplicativos gerenciados
Cenário: Atualização regular dos bancos de dados e dos aplicativos Kaspersky
Sobre atualização de bancos de dados, módulos de software e aplicativos da Kaspersky
Sobre usar os arquivos diff para atualizar bancos de dados e módulos do software Kaspersky
Ativação do recurso Baixar arquivos diff
Criar a tarefa para baixar as atualizações no repositório do Servidor de Administração
Criar as atualizações de download para a tarefa dos repositórios dos pontos de distribuição
Configurar a tarefa de Baixar as atualizações ao repositório do Servidor de Administração
Verificação das atualizações baixadas
Configuração de políticas de teste e tarefas auxiliares
Visualização de atualizações baixadas
A instalação automática do Kaspersky Endpoint Security atualiza em dispositivos
Modelo offline de download da atualização
Ativar e desativar o modelo offline de download da atualização
Atualização automática e correção para componentes do Kaspersky Security Center
Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center

- Distribuição automática de atualizações
  - Distribuição automática de atualizações para dispositivos cliente
  - Distribuindo atualizações para Servidores de Administração secundários automaticamente
  - Atribuir os pontos de distribuição automaticamente
  - Atribuir um dispositivo como um ponto de distribuição manualmente
  - Remover um dispositivo da lista de pontos de distribuição
  - Baixar atualizações por pontos de distribuição
- Excluir as atualizações do software do repositório
- Instalação do patch para um aplicativo Kaspersky no modo de cluster

Gerenciar aplicativos de terceiros em dispositivos cliente

- Instalar atualizações de software de terceiros
  - Cenário: Atualizando software de terceiros
  - Visualização de informações sobre atualizações disponíveis para aplicativos de terceiros
  - Aprovar e recusar atualizações de software
  - Sincronização de atualizações a partir do Windows Update com Servidor de Administração
    - Etapa 1. Definindo se o tráfego deve ser reduzido
    - Etapa 2. Aplicativos
    - Etapa 3. Categorias de atualização
    - Etapa 4. Idiomas das atualizações
    - Etapa 5. Selecionar a conta para iniciar a tarefa
    - Etapa 6. Configurar um agendamento de início da tarefa
    - Etapa 7. Definir o nome da tarefa
    - Etapa 8. Concluir a criação da tarefa
  - Instalar manualmente as atualizações nos dispositivos
  - Configurar as atualizações do Windows em uma política de Agente de Rede
- Corrigindo vulnerabilidades de software de terceiros
  - Cenário: Encontrar e corrigir vulnerabilidades de software de terceiros
  - Sobre como encontrar e corrigir vulnerabilidades de software
  - Exibir informações sobre as vulnerabilidades do software
  - Visualizar as estatísticas de vulnerabilidades em dispositivos gerenciados
  - Verificar os aplicativos quanto a vulnerabilidades
  - Correção das vulnerabilidades em aplicativos
  - Correção de vulnerabilidades em uma rede isolada
    - Cenário: correção de vulnerabilidades de softwares de terceiros em uma rede isolada
    - Sobre a correção de vulnerabilidades de softwares de terceiros em uma rede isolada
    - Configuração do Servidor de Administração com acesso à Internet para corrigir vulnerabilidades em uma rede isolada
    - Configuração de Servidores de Administração isolados para corrigir vulnerabilidades em uma rede isolada
    - Transmissão de patches e instalação de atualizações em uma rede isolada
    - Desativação da opção de transmissão de patches e instalação de atualizações em uma rede isolada
  - Ignorar as vulnerabilidades de software
  - Selecionar as correções do usuário para vulnerabilidades em software de terceiros
  - Regras para instalação da atualização
- Grupos de aplicativos
  - Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos clientes
  - Usar o Controle de Aplicativos para gerenciar arquivos executáveis
  - Criar categorias de aplicativos para as políticas do Kaspersky Endpoint Security for Windows
  - Criar uma categoria de aplicativos com conteúdo adicionado manualmente

Criar uma categoria de aplicativo que inclua arquivos executáveis dos dispositivos selecionados
Criar uma categoria de aplicativo que inclua arquivos executáveis de uma pasta específica
Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos
Configurar o gerenciamento da inicialização do aplicativo em dispositivos cliente
Visualização dos resultados da análise estática das regras de inicialização aplicadas a arquivos executáveis
Visualização do registro de aplicativos
Alterar o horário de início do inventário de software
Sobre o gerenciamento de chaves de licença de aplicativos de terceiros
Criar grupo de aplicativos licenciados
Gerenciamento de chaves de licença para grupos de aplicativos licenciados
Inventário de arquivos executáveis
Visualização de informações sobre arquivos executados
Monitoramento e relatórios
Cenário: Monitoramento e relatórios
Monitorando as luzes de tráfego e os eventos registrados no Console de Administração
Trabalhar com relatórios, estatísticas e notificações
Trabalhar com relatórios
Criação de um modelo de relatório
Visualização e edição das propriedades do modelo de relatório
Formato de filtro estendido nos modelos de relatório
Convertendo o filtro no formato estendido
Configurando o filtro estendido
Criação e visualização de um relatório
Para salvar um relatório
Criação de uma tarefa de entrega de relatório
Etapa 1. Selecionar o tipo de tarefa
Etapa 2. Selecionar o tipo de relatório
Etapa 3. Ações em um relatório
Etapa 4. Selecionar a conta para iniciar a tarefa
Etapa 5. Configurar um agendamento da tarefa
Etapa 6. Definir o nome da tarefa
Etapa 7. Concluir a criação da tarefa
Gerenciar estatísticas
Configurar a notificação de evento
Criar um certificado para um servidor SMTP
Seleções de eventos
Visualização de uma seleção de eventos
Personalização de uma seleção de eventos
Criar uma seleção de eventos
Exportação de uma seleção de eventos para um arquivo de texto
Exclusão de eventos da uma seleção
Adicionar aplicativos a exclusões por solicitação do usuário
Seleções de dispositivos
Exibir uma seleção de dispositivos
Configurar uma seleção de dispositivos
Exportar as configurações de uma seleção de dispositivos para um arquivo
Criar uma seleção de dispositivos

Criar uma seleção de dispositivos de acordo com as configurações importadas
Remover os dispositivos de grupos de administração em uma seleção
Monitoramento da instalação e desinstalação de aplicativos
Eventos dos componentes do Kaspersky Security Center
Estrutura de dados da descrição do tipo de evento
Eventos do Servidor de Administração
Eventos críticos do Servidor de Administração
Eventos de falha funcional do Servidor de Administração
Eventos de aviso do Servidor de Administração
Eventos informativos do Servidor de Administração
Eventos do Agente de Rede
Eventos de falha funcional do Agente de Rede
Eventos de aviso do Agente de Rede
Eventos informativos do Agente de Rede
Eventos do Servidor de MDM do iOS
Eventos de falha funcional do Servidor de MDM do iOS
Eventos de aviso do Servidor de MDM do iOS
Eventos informativos do Servidor de MDM do iOS
Eventos do Servidor de dispositivos móveis Microsoft Exchange
Eventos de falha funcional do Servidor de dispositivos móveis Exchange
Eventos informativos do Servidor de dispositivos móveis Exchange
Bloqueio de eventos frequentes
Sobre o bloqueio de eventos frequentes
Gerenciando o bloqueio de eventos frequentes
Removendo o bloqueio de eventos frequentes
Exportando uma lista de eventos frequentes para um arquivo
Controle de alterações no status de máquinas virtuais
Monitoramento do status de proteção antivírus usando informações do registro do sistema
Exibir e configurar as ações quando os dispositivos mostram inatividade
Desativando o recebimento de Novidades Kaspersky
Ajuste de pontos de distribuição e gateways de conexão
Configuração padrão de pontos de distribuição: escritório único
Configuração padrão de pontos de distribuição: múltiplos pequenos escritórios remotos
Atribuindo um dispositivo para agir como ponto de distribuição
Conectando um dispositivo Linux como um gateway em zona desmilitarizada
Conectando um dispositivo Linux ao Servidor de Administração por meio de um gateway de conexão
Adicionando um gateway de conexão na DMZ como um ponto de distribuição
Atribuir os pontos de distribuição automaticamente
Sobre a instalação local do Agente de Rede em um dispositivo selecionado como um ponto de distribuição
Sobre usar um ponto de distribuição como um gateway de conexão
Adicionar intervalos de IP na lista de intervalos sondados por um ponto de distribuição
Usando um ponto de distribuição como um servidor push
Outro trabalho de rotina
Gerenciamento de Servidores de Administração
Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário
Conexão a um Servidor de Administração e troca entre Servidores de Administração
Condições de conexão a um Servidor de Administração pela Internet

Conexão criptografado a um Servidor de Administração
Autenticar o Servidor de Administração quando um dispositivo for conectado
Autenticação do Servidor de Administração durante a conexão do Console de Administração
Configuração de uma lista de permissão de endereços IP para conexão ao Servidor de Administração
Usar o utilitário klscflag para fechar a porta 13291
Desconexão de um Servidor de Administração
Adição de um Servidor de Administração à árvore do console
Remoção de um Servidor de Administração da árvore do console
Adição de um Servidor de Administração virtual à árvore do console
Alteração de uma conta de serviço do Servidor de Administração. Utilitário klsrvswch
Alterando credenciais de DBMS
Resolução de problemas com nós do Servidor de Administração
Visualização e modificação das configurações de um Servidor de Administração
Ajuste das configurações gerais de um Servidor de Administração
Configurações de interface do Console de Administração
Processamento e armazenamento do evento no Servidor de Administração
Visualização do registro das conexões com o Servidor de Administração
Controle de ataques de vírus
Limitação de tráfego
Configuração do Servidor da Web
Trabalhar com usuários internos
Cópia backup e restauração das configurações do Servidor de Administração
Usar um instantâneo de sistema de arquivos para reduzir a duração do backup
Um dispositivo com o Servidor de Administração está inoperável
As configurações do Servidor de Administração ou o do banco de dados estão corrompidas
Cópia backup e restauração dos dados do Servidor de Administração
Tarefa de backup de dados do Servidor de Administração
Utilitário de backup de dados e recuperação (klbackup)
Backup de dados e recuperação no modo interativo
Backup de dados e recuperação no modo silencioso
Uso do utilitário klbackup para alterar dispositivos gerenciados sob gerenciamento de outro Servidor de Administração
Backup e restauração de dados do Servidor de Administração ao usar MySQL ou MariaDB
Mover Servidor de Administração para outro dispositivo
Evitar conflitos entre vários Servidores de Administração
Verificação em duas etapas
Sobre a verificação em duas etapas
Cenário: configurando a verificação em duas etapas para todos os usuários
Ativar a verificação em duas etapas para sua própria conta (baseado em MMC)
Ativar a verificação em duas etapas para todos os usuários (baseado em MMC)
Desativar a verificação em duas etapas para uma conta de usuário (baseado em MMC)
Desativar a verificação em duas etapas obrigatória para todos os usuários (baseado em MMC)
Excluir contas da verificação em duas etapas (baseado em MMC)
Editar o nome de um emissor do código de segurança (baseado em MMC)
Configurar a verificação em duas etapas para sua própria conta (baseado em MMC)
Alteração da pasta compartilhada do Servidor de Administração
Gerenciamento de grupos de administração

Criação de grupos de administração
Mover grupos de administração
Exclusão de grupos de administração
Criação automática de uma estrutura de grupos de administração
Instalação automática de aplicativos nos dispositivos em um grupo de administração
Gerenciamento de dispositivos cliente
Conectar dispositivos cliente ao Servidor de Administração
Conecte manualmente um dispositivo cliente ao Servidor de administração. Utilitário klmover
Conexão em túnel entre um dispositivo cliente e o Servidor de Administração
Conexão remota à Área de trabalho de um dispositivo cliente
Conectar-se a dispositivos clientes Windows
Conectar-se a dispositivos clientes macOS
Conexão com dispositivos cliente através do Windows Desktop Sharing
Configurar o reinício de um dispositivo cliente
Auditar ações em um dispositivo cliente remoto
Verificar a conexão entre um dispositivo cliente e o Servidor de Administração
Verificar automaticamente a conexão entre um dispositivo cliente e o Servidor de Administração
Verificar manualmente a conexão entre um dispositivo cliente e o Servidor de Administração. Utilitário klnagchk
Sobre verificar o tempo de conexão entre um dispositivo e o Servidor de Administração
Identificação de dispositivos cliente no Servidor de Administração
Mover dispositivos para um grupo de administração
Alterar o Servidor de Administração para dispositivos clientes
Migração de dispositivos conectados com o Servidor de Administração por meio de gateways de conexão para outro Servidor de Administração
Grupamentos e matrizes de servidores
Ativar, desativar e reiniciar remotamente dispositivos clientes
Sobre o uso da conexão contínua entre um dispositivo gerenciado e o Servidor de Administração
Sobre a sincronização forçada
Sobre o agendador de conexão
Enviar mensagens aos usuários de dispositivos
Gerenciar o Kaspersky Security for Virtualization
Configurar a alternância dos status do dispositivo
Atribuindo tags a dispositivos e visualizando tags atribuídas
Identificação automática do dispositivo
Exibir e configurar tags atribuídas a um dispositivo
Diagnóstico remoto de dispositivos cliente. Utilitário de diagnóstico remoto do Kaspersky Security Center
Conexão do utilitário de diagnóstico remoto com dispositivo cliente
Gerar um arquivo de dump para um aplicativo
Ativação e desativação de rastreio, download de arquivos de rastreio
Download das configurações do aplicativo
Download de registros de eventos
Download de múltiplos itens de informações de diagnóstico
Início do diagnóstico e download dos resultados
Início, interrupção e reinício de aplicativos
Dispositivos de proteção UEFI
Configurações de um dispositivo gerenciado
Configurações da política gerais

- Configurações de política do Agente de Rede
- Como gerenciar contas de usuário
  - Trabalhando com contas de usuário
  - Adicionar uma conta de usuário interno
  - Editar uma conta de usuário interno
  - Alterar o número permitido de tentativas de entrada de senha
  - Configurar a verificação do nome de um usuário interno quanto a singularidade
  - Adicionar um grupo de segurança
  - Adicionando um usuário a um grupo
  - Configurar direitos de acesso aos recursos do aplicativo. Controle de acesso baseado em função
    - Direitos de acesso ao Servidor de Administração e seus objetos
    - Direitos de acesso aos recursos do aplicativo
    - Funções de usuário predefinidas
    - Adicionar uma função de usuário
    - Atribuição de uma função a um usuário ou grupo de segurança
    - Atribuir permissões a usuários e grupos
    - Propagando funções de usuário aos Servidores de Administração secundários
  - Atribuindo o usuário como proprietário de dispositivo
  - Enviar mensagens a utilizadores
  - Visualizar a lista de dispositivos móveis de usuários
  - Instalar um certificado de um usuário
  - Visualizar a lista de certificados emitidos a um usuário
  - Sobre o administrador de um Servidor de Administração virtual
- Instalação remota de sistemas operacionais e aplicativos
  - Criação de imagens de sistemas operacionais
  - Imagens de instalação de sistemas operacionais
  - Configurar endereço de servidor proxy da KSN
  - Adição de drivers ao Windows Preinstallation Environment (WinPE)
  - Adição de drivers a um pacote de instalação com uma imagem de sistema operacional
  - Configuração do utilitário sysprep.exe
  - Implementação de sistemas operacionais em novos dispositivos na rede
  - Implementação de sistemas operacionais em dispositivos cliente
  - Criação de pacotes de instalação de aplicativos
  - Emitindo um certificado para pacotes de instalação de aplicativos
  - Instalar aplicativos em dispositivos cliente
- Gerenciar revisões de objeto
  - Exibir a seção de Histórico de revisão
  - Comparar revisões de objeto
  - Configurar o prazo de armazenamento das revisões de objeto e das informações de objeto excluídas
  - Exibir uma revisão de objeto
  - Salvar uma revisão do objeto em um arquivo
  - Reverter modificações
  - Adicionar uma descrição da revisão
- Exclusão de objetos
  - Excluir um objeto
  - Exibir informações sobre objetos excluídos
  - Excluir objetos permanentemente da lista de objetos excluídos

Gerenciamento de Dispositivos Móveis
- Cenário: Implementação do Gerenciamento de Dispositivos Móveis
- Sobre a política de grupo para gerenciar dispositivos EAS e MDM do iOS
- Ativar o Gerenciamento de Dispositivos Móveis
- Modificar as configurações de Gerenciamento de Dispositivos Móveis
- Desativar o Gerenciamento de Dispositivos Móveis
- Trabalhar com comandos para dispositivos móveis
  - Comandos para gerenciamento de dispositivos móveis
  - Usar o Firebase Cloud Messaging
  - Enviar comandos
  - Visualização do status de comandos no registro de comandos
- Trabalhar com certificados de dispositivos móveis
  - Iniciar o Assistente de instalação de certificados
  - Etapa 1. Selecionando o tipo de certificado
  - Etapa 2. Selecionando o tipo de dispositivo
  - Etapa 3. Seleção de um usuário
  - Etapa 4. Selecionando a origem do certificado
  - Etapa 5. Atribuindo uma tag ao certificado
  - Etapa 6. Especificando as configurações de publicação de certificado
  - Etapa 7. Selecionando um método de notificação ao usuário
  - Etapa 8. Geração do certificado
  - Configurar as regras de emissão do certificado
  - Integração com a infraestrutura de chaves públicas
  - Ativar o suporte de Kerberos Constrained Delegation
- Adicionando dispositivos móveis iOS na lista de dispositivos gerenciados
- Adicionando dispositivos móveis Android na lista de dispositivos gerenciados
- Gerenciamento de dispositivos móveis Exchange ActiveSync
  - Adicionar um perfil de gerenciamento
  - Remover um perfil de gerenciamento
  - Tratar as políticas do Exchange ActiveSync
  - Configurar o escopo da verificação
  - Trabalhar com dispositivos EAS
  - Exibir informações sobre um dispositivo EAS
  - Desconectar um dispositivo EAS do gerenciamento
  - Direitos do usuário para gerenciar dispositivos móveis Exchange ActiveSync
- Gerenciamento de dispositivos MDM do iOS
  - Assinando um perfil MDM do iOS por um certificado
  - Adicionar um perfil de configuração
  - Instalar um perfil de configuração no um dispositivo
  - Remover o perfil de configuração de um dispositivo
  - Adicionar um novo dispositivo ao publicar um link a um perfil
  - Adicionar um novo dispositivo através da instalação do perfil pelo administrador
  - Adicionar um perfil de provisionamento
  - Instalar um perfil de provisionamento em um dispositivo
  - Remover um perfil de provisionamento de um dispositivo
  - Adicionar um aplicativo gerenciado
  - Instalar um aplicativo em um dispositivo móvel

Remover um aplicativo de um dispositivo
Configurar o roaming em um dispositivo móvel MDM do iOS
Exibir informações sobre um dispositivo MDM do iOS
Desconectar um dispositivo MDM do iOS do gerenciamento
Enviar comandos para um dispositivo
Verificar o status de execução de comandos enviados
Gerenciar dispositivos KES
Criar um pacote de aplicativo móvel para dispositivos KES
Ativar a autenticação baseada em certificado de dispositivos do KES
Visualizar informações sobre um dispositivo KES
Desconectar um dispositivo KES do gerenciamento
Criptografia e proteção de dados
Visualização da lista de dispositivos criptografados
Visualização da lista de eventos de criptografia
Exportação da lista de eventos de criptografia para um arquivo de texto
Criação e visualização de relatórios de criptografia
Transmitindo as chave de criptografia entre Servidores de Administração
Repositórios de dados
Exportação de uma lista de objetos no repositório para um arquivo de texto
Pacotes de instalação
Status principais de arquivos no repositório
Acionamento de regras no modo de Treinamento inteligente
Exibir a lista de detecções executadas usando regras do Controle Adaptativo de Anomalias
Adicionar exclusões a partir das regras do Controle Adaptativo de Anomalias
Etapa 1. Selecionar o aplicativo
Etapa 2. Selecionar a política (políticas)
Etapa 3. Processamento da política (políticas)
Quarentena e Backup
Ativar o gerenciamento remoto para arquivos nos repositórios
Visualização de propriedades de um arquivo colocado no repositório
Excluir os arquivos dos repositórios
Restaurar arquivos dos repositórios
Salvar um arquivo dos repositórios para o disco
Verificação de arquivos em Quarentena
Ameaças ativas
Desinfeção de um arquivo não processado
Salvar um arquivo não processado no disco
Para excluir um arquivo da pasta "Ameaças ativas"
Kaspersky Security Network (KSN)
Sobre a KSN
Configurar acesso ao Kaspersky Security Network
Ativar e desativar a KSN
Visualizando a Declaração da KSN aceita
Visualizar as estatísticas do Servidor Proxy KSN
Aceitando uma declaração da KSN atualizada
Proteção avançada com a Kaspersky Security Network
Verificar se o ponto de distribuição funciona como servidor proxy da KSN

Alternando entre Ajuda On-line e Ajuda Offline
Exportação de eventos para os sistemas SIEM
Configuração da exportação de eventos para sistemas SIEM
Antes de iniciar
Sobre eventos no Kaspersky Security Center
Sobre a exportação de evento
Sobre a configuração de exportação de eventos em um sistema SIEM
Marcando eventos para exportação para sistemas SIEM em formato Syslog
Sobre a marcação de eventos para exportação para o sistema SIEM no formato Syslog
Marcando eventos de um aplicativo Kaspersky para exportação em formato Syslog
Marcando eventos gerais para exportação no formato Syslog
Sobre a exportação de eventos usando o formato Syslog
Sobre a exportação de eventos usando formatos CEF e LEEF
Conversão de eventos para o formato CEF ou LEEF
Configurando o Kaspersky Security Center para exportação de eventos para o sistema SIEM
Exportando eventos diretamente do banco de dados
Executar uma consulta SQL usando o utilitário klsql2
Exemplo de uma consulta SQL no utilitário klsql2
Exibir o nome de banco de dados do Kaspersky Security Center
Exibir os resultados da exportação
Usando SNMP para enviar estatísticas para aplicativos de terceiros
Configuração do serviço SNMP para uso com o Kaspersky Security Center
Agente SNMP e identificadores de objetos
Obtendo uma string do nome de contador de um identificador de objeto
Valores de identificadores de objetos para SNMP
Solução de problemas
Trabalhando em um ambiente nuvem
Sobre o trabalho em um ambiente de nuvem
Cenário: implementação para o ambiente em nuvem
Prerrequisitos para implementar o Kaspersky Security Center em um ambiente de nuvem
Requisitos de hardware para o Servidor de Administração no ambiente de nuvem
Opções de licenciamento em um ambiente em nuvem
Opções de banco de dados para trabalhar em um ambiente de nuvem
Trabalhando no ambiente de nuvem Amazon Web Services
Sobre o trabalho no ambiente na nuvem de Amazon Web Services
Criar funções do IAM e contas de Usuário do IAM para instâncias do Amazon EC2
Assegurar que o Servidor de Administração do Kaspersky Security Center tenha as permissões para trabalhar com AWS
Criar uma função do IAM para o Servidor de Administração
Criar uma conta de Usuário do IAM para uso com o Kaspersky Security Center
Criar uma função do IAM para a instalação de aplicativos em instâncias do Amazon EC2
Trabalhar com Amazon RDS
Criar uma instância Amazon RDS
Criar grupo de opções para instância do Amazon RDS
Modificar o grupo de opções
Modificar permissões para função do IAM para instância de banco de dados do Amazon RDS
Preparar o Amazon S3 bucket para o banco de dados

Migrar o banco de dados para o Amazon RDS
Trabalhando no ambiente de nuvem Microsoft Azure
Sobre o trabalho em o Microsoft Azure
Criar uma assinatura, ID do aplicativo e senha
Atribuir uma função ao ID do aplicativo Azure
Implementar o Servidor de Administração no Microsoft Azure e selecionar banco de dados
Trabalhar com Azure SQL
Criar uma conta de armazenamento Azure
Criar um banco de dados Azure SQL e um servidor SQL
Migrar o banco de dados para Azure SQL
Trabalhando no Google Cloud
Criar o e-mail do cliente, ID do projeto e chave privada
Trabalhar com o Google Cloud SQL para instância do MySQL
Prerrequisitos para os dispositivos cliente no um ambiente de nuvem necessários para uso com o Kaspersky Security Center
Criação de pacotes de instalação necessários para configurar o ambiente em nuvem
Configuração do ambiente em nuvem
Sobre o assistente Configurar o ambiente em nuvem
Etapa 1. Selecionando o método de ativação do aplicativo
Etapa 2. Selecionar o ambiente de nuvem
Etapa 3. Autorização no ambiente de nuvem
Etapa 4. Configurar a sincronização com a nuvem e selecionar ações adicionais
Etapa 5. Configurando o Kaspersky Security Network para o ambiente de nuvem
Etapa 6. Configurando notificações de e-mail no ambiente de nuvem
Etapa 7. Criando uma configuração inicial de proteção do ambiente de nuvem
Etapa 8. Selecione a ação quando o sistema operacional deve ser reiniciado durante a instalação (para o ambiente de nuvem)
Etapa 9. Receber atualizações por o Servidor de Administração
Configurar a verificação
Grupo de dispositivos Nuvem
Sondagem do segmento de rede
Adicionar conexões para a sondagem do segmento da nuvem
Excluir conexões da sondagem do segmento da nuvem
Configurar o agendamento da sondagem
Instalar aplicativos em dispositivos no ambiente de nuvem
Exibir as propriedades de dispositivos de nuvem
Sincronização com o nuvem
Implementação do Kaspersky Security Center no Yandex.Cloud
Apêndices
Recursos avançados
Automação de operação do Kaspersky Security Center. Utilitário klakaut
Ferramentas personalizadas
Modo de clonagem do disco do Agente de Rede
Preparando um dispositivo de referência com o Agente de Rede instalado para criar uma imagem do sistema operacional
Para configurar o recebimento de mensagens do Monitor de integridade do arquivo
Manutenção do Servidor de Administração
Acesso aos servidores DNS públicos

Janela Método de notificação ao usuário
Seção Geral
Janela Seleção de dispositivos
Definir o nome da janela de novo objeto
Seção Categorias de aplicativos
Recursos de uso da interface de gerenciamento
Árvore do console
Como atualizar dados no espaço de trabalho
Como navegar na árvore do console
Como abrir a janela de propriedades do objeto no espaço de trabalho
Como selecionar um grupo de objetos no espaço de trabalho
Como alterar o conjunto de colunas no espaço de trabalho
Informações de referência
Comandos no menu de contexto
Lista de dispositivos gerenciados. Descrição das colunas
Status de dispositivos, tarefas e políticas
Ícones de status do arquivo no Console de Administração
Pesquisar e exportar dados
Dispositivos encontrados
Configurações de pesquisa de dispositivo
Usar máscaras para variáveis de sequência
Usar expressões regulares no campo de pesquisa
Exportar listas a partir de caixas de diálogo
Configurações de tarefas
Configurações de tarefa gerais
Baixar atualizações nas configurações da tarefa do repositório do Servidor de Administração
As configurações da tarefa Baixar atualizações para os repositórios de pontos de distribuição
As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias
Configurações de tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades
Lista de sub-redes globais
Adicionar sub-redes à lista global de sub-redes
Visualização e modificação das propriedades de sub-redes na lista global de sub-redes
Uso do Agente de Rede para Windows, macOS e Linux: comparativo
Comparativo entre configurações de Agente de Rede por sistemas operacionais
Kaspersky Security Center Web Console
Sobre o Kaspersky Security Center Web Console
Requisitos de hardware e software para o Kaspersky Security Center Web Console
Diagrama de implementação do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center Web Console
Portas usadas pelo Kaspersky Security Center Web Console
Cenário: instalação e configuração inicial do Kaspersky Security Center Web Console
Instalação
Instalar o Kaspersky Security Center Web Console
Instalação do Kaspersky Security Center Web Console em plataformas Linux
Instalar o Kaspersky Security Center Web Console em plataformas Linux
Parâmetros de instalação do Kaspersky Security Center Web Console

Instalação do Kaspersky Security Center Web Console conectado ao Servidor de Administração instalado nos nós do cluster de failover
Atualizar o Kaspersky Security Center Web Console
Certificados para trabalhar com o Kaspersky Security Center Web Console
Substituir o certificado do Kaspersky Security Center Web Console
Especificar certificados para Servidores de Administração confiáveis no Kaspersky Security Center Web Console
Converter um certificado PFX para o formato PEM
Migração do Kaspersky Security Center Windows
Migração para o Kaspersky Security Center Cloud Console
Migração para o Kaspersky Next XDR Expert
Migração para o Kaspersky Security Center Linux
Migração para o Kaspersky Security Center Linux pelo Assistente de migração
Exportação de objetos de grupo a partir do Kaspersky Security Center Windows
Importação do arquivo de exportação no Kaspersky Security Center Linux
Alternância entre dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux
Migração para o Kaspersky Security Center Linux com o uso do backup de dados do Servidor de Administração
Login no Kaspersky Security Center Web Console e logout
Gerenciador de Identidade e Acesso no Kaspersky Security Center Web Console
Sobre o Gerenciador de Identidade e Acesso
Ativando o Gerenciador de Identidade e Acesso: cenário
Configurando o Gerenciador de Identidade e Acesso no Kaspersky Security Center Web Console
Registrar o aplicativo Kaspersky Industrial CyberSecurity for Networks no Kaspersky Security Center Web Console
Tempo de vida útil de tokens e tempo limite de autorização para Gerenciador de Identidade e Acesso
Baixando e distribuindo os certificados IAM
Desativando o Gerenciador de Identidade e Acesso
Configurando a autenticação de domínio usando os protocolos NTLM e Kerberos
Configurando o Servidor de Administração
Configuração da conexão do Kaspersky Security Center Web Console ao Servidor de Administração
Configuração do registro em log de eventos de conexão do Servidor de Administração
Definição das configurações de acesso à Internet para o Servidor de Administração
Configuração do número máximo de eventos no repositório de eventos
Configurações de conexão de dispositivos de proteção UEFI
Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário
Visualizar a lista de Servidores de administração secundários
Excluir uma hierarquia de Servidores de Administração
Manutenção do Servidor de Administração
Configurar interface
Gerenciar Servidores de Administração virtuais
Criar um Servidor de Administração virtual
Ativando ou desativando um Servidor de Administração virtual
Atribuição de um administrador para um Servidor de Administração virtual
Alterar o Servidor de Administração para dispositivos clientes
Excluindo um Servidor de Administração virtual
Ativando a proteção da conta contra modificações não autorizadas
Verificação em duas etapas
Sobre a verificação em duas etapas
Configuração da verificação em duas etapas para todos os usuários

Ativar a verificação em duas etapas para sua própria conta (Web Console)
Ativar a verificação em duas etapas obrigatória para todos os usuários (Web Console)
Desativar a verificação em duas etapas para uma conta de usuário (Web Console)
Desativar a verificação obrigatória em duas etapas para todos os usuários (Web Console)
Excluindo contas da verificação em duas etapas
Gerando uma nova chave secreta
Editar o nome de um emissor do código de segurança (Web Console)
Configurar a verificação em duas etapas para sua própria conta (Web Console)
Cópia backup e restauração dos dados do Servidor de Administração
Reemissão do certificado do Kaspersky Security Center Web Console
Criação de uma tarefa de backup de dados
Mover Servidor de Administração para outro dispositivo
Verificar a integridade dos módulos usando os utilitários klscmodchk e integrity_checker
Instalação e configuração inicial do Kaspersky Security Center Web Console
Assistente de início rápido (Kaspersky Security Center Web Console)
Etapa 1. Especificando as configurações de conexão da Internet
Etapa 2. Download das atualizações necessárias
Etapa 3. Seleção dos ativos a serem protegidos
Etapa 4. Selecionar a criptografia em soluções
Etapa 5. Configurar a instalação dos plugins para os aplicativos gerenciados
Etapa 6. Baixando os pacote de distribuição e criando pacotes de instalação
Etapa 7. Configurar a Kaspersky Security Network
Etapa 8. Selecionando o método de ativação do aplicativo
Etapa 9. Especificar as configurações de gerenciamento de atualização de terceiros
Etapa 10. Criar uma configuração básica de proteção de rede
Etapa 11. Configurar notificações por e-mail
Etapa 12. Executar uma pesquisa de rede
Etapa 13. Fechar o Assistente de início rápido
Conectando dispositivos fora do escritório
Cenário: Conectando dispositivos externos por meio de um gateway de conexão
Cenário: conectando dispositivos ausentes do escritório por meio de um Servidor de Administração secundário na DMZ
Sobre a conexão de dispositivos externos
Conexão de dispositivos de desktop externos com o Servidor de Administração
Sobre a configuração de perfis de conexão para usuários ausentes
Criando um perfil de conexão para usuários ausentes
Sobre a mudança do Agente de Rede para outro servidor de Administração
Criar uma regra de troca do Agente de Rede por localização da rede
Assistente de implementação da proteção
Etapa 1. Iniciar o assistente de implementação da proteção
Etapa 2. Seleção do pacote de instalação
Etapa 3. Seleção de um método de distribuição de arquivo de chave ou código de ativação
Etapa 4. Seleção de versão do Agente de Rede
Etapa 5. Seleção de dispositivos
Etapa 6. Especificação das configurações de tarefa de instalação remota
Etapa 7. Gerenciamento de reinício
Etapa 8. Remoção de aplicativos incompatíveis antes de instalação
Etapa 9. Movimentação de dispositivos para dispositivos gerenciados

Etapa 10. Seleção de contas para acessar dispositivos
Etapa 11. Início da instalação
Implementação de aplicativos Kaspersky por meio do Kaspersky Security Center Web Console
Cenário: implementação de aplicativos Kaspersky por meio do Kaspersky Security Center Web Console
Aquisição de plugins para aplicativos Kaspersky
Download e criação de pacotes de instalação para aplicativos Kaspersky
Alteração do limite de tamanho dos dados de pacotes de instalação personalizada
Download de pacotes de distribuição para aplicativos Kaspersky
Verificando se o Kaspersky Endpoint Security foi implantado com sucesso
Criação do pacote de instalação independente
Visualizar a lista de pacotes de instalação independente
Criar pacotes de instalação personalizados
Distribuindo pacotes de instalação para Servidores de Administração secundários
Instalação de aplicativos usando a tarefa de instalação remota
Instalar um aplicativo remotamente
Instalar um aplicativo usando as políticas de grupo do Active Directory
Instalando aplicativos nos Servidores de Administração secundários
Especificando configurações para instalação remota em dispositivos Unix
Início e interrupção de aplicativos da Kaspersky
Gerenciamento de Dispositivos Móveis
Substituição de aplicativos de segurança de terceiros
Localizar dispositivos na rede
Cenário: Localizar dispositivos na rede
Localização dos dispositivos
Sondagem da rede do Windows
Sondagem do Active Directory
Sondagem do conjunto de IPs
Adição e modificação de um conjunto de IPs
Sondagem Zeroconf
Configuração de regras de retenção para dispositivos não atribuídos
Aplicativos Kaspersky: licenciamento e ativação
Licenciamento de aplicativos gerenciados
Adição de uma chave de licença ao repositório do Servidor de Administração
Implementando uma chave de licença para dispositivos clientes
Distribuição automática de uma chave de licença
Visualizando de informações sobre chaves de licença em uso
Remover uma chave de licença do repositório
Revogando o consentimento com um Contrato de Licença do Usuário Final
Renovando licenças para aplicativos da Kaspersky
Usando o Kaspersky Marketplace para escolher as soluções comerciais Kaspersky de sua preferência
Configuração da proteção da rede
Cenário: Configurar a proteção da rede
Sobre as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário
Configuração e propagação de políticas: abordagem centrada no dispositivo
Configuração e propagação de políticas: abordagem centrada no usuário
Configurações de política do Agente de Rede
Configuração manual da política do Kaspersky Endpoint Security

- Configurar a Kaspersky Security Network
- Verificação da lista das redes protegidas por Firewall
- Desativar a verificação de unidades de rede
- Excluir detalhes de software da memória do Servidor de Administração
- Configurar o acesso à interface do Kaspersky Endpoint Security for Windows em estações de trabalho
- Salvar eventos de política importantes no banco de dados do Servidor de Administração

Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security

Concedendo acesso offline ao dispositivo externo bloqueado pelo Controle de Dispositivos

Remover aplicativos ou atualizações de software remotamente

Reverter um objeto para uma revisão anterior

Tarefas

- Sobre as tarefas
- Sobre o escopo de tarefa
- Criar uma tarefa
- Como iniciar uma tarefa manualmente
- Visualizando a lista de tarefas
- Configurações de tarefa gerais
- Exportação de tarefa
- Importação de uma tarefa
- Iniciar o Assistente para alterar a senha das tarefas
  - Etapa 1. Especificar as credenciais
  - Etapa 2. Selecionar uma ação a ser executada
  - Etapa 3. Visualizar os resultados

Gerenciamento de dispositivos cliente

- Configurações de um dispositivo gerenciado
- Criação de grupos de administração
- Adicionar dispositivos manualmente a um grupo de administração
- Migrando dispositivos manualmente para um grupo de administração
- Criar regras para mover dispositivos
- Copiar as regras para mover dispositivos
- Condições para migrar uma regra de um dispositivo
- Exibir e configurar as ações quando os dispositivos mostram inatividade
- Sobre os status do dispositivo
- Configurar a alternância dos status do dispositivo
- Conexão remota à Área de trabalho de um dispositivo cliente
- Conexão com dispositivos cliente através do Windows Desktop Sharing
- Seleções de dispositivos
  - Visualização da lista de dispositivos a partir de uma seleção de dispositivos
  - Criar uma seleção de dispositivos
  - Configurar uma seleção de dispositivos
  - Exportação da lista de dispositivos a partir de uma seleção de dispositivos
  - Remover os dispositivos de grupos de administração em uma seleção
- Tags de dispositivo
  - Tags de dispositivo
  - Criando uma tag de dispositivo
  - Renomeando uma tag de dispositivo
  - Excluindo uma tag de dispositivo

Visualizando dispositivos aos quais uma tag está atribuída
Visualizando as tags atribuídas a um dispositivo
Identificação de um dispositivo manualmente
Removendo uma tag atribuído de um dispositivo
Visualização de regras para identificar dispositivos automaticamente
Edição de uma regra para identificar dispositivos automaticamente
Criação de uma regra para identificar dispositivos automaticamente
Execução de regras para identificar dispositivos automaticamente
Exclusão de uma regra para identificar dispositivos automaticamente
Gerenciamento de tags de dispositivo usando o utilitário klscflag
Políticas e perfis da política
Sobre as políticas e perfis de política
Sobre as configurações de bloqueio e bloqueadas
Herança de políticas e perfis de política
Hierarquia de políticas
Perfis de política em uma hierarquia de políticas
Como as configurações são implementadas em um dispositivo gerenciado
Gerenciamento de políticas
Visualização da lista de políticas
Criação de uma política
Modificar uma política
Configurações da política gerais
Ativando o desativando uma opção de herança de política
Cópia de uma política
Mover uma política
Exportação de uma política
Importação de uma política
Visualizar o gráfico de status de distribuição da política
Exclusão de uma política
Gerenciando perfis de política
Visualização dos perfis de uma política
Alteração de uma prioridade de perfil da política
Criar um perfil da política
Modificar um perfil da política
Copiar um perfil de política
Criar uma regra de ativação do perfil da política
Excluir um perfil de política
Criptografia e proteção de dados
Visualização da lista de unidades criptografadas
Visualização da lista de eventos de criptografia
Criação e visualização de relatórios de criptografia
Concessão de acesso a uma unidade criptografada no modo offline
Usuários e funções dos usuários
Sobre as funções dos usuários
Exibição de contas de usuário e sessões
Configurar direitos de acesso aos recursos do aplicativo. Controle de acesso baseado em função
Direitos de acesso aos recursos do aplicativo

Funções de usuário predefinidas
Atribuição de direitos de acesso a objetos específicos
Atribuição de direitos de acesso a usuários e grupos de segurança
Adicionar uma conta de usuário interno
Criação de um grupo de segurança
Editar uma conta de usuário interno
Edição de um grupo de segurança
Adicionar as contas de usuário em um grupo interno
Atribuir um usuário como um proprietário de dispositivo
Excluir um usuário ou um grupo de segurança
Criar uma função de usuário
Editar uma função de usuário
Editar o escopo de uma função de usuário
Excluir uma função de usuário
Associação de perfis da política a funções
Propagando funções de usuário aos Servidores de Administração secundários
Gerenciar objetos no Kaspersky Security Center Web Console
Adicionar uma descrição da revisão
Exclusão de objetos
Kaspersky Security Network (KSN)
Sobre a KSN
Configurar o acesso à KSN
Ativar e desativar a KSN
Visualizando a Declaração da KSN aceita
Aceitando uma declaração da KSN atualizada
Verificar se o ponto de distribuição funciona como servidor proxy da KSN
Atualização dos bancos de dados e dos aplicativos da Kaspersky
Cenário: Atualização regular dos bancos de dados e dos aplicativos Kaspersky
Sobre atualização de bancos de dados, módulos de software e aplicativos da Kaspersky
Criação da tarefa baixar atualizações no repositório do Servidor de Administração
Verificação das atualizações baixadas
Criar as atualizações de download para a tarefa dos repositórios dos pontos de distribuição
Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center
Instalação automática de atualizações para o Kaspersky Endpoint Security for Windows
Aprovar e recusar atualizações de software
Atualizando o Servidor de Administração
Ativar e desativar o modelo offline de download da atualização
Atualização de bancos de dados e módulos de software da Kaspersky em dispositivos offline
Fazendo backup e restaurando plug-ins da web
Ajuste de pontos de distribuição e gateways de conexão
Configuração padrão de pontos de distribuição: escritório único
Configuração padrão de pontos de distribuição: múltiplos pequenos escritórios remotos
Sobre os pontos de distribuição atribuídos
Atribuir os pontos de distribuição automaticamente
Atribuir os pontos de distribuição manualmente
Modificar a lista de pontos de distribuição para um grupo de administração
Sincronização forçada

Ativando um servidor push
Gerenciar aplicativos de terceiros em dispositivos cliente
Sobre aplicativos de terceiros
Instalar atualizações de software de terceiros
Instalar atualizações de software de terceiros
Criar a tarefa Encontrar vulnerabilidades e atualizações necessárias
As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias
Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades
Adicionar regras para instalação da atualização
Criar a tarefa Instalar atualizações do Windows Update
Exibir informações sobre atualizações disponíveis para software de terceiros
Exportando a lista de vulnerabilidades de software para um arquivo
Aprovando e recusando atualizações de software de terceiros
Criação da tarefa Executar a sincronização do Windows Update
Atualizar aplicativos de terceiros automaticamente
Cenário: Atualizando software de terceiros
Corrigindo vulnerabilidades de software de terceiros
Cenário: Encontrar e corrigir vulnerabilidades de software de terceiros
Sobre como encontrar e corrigir vulnerabilidades de software
Corrigindo vulnerabilidades de software de terceiros
Criar a tarefa Corrigir vulnerabilidades
Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades
Adicionar regras para instalação da atualização
Selecionar as correções do usuário para vulnerabilidades em software de terceiros
Visualizar informações sobre vulnerabilidades de software detectadas em todos os dispositivos gerenciados
Visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado
Visualizar as estatísticas de vulnerabilidades em dispositivos gerenciados
Exportar a lista de vulnerabilidades de software para um arquivo
Ignorar as vulnerabilidades de software
Gerenciando a execução de aplicativos em dispositivos cliente
Usar o Controle de Aplicativos para gerenciar arquivos executáveis
Modos e categorias do Controle de Aplicativos
Obter e visualizar uma lista de aplicativos instalados nos dispositivos clientes
Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos clientes
Criar uma categoria de aplicativos com conteúdo adicionado manualmente
Criar uma categoria de aplicativo que inclua arquivos executáveis dos dispositivos selecionados
Criar uma categoria de aplicativo que inclua arquivos executáveis da pasta selecionada
Visualizando a lista de categorias de aplicativo
Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows
Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos
Criação de um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky
Ver e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky
Configurações do pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky
Tags de aplicativo
Criando uma tag de aplicativo
Renomeando uma tag de aplicativo

- Atribuindo uma tag de aplicativos
- Removendo tags atribuídas de um aplicativo
- Excluir uma tag de aplicativos

Monitoramento e relatórios

- Cenário: Monitoramento e relatórios
- Sobre os tipos do monitoramento e relatórios
- Painel e widgets
  - Usar o painel
  - Adição de widgets ao painel
  - Ocultação de um widget do painel
  - Movimentação de um widget no painel
  - Alteração do tamanho ou da aparência do widget
  - Alteração das configurações do widget
  - Sobre o modo somente painel
  - Configurando o modo somente painel
- Relatórios
  - Usar os relatórios
  - Criação de um modelo de relatório
  - Visualização e edição das propriedades do modelo de relatório
  - Exportar um relatório para um arquivo
  - Como gerar e visualizar um relatório
  - Criação de uma tarefa de entrega de relatório
  - Excluir os modelos de relatório
- Eventos e seleções de eventos
  - Sobre os eventos do Kaspersky Security Center
  - Usar as seleções de eventos
    - Criar uma seleção de eventos
    - Editar uma seleção de eventos
    - Visualizando uma lista de uma seleção de eventos
    - Excluir as seleções de eventos
  - Visualização dos detalhes de um evento
  - Exportar eventos para um arquivo
  - Exportando eventos para os sistemas SIEM
    - Configuração da exportação de eventos para sistemas SIEM
    - Antes de iniciar
    - Sobre a exportação de evento
    - Sobre a configuração de exportação de eventos em um sistema SIEM
    - Marcando eventos para exportação para sistemas SIEM em formato Syslog
      - Sobre a marcação de eventos para exportação para o sistema SIEM no formato Syslog
      - Marcando eventos de um aplicativo da Kaspersky para exportação em formato Syslog
      - Marcando eventos gerais para exportação no formato Syslog
    - Sobre a exportação de eventos usando formatos CEF e LEEF
    - Sobre a exportação de eventos usando o formato Syslog
    - Configurando o Kaspersky Security Center para exportação de eventos para o sistema SIEM
    - Exportando eventos diretamente do banco de dados
      - Executar uma consulta SQL usando o utilitário klsql2
      - Exemplo de uma consulta SQL no utilitário klsql2

Exibir o nome de banco de dados do Kaspersky Security Center
Exibir os resultados da exportação
Visualização de um histórico de eventos a partir de um evento
Excluir os eventos
Configuração do termo de armazenamento de um evento
Eventos dos componentes do Kaspersky Security Center
Estrutura de dados da descrição do tipo de evento
Eventos do Servidor de Administração
Eventos críticos do Servidor de Administração
Eventos de falha funcional do Servidor de Administração
Eventos de aviso do Servidor de Administração
Eventos informativos do Servidor de Administração
Eventos do Agente de Rede
Eventos de falha funcional do Agente de Rede
Eventos de aviso do Agente de Rede
Eventos informativos do Agente de Rede
Eventos do Servidor de MDM do iOS
Eventos de falha funcional do Servidor de MDM do iOS
Eventos de aviso do Servidor de MDM do iOS
Eventos informativos do Servidor de MDM do iOS
Eventos do Servidor de dispositivos móveis Microsoft Exchange
Eventos de falha funcional do Servidor de dispositivos móveis Exchange
Eventos informativos do Servidor de dispositivos móveis Exchange
Bloqueio de eventos frequentes
Sobre o bloqueio de eventos frequentes
Gerenciando o bloqueio de eventos frequentes
Removendo o bloqueio de eventos frequentes
Recebendo eventos do Kaspersky Security for Microsoft Exchange Servers
Notificações e status do dispositivo
Usar as notificações
Visualização de notificações na tela
Sobre os status do dispositivo
Configurar a alternância dos status do dispositivo
Configurar a entrega de notificações
Notificações de evento exibidas executando um arquivo executável
Novidades da Kaspersky
Sobre as Novidades Kaspersky
Especificando configurações para receber as Novidades Kaspersky
Desativando o recebimento de Novidades Kaspersky
Visualizando informações sobre detecção de ameaças
Baixando e excluindo arquivos da quarentena e backup
Baixando arquivos da quarentena e backup
Registro da atividade do Kaspersky Security Center Web Console
Integração entre o Kaspersky Security Center e outras soluções
Configurar o acesso ao Console da Web KATA / KEDR
Estabelecendo uma conexão em segundo plano
Trabalhar com o Kaspersky Security Center Web Console em um ambiente de nuvem

Configuração de ambiente em nuvem no Kaspersky Security Center Web Console
Etapa 1. Verificação dos plug-ins e pacotes de instalação necessários
Etapa 2. Licenciar o aplicativo
Etapa 3. Seleção do ambiente em nuvem e autorização
Etapa 4. Amostragem de segmentos, configuração da sincronização com a Nuvem e seleção de ações adicionais
Etapa 5. Seleção de um aplicativo para criar uma política e tarefas
Etapa 6. Configurar o Kaspersky Security Network para o Kaspersky Security Center
Etapa 7. Criar uma configuração inicial de proteção
Amostragem do segmento de rede por meio do Kaspersky Security Center Web Console
Adicionar conexões para a sondagem do segmento da nuvem
Excluindo uma conexão para sondagem do segmento da nuvem
Configurar o agendamento da amostragem por meio do Kaspersky Security Center Web Console
Visualizar os resultados da amostragem de segmentos da nuvem por meio do Kaspersky Security Center Web Console
Visualizar as propriedades dos dispositivos na nuvem por meio do Kaspersky Security Center Web Console
Sincronização com a nuvem: configuração da regra móvel
Instalação remota de aplicativos nas máquinas virtuais do Azure
Criação da tarefa de Backup dos dados do Servidor de Administração usando um DBMS na nuvem
Diagnóstico remoto de dispositivos cliente
Abertura da janela de diagnóstico remoto
Ativação e desativação do rastreamento para aplicativos
Download de arquivos de rastreamento de um aplicativo
Exclusão de arquivos de rastreamento
Download das configurações do aplicativo
Download de registros de eventos
Início, interrupção e reinício do aplicativo
Execução do diagnóstico remoto do Agente de Rede do Kaspersky Security Center e download dos resultados
Execução de um aplicativo em um dispositivo cliente
Gerar um arquivo de dump para um aplicativo
Alteração do idioma da interface do Kaspersky Security Center Web Console
Guia de referência de API
Práticas recomendadas para Provedores de Serviços
Planejar a implementação do Kaspersky Security Center
Fornecer acesso à Internet ao Servidor de Administração
Configuração padrão do Kaspersky Security Center
Sobre os pontos de distribuição
Hierarquia de Servidores de Administração
Servidores de Administração virtual
Gerenciar dispositivos móveis com o Kaspersky Endpoint Security for Android
Implementação e configuração inicial
Recomendações sobre a instalação do Servidor de Administração
Criar contas para os serviços do Servidor de Administração em um cluster para falhas
Selecionar um DBMS
Especificar o endereço do Servidor de Administração
Configurar a proteção em uma rede da organização cliente
Configuração manual da política do Kaspersky Endpoint Security
Configurar a política na seção Proteção Avançada Contra Ameaças
Configurar a política na seção Proteção Essencial Contra Ameaças

Configurar a política na seção Configurações Gerais
Configurando a política na seção Configuração de eventos
Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security
Configuração manual da tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security
Agendar a tarefa Encontrar vulnerabilidades e atualizações necessárias
Configuração manual da tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades
Criação de uma estrutura de grupos de administração e atribuir pontos de distribuição
Configuração de cliente MSP padrão: escritório único
Configuração de cliente MSP padrão: múltiplos pequenos escritórios remotos
Hierarquia de políticas, usando perfis de política
Hierarquia de políticas
Perfis da política
Tarefas
Regras de migração de dispositivos
Categorização de software
Sobre os aplicativos para múltiplos usuários
Cópia backup e restauração das configurações do Servidor de Administração
Um dispositivo com o Servidor de Administração está inoperável
As configurações do Servidor de Administração ou o do banco de dados estão corrompidas
Implementar o Agente de Rede e o aplicativo de segurança
Implementação inicial
Configurar os instaladores
Pacotes de instalação
Propriedades MSI e arquivos de transformação
Implementação com ferramentas de terceiros para a instalação remota de aplicativos
Informação geral sobre as tarefas de instalação remotas no Kaspersky Security Center
Implementar usando políticas de grupo do Microsoft Windows
Implementação forçada através da tarefa de instalação remota do Kaspersky Security Center
Executar pacotes independentes criados pelo Kaspersky Security Center
Opções para a instalação manual de aplicativos
Como criar um arquivo MST
Instalação remota de aplicativos em dispositivos com o Agente de Rede instalado
O gerenciamento do dispositivo reinicia na tarefa de instalação remota
Adequabilidade da atualização dos bancos de dados em um pacote de instalação de um aplicativo de antivírus
Removendo aplicativos de segurança de terceiros incompatíveis
Remoção do Agente de Rede protegido por senha usando o prompt de comando
Usar as ferramentas da instalação remota de aplicativos no Kaspersky Security Center para executar arquivos executáveis relevantes em dispositivos gerenciados
Monitorar a implementação
Configurar os instaladores
Informações gerais
Instalação em modo silencioso (com um arquivo de resposta)
Instalação do Agente de Rede no modo silencioso (sem um arquivo de resposta)
Configuração de instalação parcial através de setup.exe
Parâmetros de instalação do Servidor de Administração
Parâmetros de instalação do Agente de Rede
Infraestrutura virtual

Dicas sobre como reduzir a carga em máquinas virtuais
Suporte de máquinas virtuais dinâmicas
Suporte para copiar máquinas virtuais
O suporte do sistema de arquivos reverte para dispositivos com o Agente de Rede
Sobre a configuração de perfis de conexão para usuários ausentes
Implementar o recurso de Gerenciamento de dispositivos móveis
Conectar dispositivos KES ao Servidor de Administração
Conexão direta de dispositivos ao Servidor de Administração
Esquema para conectar dispositivos KES ao servidor envolvendo a delegação de restrição Kerberos (KCD)
Usar o Firebase Cloud Messaging
Integração com a infraestrutura de chaves públicas
Servidor Web do Kaspersky Security Center
Outro trabalho de rotina
Monitorando as luzes de tráfego e os eventos registrados no Console de Administração
Acesso remoto aos dispositivos gerenciados
Uso da opção "Não desconectar do Servidor de Administração" para fornecer conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração
Sobre verificar o tempo de conexão entre um dispositivo e o Servidor de Administração
Sobre a sincronização forçada
Sobre tunelamento
Guia de dimensionamento
Sobre este Guia
Informações sobre as limitações do Kaspersky Security Center
Cálculos para os Servidores de Administração
Cálculo de recursos de hardware para o Servidor de Administração
Requisitos de hardware para o DBMS e para o Servidor de Administração
Cálculo do espaço do banco de dados
Cálculo de espaço em disco (sem e com o uso do recursos de Gerenciamento de vulnerabilidade e de correção)
Cálculo do número e configuração de Servidores de Administração
Recomendações para conectar máquinas virtuais dinâmicas ao Kaspersky Security Center
Cálculos para pontos de distribuição e gateways de conexão
Requisitos para um ponto de distribuição
Calcular o número e a configuração de pontos de distribuição
Cálculo do número de gateways de conexão
Registro de informações sobre eventos de tarefas e políticas
Considerações específicas e configurações ótimas de determinadas tarefas
Frequência da descoberta de dispositivos
Tarefa de backup de dados do Servidor de Administração e tarefa de manutenção do Servidor de Administração
Tarefas de grupo para atualizar o Kaspersky Endpoint Security
Tarefa de inventário
Detalhes da carga da rede espalhada entre o Servidor de Administração e os dispositivos protegidos
Consumo de tráfego sob diversos cenários
Uso de tráfego médio durante 24 horas
Contatar o Suporte Técnico
Como obter suporte técnico
Suporte técnico via Kaspersky CompanyAccount
Obter arquivos de dump do Servidor de Administração

Fontes de informação sobre o aplicativo
Glossário
Administrador cliente
Administrador do Kaspersky Security Center
Administrador do provedor de serviço
Agente de autenticação
Agente de Rede
Ambiente nuvem
Aplicativo incompatível
Arquivo de chave
Ataque de vírus
Ataque MITM
Atualização disponível
Atualizar
Backup de dados do Servidor de Administração
Bancos de dados antivírus
Certificado compartilhado
Certificado do Servidor de Administração
Chave ativa
Chave de acesso AWS IAM
Chave de licença adicional (ou chave reserva)
Configurações de Programa
Configurações de tarefa
Console de Administração
Console de Gerenciamento AWS
Direitos de administrador
Dispositivo Android
Dispositivo de proteção UEFI
Dispositivo EAS
Dispositivo KES
Dispositivo MDM do iOS
Dispositivos gerenciados
Domínio de difusão
Estação de trabalho do administrador
Função do IAM
Gateway de conexão
Gerenciamento centralizado de aplicativos
Gerenciamento de identidades e acesso (IAM)
Gerenciamento direto de aplicativos
Gravidade do evento
Grupo de administração
Grupo de aplicativos licenciados
Grupo de funções
HTTPS
Imagem de máquina da Amazon (AMI, Amazon Machine Image)
Instalação forçada
Instalação local

Instalação manual

Instalação remota

Instância Amazon EC2

Interface do Programa de Aplicativo AWS (AWS API)

JavaScript

Kaspersky Private Security Network (KPSN)

Kaspersky Security Network (KSN)

Lightweight Nagent (LWNGT)

Limite de atividade de vírus

Loja de aplicativos

Nível de importância do patch

Operador do Kaspersky Security Center

Pacote de instalação

Pasta de backup

Perfil

Perfil de configuração

Perfil de MDM do iOS

Perfil de provisionamento

Período da licença

Plugin de gerenciamento

Política

Ponto de distribuição

Proprietário do dispositivo

Proteção antivírus da rede

Provedor de serviço de proteção antivírus

Reconhecimento de Localização de Rede (NLA)

Repositório de eventos

Restauração

Restauração dos dados do Servidor de Administração

Servidor de Administração

Servidor de Administração cliente (Dispositivo cliente)

Servidor de Administração Principal

Servidor de Administração virtual

Servidor de dispositivos móveis

Servidor de dispositivos móveis Exchange

Servidor MDM do iOS

Servidor Web do Kaspersky Security Center

Servidores de atualização da Kaspersky

SSL

Status de proteção

Status de proteção da rede

Tarefa

Tarefa de grupo

Tarefa local

Tarefa para dispositivos específicos

Usuário do IAM

Usuários internos

Validador de Integridade do Sistema do Kaspersky Security Center (SHV)
Vulnerabilidade
Windows Server Update Services (WSUS)
Zona desmilitarizada (DMZ)
Informação sobre código de terceiros
Avisos de marca registrada
Problemas conhecidos

Ajuda do Kaspersky Security Center 14.2

	**O que há de novo** Descubra o que há de novo na versão mais recente do aplicativo.		**Configuração da proteção da rede** Gerencie a segurança da organização.
	**Requisitos de hardware e software** Verifique quais sistemas operacionais e versões de aplicativo são compatíveis.		**Aplicativos da Kaspersky. Atualização dos bancos de dados e módulos de software** Mantenha a confiabilidade do sistema de proteção.
	**Implementação e configuração inicial** Planeje o uso de recursos, instale o Servidor de Administração, instale o Agente de Rede e os aplicativos de segurança em dispositivos cliente, e consolide dispositivos em grupos de administração.		**Monitoramento e relatórios** Visualize sua infraestrutura, status de proteção e estatísticas.
	**Localizar dispositivos na rede** Detecte os dispositivos existentes e os novos na rede da sua organização.		**Substituição de aplicativos de segurança de terceiros** Conheça métodos para desinstalar aplicativos incompatíveis.
	**Aplicativos da Kaspersky. Implementação centralizada** Implementar aplicativos Kaspersky.		**Ajuste de pontos de distribuição e gateways de conexão** Configurar os pontos de distribuição.
	**Atualização do Kaspersky Security Center a partir de uma versão anterior** Faça o upgrade do Kaspersky Security Center 14.2 a partir de uma versão anterior.		**Práticas recomendadas para provedores de serviços (ajuda online apenas)** Conheça recomendações sobre como implementar, configurar e usar o aplicativo, assim como formas para solucionar problemas típicos na operação do aplicativo.
	**Aplicativos da Kaspersky. Licenciamento e ativação** Ative os aplicativos Kaspersky em algumas etapas.		**Guia de dimensionamento (ajuda online apenas)** Para o desempenho ótimo sob a variação de condições, leve em conta o número de dispositivos na rede, a topologia da rede e o conjunto de recursos do Kaspersky Security Center que você necessita.
	**Exportando eventos para os sistemas SIEM** Configure a exportação de eventos para sistemas SIEM para análise.		**Gerenciamento de patches e vulnerabilidades** Encontre e corrija vulnerabilidades em softwares de terceiros.
	**Trabalhando em um ambiente nuvem** Implemente o Kaspersky Security Center em ambientes em nuvem: Amazon Web Services™, Microsoft Azure™, Google™ Cloud Platform.		**Perguntas frequentes (apenas em inglês)** Encontre instruções sobre como resolver problemas comuns.
	**Guia de início rápido do Kaspersky Endpoint Security for Business** Comece com o Kaspersky Endpoint Security for Business: instale e configure esta solução. Você também pode examinar a comparação de recursos do Kaspersky Security Center para escolher a maneira mais adequada de gerenciar a segurança da rede.		

O que há de novo

Kaspersky Security Center 14.2

O Kaspersky Security Center 14.2 inclui vários novos recursos e aprimoramentos:

- Um novo Guia de Proteção foi lançado. É altamente recomendável ler atentamente o guia e seguir as recomendações de segurança para configurar o Kaspersky Security Center e sua infraestrutura de rede.

  Além disso, instale a atualização mais recente do Kaspersky Security Center. Esta atualização inclui recursos de proteção de infraestrutura, como a verificação em duas etapas de contas de usuário e outras melhorias.

- O acesso aos servidores Kaspersky agora é verificado automaticamente. Se não for possível acessar os servidores por meio do DNS do sistema, o aplicativo usará o DNS público.

- Direitos do usuário em um Servidor de Administração virtual estão disponíveis para configuração a qualquer momento, seja qual for o Servidor de Administração principal. Além disso, você pode atribuir aos usuários do Servidor principal os direitos de gerenciar um Servidor virtual.

- O Kaspersky Security Center agora oferece suporte ao trabalho com os seguintes DBMSs:

  - PostgreSQL 13.x
  - PostgreSQL 14.x
  - Postgres Pro 13.x (todas as edições)
  - Postgres Pro 14.x (todas as edições)
  - MariaDB 10.1, 10.4, 10.5

- É possível usar o Kaspersky Security Center Web Console para exportar políticas e tarefas para um arquivo e, em seguida, importar as políticas e as tarefas para o Kaspersky Security Center Windows ou Kaspersky Security Center Linux.

- A opção **Não usar o servidor proxy** foi removida das seguintes tarefas:

  - *Baixar atualizações no repositório do Servidor de Administração*
  - *Baixar atualizações para os repositórios de pontos de distribuição*

- Para proteger dispositivos clientes em um ambiente em nuvem, você pode implementar o Kaspersky Endpoint Security for Windows em vez do Kaspersky Security for Windows Server. Agora, este recurso está disponível após o lançamento da versão do Kaspersky Endpoint Security 12.0 for Windows.

- Agora, o trabalho com as chaves de criptografia é limitado pelo direitos de acesso para a área funcional **Funcionalidades gerais**: **Gerenciamento de chaves de criptografia**. Agora, os usuários do Kaspersky Security Center podem exportar chaves de criptografia caso tenham o direito de **Leitura** e podem importar as chaves de criptografia caso tenham o direito de **Escrita**.

Kaspersky Security Center 14

O Kaspersky Security Center 14 inclui vários novos recursos e aprimoramentos:

- É possível instalar as atualizações e corrigir as vulnerabilidades do software de terceiros (com exceção de software da Microsoft) em uma rede isolada. Essas redes incluem Servidores de Administração e dispositivos gerenciados sem acesso à Internet. Para corrigir vulnerabilidades nesse tipo de rede, baixe as atualizações necessárias usando um Servidor de Administração com acesso à Internet e, em seguida, transmita os patches para os Servidores de Administração isolados.

- Perfis de conexão para usuários remotos foram adicionados para dispositivos macOS. Ao usar perfis de conexão, é possível configurar as regras para Agentes de Rede em dispositivos macOS se conectarem ao mesmo ou a diferentes Servidores de Administração, dependendo da localização do dispositivo.

- O Agente de Rede agora pode ser instalado em dispositivos que executam o Microsoft Windows 10 IoT Enterprise.

- No **Relatório de ameaças**, é possível filtrar a lista de ameaças para visualizar apenas aquelas que foram detectadas pelo Cloud Sandbox.

- Agora, o Kaspersky Security Center é compatível com o Kaspersky Industrial Cybersecurity for Linux Nodes 1.3 como um aplicativo gerenciado.

O Kaspersky Security Center Web Console inclui vários novos recursos e aprimoramentos:

- É possível configurar o modo somente painel para funcionários que não gerenciam a rede, mas que desejam visualizar as estatísticas de proteção da rede no Kaspersky Security Center (por exemplo, um gerente superior). Quando um usuário tem esse modo ativado, apenas um painel com um conjunto predefinido de widgets é exibido. Assim, ele pode monitorar as estatísticas especificadas nos widgets, por exemplo, o status de proteção de todos os dispositivos gerenciados, o número de ameaças detectadas recentemente ou a lista das ameaças mais frequentes na rede.

- O Kaspersky Security Center Web Console agora é compatível com o Kaspersky Security for iOS como um aplicativo de segurança.

- Nas propriedades da tarefa, é possível especificar se deseja ou não aplicar a tarefa a subgrupos e Servidores de Administração secundários (incluindo os virtuais).

- Agora, o Kaspersky Security Center é compatível com o Kaspersky Industrial Cybersecurity for Linux Nodes 1.3 como um aplicativo gerenciado.

Kaspersky Security Center 13.2

O Kaspersky Security Center 13.2 inclui vários novos recursos e aprimoramentos:

- Agora você pode instalar o Servidor de Administração, o Console de Administração, o Kaspersky Security Center 13.2 Web Console e o Agente de Rede nos novos sistemas operacionais a seguir (consulte os requisitos de software para obter detalhes):
  - Microsoft Windows 11
  - Microsoft Windows 10 21H2 (Atualização de outubro de 2021)
  - Windows Server 2022
- Você pode usar o MySQL 8.0 como banco de dados.
- É possível implantar o Kaspersky Security Center em um cluster de failover Kaspersky Security Center para fornecer alta disponibilidade do Kaspersky Security Center.
- O Kaspersky Security Center agora funciona com endereços IPv6, além de endereços IPv4. O Servidor de Administração pode sondar redes que possuem dispositivos com endereços IPv6.

O Kaspersky Security Center 13.2 Web Console inclui vários novos recursos e aprimoramentos:

- Agora, você pode gerenciar dispositivos móveis executados em Android por meio do Kaspersky Security Center 13.2 Web Console.
- O Kaspersky Marketplace está disponível como uma nova seção de menu: você pode pesquisar o aplicativo Kaspersky por meio do Kaspersky Security Center 13.2 Web Console.
- O Kaspersky Security Center agora é compatível com os seguintes aplicativos 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

O Kaspersky Security Center 13.1 inclui vários novos recursos e aprimoramentos:

- A integração com sistemas SIEM foi aprimorada. Você agora pode exportar eventos para os sistemas SIEM via canal criptografado (TLS). O recurso está disponível para o Kaspersky Security Center Web Console e o Console de Administração baseado em MMC.
- Você pode agora receber patches para o Servidor de Administração como um pacote de distribuição, que pode ser usado para futuras atualizações para versões mais recentes.
- Uma nova seção de **Alertas** foi adicionada ao Kaspersky Endpoint Detection and Response Optimum para o Kaspersky Security Center 13.1 Web Console. Vários novos widgets também foram adicionados para trataar as ameaças detectadas pelo Kaspersky Endpoint Detection and Response Optimum.

- No Kaspersky Security Center 13.1 Web Console, você agora pode receber notificações sobre licenças prestes a expirar para os aplicativos Kaspersky.

- O tempo de resposta do Kaspersky Security Center 13.1 Web Console foi reduzido.

Kaspersky Security Center 13

Os seguintes recursos foram adicionados ao Kaspersky Security Center 13 Web Console:

- Verificação em duas etapas implementada. Você pode ativar a verificação em duas etapas para reduzir o risco de acesso não autorizado ao Kaspersky Security Center 13 Web Console.

- Autenticação de domínio implementada usando os protocolos NTLM e Kerberos (autenticação única). O recurso de autenticação única permite ao usuário do Windows ativar a autenticação segura no Kaspersky Security Center 13 Web Console sem ter que inserir novamente a senha na rede corporativa.

- Agora você pode configurar um plugin para funcionar com o Kaspersky Managed Detection and Response. Você pode usar essa integração para ver incidentes e gerenciar estações de trabalho.

- Agora, você pode especificar as configurações do Kaspersky Security Center 13 Web Console no assistente de instalação do Servidor de Administração.

- As notificações são exibidas sobre novos lançamentos de atualizações e patches. Você pode instalar uma atualização imediatamente ou mais tarde a qualquer momento. Agora, você pode instalar patches para o Servidor de Administração por meio do Kaspersky Security Center 13 Web Console.

- Ao trabalhar com tabelas, agora você pode especificar a ordem e a largura das colunas, classificar os dados e especificar o tamanho da página.

- Agora, você pode abrir qualquer relatório clicando no nome.

- O Kaspersky Security Center 13 Web Console agora está disponível também no idioma coreano.

- Uma nova seção, Novidades Kaspersky, está disponível no menu **Monitoramento e relatórios**. A seção mantém você a par de informações relacionadas à sua versão do Kaspersky Security Center e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. O Kaspersky Security Center atualiza periodicamente as informações desta seção, removendo informações antigas e adicionando novas. No entanto, você pode desativar os informativos da Kaspersky, se desejar.

- Autenticação adicional implementada, após alterar as configurações de uma conta de usuário. Você pode ativar a proteção de uma conta de usuário contra modificações não autorizadas. Se essa opção for ativada, a modificação das configurações da conta do usuário requer autorização por um usuário com direitos para modificação.

Os seguintes recursos foram adicionados ao Kaspersky Security Center 13:

- Verificação em duas etapas implementada. Você pode ativar a verificação em duas etapas para reduzir o risco de acesso não autorizado ao Console de Administração. Se essa opção for ativada, a modificação das configurações da conta do usuário requer autorização do usuário com direitos para modificação. Agora, você pode ativar ou desativar a verificação em duas etapas para dispositivos KES.

- Você pode enviar mensagens ao Servidor de Administração via HTTP. Um guia de referência e uma biblioteca Python para uso com o OpenAPI do Servidor de Administração.

- Você pode emitir um certificado reserva para uso em perfis de MDM do iOS, para garantir a alternância perfeita de dispositivos iOS gerenciados após a expiração do certificado do Servidor de MDM do iOS.

- A pasta de aplicativos multitenant não é mais exibida no Console de Administração.

Kaspersky Security Center 14.2

Esta seção fornece informações sobre a utilização do Kaspersky Security Center 14.2.

As informações fornecidas na Ajuda online podem diferenciar-se das informações fornecidas em documentos fornecidos com o aplicativo; neste caso, considera-se a Ajuda online como a versão mais atualizada. Você pode prosseguir à Ajuda on-line clicando nos links na interface do aplicativo, ou clicando no link da Ajuda on-line nos documentos. A Ajuda on-line pode ser atualizada sem prévio aviso. É possível alternar entre a Ajuda on-line e a Ajuda offline, caso necessário.

Conceitos básicos

Esta seção explica os conceitos básicos relacionados com o Kaspersky Security Center.

Servidor de Administração

Os componentes do Kaspersky Security Center permitem o gerenciamento remoto dos aplicativos Kaspersky instalados em dispositivos cliente.

Os dispositivos com o componente do Servidor de Administração instalado serão referidos como *Servidores de Administração* (aqui referidos como *Servidores*). Os Servidores de Administração devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

O Servidor de Administração é instalado em um dispositivo como um serviço, com o seguinte conjunto de atributos:

- Com o nome "Servidor de Administração do Kaspersky Security Center"
- Configurado para iniciar automaticamente ao inicializar o sistema operacional
- Com a conta **LocalSystem** ou a conta do usuário selecionada durante a instalação do Servidor de Administração

O Servidor de Administração realiza as seguintes funções:

- Armazenamento da estrutura dos grupos de administração
- Armazenamento de informações sobre a configuração de dispositivos cliente
- Organização dos repositórios para pacotes de distribuição de aplicativos
- Instalação remota de aplicativos para dispositivos cliente e remoção de aplicativos
- Atualização de bancos de dados de aplicativos e módulos de software dos aplicativos Kaspersky
- Gerenciamento de políticas e tarefas nos dispositivos cliente

- Armazenamento de informações sobre eventos que ocorreram em dispositivos cliente
- Geração de relatórios na operação dos aplicativos Kaspersky
- Implementação de chaves de licença para os dispositivos cliente e armazenamento de informações sobre chaves de licença
- O encaminhamento de notificações sobre o progresso das tarefas (tal como detecção de vírus em um dispositivo cliente)

Nomeando Servidores de Administração na interface do aplicativo

Na interface do Console de Administração baseado em MMC e do Kaspersky Security Center Web Console, os Servidores de Administração podem ter os seguintes nomes:

- Nome do dispositivo do Servidor de Administração, por exemplo: "*nome do dispositivo*" ou "Servidor de Administração: *nome do dispositivo*".
- Endereço IP do dispositivo do Servidor de Administração, por exemplo: "*Endereço de IP*" ou "Servidor de Administração: *Endereço de IP*".
- Os Servidores de Administração secundários e virtuais têm nomes personalizados que você especifica ao conectar um Servidor de Administração virtual ou secundário ao Servidor de Administração principal.
- Se você usar o Kaspersky Security Center Web Console: instalado em um dispositivo Linux, o aplicativo exibe os nomes dos Servidores de Administração especificados como confiáveis no arquivo de resposta.

Você pode conectar-se ao Servidor de Administração por meio do Console de Administração ou do Kaspersky Security Center Web Console.

Hierarquia de Servidores de Administração

Os Servidores de Administração podem ser dispostos numa hierarquia principal/secundário. Cada Servidor de Administração pode possuir vários Servidores de Administração secundários (citados como *Servidores secundários*) em diferentes níveis de alojamento da hierarquia. O nível de alojamento para Servidores secundários não é limitado. Os grupos de administração do Servidor de Administração principal incluirão então os dispositivos cliente de todos os Servidores de Administração secundários. Portanto, as seções isoladas e independentes das redes podem ser gerenciadas por diferentes Servidores de Administração que, por sua vez, são gerenciadas pelo Servidor principal.

Os *Servidores de Administração virtuais* são um caso particular de Servidores de Administração secundários.

A hierarquia dos Servidores de Administração pode ser usada para o seguinte:

- Diminuir a carga no Servidor de Administração (em comparação com um único Servidor de Administração instalado para uma rede inteira).
- Diminuir o tráfego na intranet e simplificar o trabalho com escritórios remotos. Você não é precisa estabelecer conexões entre o Servidor de Administração principal e todos os dispositivos na rede, os quais podem estar localizados, por exemplo, em outras regiões. É suficiente para instalar em cada segmento de rede um Servidor de Administração secundário, distribuir dispositivos entre os grupos de administração de servidores secundários e estabelecer conexões entre os servidores secundários e o servidor principal em canais de comunicação rápida.

- Distribuir responsabilidades entre os administradores de segurança antivírus. Todos os recursos para gerenciamento e monitoramento centralizado do status de segurança antivírus em redes corporativas permanecem disponíveis.

- Use o Kaspersky Security Center de provedores de serviços. Um provedor de serviços somente necessita instalar o Kaspersky Security Center e o Kaspersky Security Center Web Console. Para gerenciar um número maior de dispositivos cliente de várias organizações, um provedor de serviço pode adicionar Servidores de Administração secundários (inclusive servidores virtuais) na hierarquia de Servidores de Administração.

Cada dispositivo incluído na hierarquia dos grupos de administração pode ser conectado apenas a um Servidor de Administração. Você deve monitorar de forma independente a conexão de dispositivos aos Servidores de Administração. Use os recursos para a pesquisa de dispositivo em grupos de administração de diferentes Servidores com base em atributos de rede.

Servidor de Administração virtual

O Servidor de Administração virtual (também referido como *Servidor virtual*) é um componente do Kaspersky Security Center projetado para gerenciar a proteção antivírus da rede de uma organização cliente.

O Servidor de Administração virtual é um caso particular de um Servidor de Administração secundário com as seguintes restrições em comparação com o Servidor de Administração físico:

- O Servidor de Administração virtual só pode ser criado no Servidor de Administração principal.

- O Servidor de Administração virtual usa o banco de dados do Servidor de Administração principal. Tarefas de backup e restauração de dados, bem como tarefas de verificação de atualização e download, não são compatíveis com um Servidor de Administração virtual.

- O Servidor virtual não é compatível com a criação de Servidores de Administração secundários (incluindo Servidores virtuais).

Além disso, o Servidor de Administração virtual possui as seguintes restrições:

- Na janela de propriedades do Servidor de Administração virtual, o número de seções é limitado.

- Para instalar aplicativos Kaspersky remotamente em dispositivos cliente gerenciados pelo Servidor Administrativo virtual, você deve certificar-se de que o Agente de Rede está instalado em um dos dispositivos cliente para poder garantir a comunicação com o Servidor de Administração virtual. Na primeira conexão ao Servidor de Administração virtual, esse dispositivo é automaticamente atribuído como o ponto de distribuição, funcionando como um gateway de conexão entre os dispositivos cliente e o Servidor de Administração virtual.

- Um servidor virtual pode amostrar a rede somente através de pontos de distribuição.

- Para reiniciar um Servidor virtual que não está funcionando corretamente, o Kaspersky Security Center reinicia o Servidor de Administração principal e todos os Servidores virtuais.

- Os usuários criados em um servidor virtual não podem receber uma função no Servidor de Administração.

O administrador de um Servidor virtual possui todos os privilégios neste Servidor virtual em particular.

Servidor de dispositivos móveis

O *Servidor de dispositivos móveis* é um componente do Kaspersky Security Center que fornece acesso a dispositivos móveis e permite gerenciá-los através do Console de Administração. O Servidor de dispositivos móveis obtém informações sobre dispositivos móveis e armazena seus perfis.

Existem dois tipos de Servidores de dispositivos móveis:

- Servidor de dispositivos móveis Exchange. Isso é instalado em um dispositivo onde um Microsoft Exchange Server foi instalado, que permite recuperar dados do Microsoft Exchange Server e efetuar a transmissão dos dados para o Servidor de Administração. Este Servidor de dispositivos móveis é usado para o gerenciamento de dispositivos móveis que suportam o protocolo Exchange ActiveSync.

- Servidor MDM do iOS. Este Servidor de dispositivos móveis é usado para gerenciamento de dispositivos móveis que suportam o serviço Apple® Push Notification (APNs).

Os Servidores de dispositivos móveis do Kaspersky Security Center permitem o gerenciamento dos seguintes objetos:

- Um dispositivo móvel individual.

- Vários dispositivos móveis.

- Vários dispositivos móveis conectados a um agrupamento de servidores em simultâneo. Depois de conectar a um agrupamento de servidores, o servidor de dispositivos móveis instalado neste agrupamento é exibido no Console de Administração como um servidor único.

Servidor Web

O *Servidor Web* do Kaspersky Security Center (daqui em diante referido como *Servidor Web*) é um componente do Kaspersky Security Center que é instalado junto com o Servidor de Administração. O Servidor da Web foi projetado para a transmissão, através de uma rede, de pacotes de instalação independentes, perfis MDM do iOS e arquivos de uma pasta compartilhada.

Ao criar um pacote de instalação independente, ela é automaticamente publicada no Servidor da Web. Um link para o download do pacote independente é exibido na lista de pacotes de instalação independentes criados. Se necessário, você poderá cancelar a publicação do pacote independente ou publicá-lo novamente no Servidor da Web.

Ao criar um perfil de MDM do iOS para o dispositivo móvel do usuário, ele é também publicado automaticamente no Servidor da Web. O perfil publicado é automaticamente excluído do Servidor Web assim que ele seja instalado com êxito no dispositivo móvel do usuário.

A pasta compartilhada é usada para o armazenamento de informações que estão disponíveis para todos os usuários cujos dispositivos são gerenciados através do Servidor de Administração. Se um usuário não tiver acesso direto à pasta compartilhada, ele poderá receber informações a partir dessa pasta usando o Servidor da Web.

Para fornecer aos usuários informações da pasta compartilhada usando o Servidor Web, o administrador deve criar uma subpasta com o nome de "pública" na pasta compartilhada e colar as informações nela.

A sintaxe do link de transferência de informações é a seguinte:

`https://<Nome do Servidor d Web>:<Porta HTTPS>/public/<objeto>`

onde:

- `<nome do Servidor Web>` é o nome do Servidor Web do Kaspersky Security Center.
- `<porta HTTPS>` é uma porta HTTPS do Servidor Web que foi definida pelo Administrador. A porta HTTPS pode ser definida na seção **Servidor da Web** da janela Propriedades do Servidor de Administração. O número da porta padrão é 8061.
- `<objeto>` é uma subpasta ou um arquivo ao qual o usuário tem acesso.

O administrador pode enviar o novo link ao usuário de qualquer forma prática: por exemplo, por e-mail.

Ao usar este link, o usuário poderá baixar as informações necessárias para um dispositivo local.

Agente de Rede

A interação entre o Servidor de Administração e os dispositivos é realizada pelo componente *Agente de Rede* do Kaspersky Security Center. O Agente de Rede deve ser instalado em todos os dispositivos cliente, nos quais o Kaspersky Security Center é usado para gerenciar os aplicativos Kaspersky.

O Agente de Rede é instalado no dispositivo como um serviço, com o seguinte conjunto de atributos:

- Com o nome "Agente de Rede do Kaspersky Security Center"
- Configurado para iniciar automaticamente ao inicializar o sistema operacional
- Usar o LocalSystem Account

Um dispositivo com o Agente de Rede instalado é denominado de *dispositivo gerenciado* ou *dispositivo*.

Você pode instalar o Agente de Rede em um dispositivo Windows, Linux ou Mac. Você pode obter o componente de uma das seguintes fontes:

- Pacote de instalação no armazenamento do Servidor de Administração (você precisa ter o Servidor de Administração instalado)
- Pacote de instalação localizado nos servidores da web Kaspersky

Você não precisa instalar o Agente de Rede no dispositivo onde instalou o Servidor de Administração, porque a versão de servidor do Agente de Rede é automaticamente instalada em conjunto com o Servidor de Administração.

O nome do processo que o Agente de Rede inicia é *klnagent.exe*.

O Agente de Rede sincroniza o dispositivo gerenciado com o Servidor de Administração. Recomendamos definir o intervalo de sincronização (também conhecido como *heartbeat*) para 15 minutos a cada 10.000 dispositivos gerenciados.

Grupos de administração

Um *grupo de administração* (aqui também referido como um *grupo*) é um conjunto lógico de dispositivos gerenciados combinados na base de um tratado específico com o propósito de gerenciar os dispositivos agrupados como uma unidade única dentro do Kaspersky Security Center.

Todos os dispositivos gerenciados dentro de um grupo de administração são configurados para fazer o seguinte:

- Usar as mesmas configurações de aplicativo (que você pode definir nas políticas de grupo).
- Use um modo de operação comum para todos os aplicativos por meio da criação de tarefas de grupo com configurações especificadas. Exemplos de tarefas de grupo incluem criar e instalar um pacote de instalação comum, atualizar os bancos de dados e módulos de aplicativos, verificar dispositivo sob demanda e ativar a proteção em tempo real.

Um dispositivo gerenciado pode pertencer a um somente grupo de administração.

Você pode criar hierarquias que têm qualquer grau de aninhamento para Servidores de Administração e grupos. Um único nível de hierarquia pode incluir servidores de administração secundários e virtuais, grupos e dispositivos gerenciados. Você pode migrar dispositivos de um grupo ao outro sem movê-los fisicamente. Por exemplo, se o cargo de um funcionário na empresa for alterado de contador para desenvolvedor, você pode mover o dispositivo desse funcionário do grupo de administração Contadores para o grupo de administração Desenvolvedores. Depois disso, o dispositivo receberá automaticamente as configurações de aplicativo necessárias para os desenvolvedores.

Dispositivo gerenciado

Um *dispositivo gerenciado* é um dispositivo que executa Windows, Linux ou macOS no qual o Agente de Rede está instalado ou um dispositivo móvel no qual um aplicativo de segurança da Kaspersky está instalado. Você pode gerenciar esses dispositivos criando tarefas e políticas para os aplicativos instalados nos dispositivos. Você também pode receber relatórios dos dispositivos gerenciados.

Você pode transformar uma função de dispositivo gerenciado não-móvel em um ponto de distribuição e em um gateway de conexão.

Um dispositivo pode ser gerenciado somente por um Servidor de Administração. Um Servidor de Administração pode gerenciar até 100.000 dispositivos, incluindo dispositivos móveis.

Dispositivo não atribuído

Um *dispositivo não atribuído* é um dispositivo na rede que não estava incluído em nenhum grupo de administração. Você pode executar algumas ações em dispositivos não atribuídos, por exemplo, movê-los para seus grupos de administração ou instalar aplicativos neles.

Quando um novo dispositivo é descoberto na rede, esse dispositivo vai para o grupo de administração **Dispositivos não atribuídos**. Você pode configurar regras para que os dispositivos sejam movidos automaticamente para outros grupos de administração após serem descobertos.

Estação de trabalho do administrador

Estação de trabalho do administrador é um dispositivo no qual o Console de Administração está instalado ou que você usa para abrir o Kaspersky Security Center Web Console. Os administradores podem usar esses dispositivos para o gerenciamento remoto centralizado dos aplicativos Kaspersky instalados nos dispositivos cliente.

Após o Console de Administração ter sido instalado em seu dispositivo, seu ícone é exibido e pode ser usado para iniciar o Console de Administração. Localize-o no menu **Iniciar** → **Programas** → **Kaspersky Security Center**.

Não há restrições quanto ao número de estações de trabalho do administrador. Em qualquer estação de trabalho do administrador, você pode gerenciar os grupos de administração de vários Servidores de Administração na rede de uma só vez. Você pode conectar uma estação de trabalho do administrador a um Servidor de Administração (físico ou virtual) de qualquer nível de hierarquia.

Você pode incluir uma estação de trabalho do administrador em um grupo de administração como um dispositivo cliente.

Dentro dos grupos de administração de qualquer Servidor de Administração, o mesmo dispositivo pode funcionar como um Servidor de Administração cliente, um Servidor de Administração ou uma estação de trabalho do administrador.

Plugin de gerenciamento

Os aplicativos Kaspersky são gerenciados via Console de Administração usando um componente dedicado chamado de *plugin de gerenciamento*. Cada aplicativo da Kaspersky que pode ser gerenciado pelo Kaspersky Security Center inclui um plugin de gerenciamento.

Usando o plugin de gerenciamento, você poderá executar as seguintes ações no Console de Administração:

- Criação e edição das políticas e configurações de aplicativos, assim como configurações das tarefas de aplicativo.
- Obtenção de informações sobre as tarefas de aplicativo, eventos que ocorrem em sua operação, assim como estatísticas da operação de aplicativo recebidas dos dispositivos cliente.

É possível baixar os plug-ins de gerenciamento na página de Suporte Técnico da Kaspersky.

Plug-in da Web de gerenciamento

Um componente especial (o *plugin de gerenciamento da Web*) é usado para a administração remota de softwares da Kaspersky por meio do Kaspersky Security Center Web Console. No presente documento, o plug-in da Web de gerenciamento será referido como *plug-in de gerenciamento*. Um plug-in de gerenciamento é uma interface entre o Kaspersky Security Center Web Console e um aplicativo da Kaspersky específico. Com um plug-in de gerenciamento, você pode configurar tarefas e políticas para o aplicativo.

É possível baixar plug-ins de gerenciamento da Web a partir da página do Suporte Técnico da Kaspersky.

O plug-in de gerenciamento fornece o seguinte:

- Interface para criar e editar tarefas e configurações de aplicativo
- Interface para criar e editar políticas e perfis da política para a configuração remota e centralizada de aplicativos e dispositivos da Kaspersky
- Transmissão de eventos gerados pelo aplicativo
- Funções do Kaspersky Security Center Web Console para exibir os dados operacionais e os eventos do aplicativo, além das estatísticas transmitidas de dispositivos clientes

Políticas

Uma *política* é um conjunto de configurações do aplicativo Kaspersky, aplicadas a um grupo de administração e seus subgrupos. Você pode instalar vários aplicativos Kaspersky nos dispositivos de um grupo de administração. O Kaspersky Security Center fornece uma única política para cada aplicativo Kaspersky em um grupo de administração. Uma política tem um dos seguintes status (consulte a tabela abaixo):

O status da política

Status	Descrição
Ativo	A política atual aplicada ao dispositivo. Apenas uma política pode estar ativa por aplicativo Kaspersky em cada grupo de administração. Os dispositivos aplicam os valores de configuração de uma política ativa para um aplicativo Kaspersky.
Inativo	Uma política que não é aplicada atualmente a um dispositivo.
Ausência	Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

As políticas funcionam de acordo com as seguintes regras:

- Várias políticas com valores diferentes podem ser configuradas para um único aplicativo.
- Apenas uma política pode estar ativa para o aplicativo atual.
- É possível ativar uma política desativada quando um evento específico ocorre. Por exemplo, você pode forçar configurações de proteção antivírus mais rigorosas durante surtos de vírus.
- Uma política pode ter políticas secundárias.

Geralmente, você pode usar políticas como preparação para situações de emergência, como um ataque de vírus. Se houver um ataque por meio de unidades flash, você pode ativar uma política que bloqueie o acesso a unidades flash. Nesse caso, a política ativa atual torna-se automaticamente inativa.

Para evitar ter que efetuar manutenção de várias políticas, por exemplo, quando ocasiões diferentes pressupõem a alteração de várias configurações apenas, você pode usar perfis de política.

Um *perfil de política* é um subconjunto nomeado de valores de configuração que substitui os valores de configuração de uma política. Um perfil de política afeta a formação de configurações efetivas em um dispositivo gerenciado. *Configurações em vigor* são um conjunto de configurações de política, configurações de perfil de política e configurações de aplicativo locais aplicadas atualmente ao dispositivo.

Os perfis de política funcionam de acordo com as seguintes regras:

- Um perfil de política entra em vigor quando ocorre uma condição de ativação específica.
- Os perfis contêm valores de configurações que diferem das configurações de política.

- A ativação de um perfil de política altera as configurações em vigor do dispositivo gerenciado.
- Uma política pode incluir no máximo 100 perfis de política.

Perfis da política

Às vezes pode ser necessário criar diversas instâncias de uma única política para diferentes grupos de administração; também convém sincronizar os as configurações dessas políticas centralmente. Essas instâncias podem diferir por apenas uma ou duas configurações. Por exemplo, todos os contadores em uma empresa trabalham segundo a mesma política, mas os contadores sênior estão autorizados a usar unidades flash e os contadores júnior, não. Neste caso, aplicar políticas aos dispositivos somente através da hierarquia de grupos de administração pode ser inconveniente.

Para ajudá-lo a evitar a criação de várias instâncias de uma única política, o Kaspersky Security Center permite criar *perfis de política*. Os perfis de política são destinados se você quiser que os dispositivos dentro de um grupo de administração único executem sob configurações de política diferentes.

Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos de destino em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo gerenciado. A ativação de um perfil modifica as configurações da política "básica" que estavam inicialmente ativas no dispositivo. As configurações modificadas assumem valores que foram especificados no perfil.

Tarefas

O Kaspersky Security Center gerencia os aplicativos de segurança da Kaspersky instalados nos dispositivos cliente criando e executando *tarefas*. As tarefas são necessárias para a instalação, inicialização e interrupção de aplicativos, verificação de arquivos, atualização de bancos de dados e módulos de software e para a realização de outras ações em aplicativos.

As tarefas de um aplicativo específico podem ser criadas apenas se o plugin de gerenciamento desse aplicativo estiver instalado.

As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

As seguintes tarefas que são realizadas no Servidor de Administração:

- Distribuição automática de relatórios
- Baixar atualizações no repositório do Servidor de Administração
- Backup de dados do Servidor de Administração
- Manutenção do banco de dados
- Sincronização com o Windows Update
- Criação de um pacote de instalação com base na imagem do sistema operacional (SO) de um dispositivo de referência

Os seguintes tipos de tarefas são executados nos dispositivos:

- *Tarefas locais* – Tarefas que são executadas em um dispositivo específico

  As tarefas locais podem ser modificadas pelo administrador, usando as ferramentas do Console de Administração ou por um usuário de um dispositivo remoto (por exemplo, através da interface do aplicativo de segurança). Se uma tarefa local tiver sido modificada simultaneamente pelo administrador e pelo usuário de um dispositivo gerenciado, as modificações feitas pelo administrador entrarão em vigor porque elas têm uma maior prioridade.

- *Tarefas de grupo* – Tarefas que são executadas em todos os dispositivos de um grupo específico

  Salvo de especificado de outra maneira nas propriedades de tarefa, uma tarefa de grupo também afeta todos os subgrupos do grupo selecionado. Uma tarefa de grupo também afeta (opcionalmente) os dispositivos que foram conectados aos Servidores de Administração secundários e virtuais implementados no grupo ou em algum dos seus subgrupos.

- *Tarefas globais* – Tarefas que são realizadas em um conjunto de dispositivos, independentemente se os mesmos estão incluídos em qualquer grupo

Para cada aplicativo, você pode criar qualquer número de tarefas de grupo, tarefas globais ou tarefas locais.

Você pode efetuar alterações nas configurações de tarefas, exibir o andamento das tarefas, copiar, exportar, importar e excluir tarefas.

Uma tarefa é iniciada em um dispositivo cliente somente se um aplicativo para o qual a tarefa foi criada estiver sendo executado.

Os resultados das tarefas são salvos no log de eventos do Microsoft Windows e no log de eventos do Kaspersky Security Center, tanto centralmente no Servidor de Administração como localmente em cada dispositivo.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Escopo da tarefa

O *escopo de uma tarefa* é o conjunto de dispositivos nos quais a tarefa é executada. Os tipos de escopo são os seguintes:

- Para uma *tarefa local*, o escopo é o próprio dispositivo.
- Para uma tarefa do *Servidor de Administração*, o escopo é o Servidor de Administração.
- Para uma *tarefa de grupo*, o escopo é a lista de dispositivos incluídos no grupo.

Ao criar uma *tarefa global*, você pode usar os seguintes métodos para especificar o escopo:

- Especificar determinados dispositivos manualmente.

  Você pode usar um endereço IP (ou uma faixa IP), nome NetBIOS ou nome DNS como o endereço do dispositivo.

- Importar uma lista de dispositivos de um arquivo TXT com os endereços dos dispositivos a serem adicionados (cada endereço deve ser colocado em uma linha individual).

  Se você importar uma lista de dispositivos a partir de um arquivo ou cria uma lista manualmente, e se os dispositivos cliente estão identificados pelos seus nomes, a lista deve conter somente os dispositivos cuja informação já foi adicionada ao banco de dados do Servidor de Administração. Além disso, as informações devem ter sido inseridas quando os dispositivos foram conectados ou durante a descoberta de dispositivos.

- Especificar uma seleção de dispositivos.

  Ao longo do tempo, o escopo de uma tarefa se modifica quando o conjunto de dispositivos incluídos na seleção são modificados. Uma seleção de dispositivos pode ser feita com base nos atributos do dispositivo, incluindo o software instalado em um dispositivo, e com base em tags atribuídas aos dispositivos. A seleção de dispositivos é o modo mais flexível para especificar o escopo de uma tarefa.

  As tarefas para seleções de dispositivos sempre são executadas de acordo com um agendamento pelo Servidor de Administração. Estas tarefas não podem ser executadas em dispositivos que não tenham uma conexão com o Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas diretamente nos dispositivos e, por isso, não dependem da conexão do dispositivo com o Servidor de Administração.

  As tarefas para Seleções de dispositivos não são executadas na hora local de um dispositivo; em vez disso, elas serão executadas na hora local do Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas na hora local de um dispositivo.

Como as configurações do aplicativo local se relacionam com as políticas

Você pode usar as políticas para definir valores idênticos das configurações do aplicativo para todos os dispositivos no grupo.

Os valores das configurações especificados por uma política podem ser redefinidos para dispositivos individuais em um grupo usando as configurações do aplicativo locais. Você somente pode definir os valores das configurações, cuja alteração seja permitida pela política, ou seja, configurações desbloqueadas.

O valor de uma configuração que um aplicativo usa em um dispositivo cliente é definido pela posição do cadeado (🔒) para aquela configuração na política:

- Se a modificação da configuração estiver bloqueada, o mesmo valor (definido na política) é utilizado e todos os dispositivos cliente.

- Se a modificação da configuração estiver desbloqueada, o aplicativo usa um valor de configuração local em cada dispositivo cliente em vez do valor especificado na política. O valor do parâmetro pode então ser alterado nas configurações de aplicativo locais.

Deste modo, quando a tarefa está sendo executada em um dispositivo cliente, o aplicativo usa as configurações definidas de duas formas diferentes:

- Por configurações de tarefa e configurações locais de aplicativo, se a configuração não estiver bloqueada contra alteração na política.
- Por política de grupo, se a configuração estiver bloqueada contra alteração.

As configurações de aplicativo locais são alteradas depois da primeira imposição de política de acordo com as configurações de política.

Ponto de distribuição

Ponto de distribuição (anteriormente conhecido como agente de atualização) é um dispositivo com o Agente de Rede instalado, usado para a distribuição de atualizações, instalação remota de aplicativos e recuperação de informações sobre os dispositivos na rede. Os pontos de distribuição agilizam a distribuição da atualização e permite liberar recursos do Servidor de Administração.

Os recursos e casos de uso do Agente de Rede instalado em um dispositivo usado como ponto de distribuição variam conforme o sistema operacional.

Um ponto de distribuição pode executar as seguintes funções:

- Distribuir arquivos recebidos do Servidor de Administração para os dispositivos cliente no grupo (incluindo a distribuição por meio de multicasting usando UDP).

  A lista de arquivos que podem ser transferidos por pontos de distribuição inclui:

  - Atualizações de bancos de dados e módulos de software da Kaspersky
  - Atualizações de softwares de terceiros
  - Pacotes de instalação
  - Atualizações do Windows ao usar o Servidor de Administração como servidor WSUS

  As atualizações podem ser recebidas do Servidor de Administração ou dos servidores de atualização Kaspersky. Nesse caso, uma tarefa de atualização precisa ser criada para o ponto de distribuição. Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky.

  Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.

- Distribuir políticas e tarefas de grupo através de multicasting usando UDP.

- Atua como um gateway para conexão ao Servidor de Administração para dispositivos em um grupo de administração.

  Se não for possível estabelecer uma conexão direta entre os dispositivos gerenciados no grupo e o Servidor de Administração, o ponto de distribuição pode ser usado como um gateway de conexão para o Servidor de Administração para esse grupo. Nesse caso, os dispositivos gerenciados serão conectados ao gateway de conexão, o qual, por sua vez, será conectado ao Servidor de Administração.

  A presença de um ponto de distribuição que opera como um gateway de conexão não bloqueia a opção de conexão direta entre os dispositivos gerenciados e o Servidor de Administração. Se o gateway de conexão não estiver disponível, mas a conexão direta com o Servidor de Administração for tecnicamente possível, os dispositivos gerenciados serão conectados ao Servidor de Administração diretamente.

- Faça a sondagem da rede para detectar novos dispositivos e para atualizar as informações sobre os existentes. Um ponto de distribuição pode aplicar os mesmos métodos de localização dos dispositivos que os do Servidor de Administração.

- Execute a instalação remota de software de terceiros e aplicativos Kaspersky usando ferramentas do sistema operacional do ponto de distribuição. Observe que o ponto de distribuição pode executar a instalação em dispositivos clientes sem o Agente de Rede.

  Esse recurso permite a transferência remota de pacotes de instalação do Agente de Rede para dispositivos cliente localizados em redes às quais o Servidor de Administração não tem acesso direto.

- Atue como um servidor proxy participando da Kaspersky Security Network (KSN).

  Você pode ativar o servidor proxy da KSN no lado do ponto de distribuição para fazer o dispositivo funcionar como um servidor proxy da KSN. Neste caso, o serviço de Proxy da KSN (ksnproxy) é executado no dispositivo.

Os Arquivos são transmitidos do Servidor de Administração a um ponto de distribuição através de HTTP ou, se a Conexão SSL estiver ativada, através de HTTPS. Usar HTTP ou HTTPS resulta em um desempenho mais alto, comparando com o SOAP, através da redução de tráfego.

Aos dispositivos com o Agente de Rede instalado podem ser atribuídos pontos de distribuição de forma manual (pelo administrador) ou automaticamente (pelo Servidor de Administração). A lista completa de pontos de distribuição para grupos de administração especificados é exibida no relatório na lista de pontos de distribuição.

O escopo de um ponto de distribuição é o grupo de administração ao qual ele foi atribuído pelo administrador, assim como seus subgrupos de todos os níveis de incorporação. Se múltiplos pontos de distribuição tiverem sido atribuídos na hierarquia de grupos de administração, o Agente de Rede do dispositivo gerenciado se conecta ao ponto de distribuição mais próximo na hierarquia.

Uma localização da rede também pode ser o escopo dos pontos de distribuição. A localização da rede é então usada para a criação manual de um conjunto de dispositivos ao qual o ponto de distribuição distribuirá as atualizações. A localização da rede somente pode ser determinada para dispositivos que executam um sistema operacional Windows.

Se os pontos de distribuição forem automaticamente atribuídos pelo Servidor de Administração, ele os atribui por domínios de difusão, não por grupos de administração. Isso ocorre quando todos os domínios de difusão são conhecidos. O Agente de Rede troca mensagens com outros Agentes de Rede na mesma sub-rede e, a seguir, envia informações ao Servidor de Administração sobre si mesmo e de outros Agentes de Rede. O Servidor de Administração usa estas informações para agrupar os Agentes de atualização por domínios de difusão. Os domínios de difusão são conhecidos para o Servidor de Administração após mais de 70% dos Agentes de rede nos grupos de administração forem amostrados. O Servidor de Administração efetua a sondagem dos domínios de difusão a cada duas horas. Após os pontos de distribuição terem sido atribuídos pelo domínio de difusão, eles não podem ser reatribuídos por grupos de administração.

Se o administrador atribuir manualmente pontos de distribuição, eles poderão ser atribuídos a grupos de administração ou locais de rede.

Os Agentes de Rede com o perfil de conexão ativo não participam na detecção do domínio de difusão.

O Kaspersky Security Center atribui a cada Agente de Rede um endereço IP multicast único que se diferencia de cada outro endereço. Isto lhe permite evitar a sobrecarga de rede que poderia ocorrer devido a sobreposições de IP.

Quando dois ou mais pontos de distribuição forem atribuídos à uma única área de rede ou para um único grupo de administração, um deles se torna o ponto de distribuição ativo, e o restante deles se tornam pontos de distribuição em standby. O ponto de distribuição ativo baixa as atualizações e os pacotes de instalação diretamente do Servidor de Administração, enquanto os pontos de distribuição em standby recuperam as atualizações somente do ponto de distribuição ativo. Neste caso, após os arquivos terem sido baixados do Servidor de Administração eles são distribuídos entre os pontos de distribuição. Se o ponto de distribuição ativo se tornar indisponível por qualquer motivo, um dos pontos de distribuição independentes se torna ativo. O Servidor de Administração atribui automaticamente um ponto de distribuição para agir como standby.

O status do ponto de distribuição (*Ativo* / *Standby*) é exibido com uma caixa de seleção no relatório klnagchk.

Um ponto de distribuição requer ao menos 4 GB de espaço livre no disco. Se o espaço disponível livre do ponto de distribuição for menor do que 2 GB, o Kaspersky Security Center cria um incidente com o nível de importância de *Advertência*. O incidente será publicado nas propriedades do dispositivo, na seção **Incidentes**.

Executar tarefas de instalação remota em um dispositivo atribuído como ponto de distribuição exige espaço livre adicional no disco. O volume do espaço em disco disponível livre deve exceder o tamanho total de todos os pacotes de instalação a ser instalados.

Executar qualquer tarefa de atualização (patch) e de correção de vulnerabilidades em um dispositivo atribuído como ponto de distribuição exige espaço livre adicional no disco. O volume do espaço em disco disponível livre deve ser pelo menos duas vezes o tamanho total de todos os patches a serem instalados.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Gateway de conexão

Um *gateway de conexão* é um Agente de Rede atuando em um modo especial. Um gateway de conexão aceita conexões de outros Agentes de Rede e os canaliza para o Servidor de Administração por meio de sua própria conexão com o Servidor. Ao contrário de um Agente de Rede comum, um gateway de conexão aguarda por conexões do Servidor de Administração, em vez de estabelecer conexões com o Servidor de Administração.

Um gateway de conexão pode receber conexões de até 10.000 dispositivos.

Você tem duas opções para usar gateways de conexão:

- Recomendamos instalar um gateway de conexão em uma zona desmilitarizada (DMZ). Para outros Agentes de Rede instalados em dispositivos externos, você precisa configurar especialmente uma conexão ao Servidor de Administração por meio do gateway de conexão.

  Um gateway de conexão não modifica ou processa de forma alguma os dados transmitidos dos Agentes de Rede para o Servidor de Administração. Além disso, ele não grava esses dados em nenhum buffer e, portanto, não pode aceitar dados de um Agente de Rede e posteriormente encaminhá-los ao Servidor de Administração. Se o Agente de Rede tentar se conectar ao Servidor de Administração através do gateway de conexão, mas esse não puder se conectar ao Servidor de Administração, o Agente de Rede interpretará isso como se o Servidor de Administração estivesse inacessível. Todos os dados permanecem no Agente de Rede (não no gateway de conexão).

  Um gateway de conexão não pode se conectar ao Servidor de Administração por meio de outro gateway de conexão. Isso significa que o Agente de Rede não pode ser simultaneamente um gateway de conexão e usar um gateway de conexão para se conectar ao Servidor de Administração.

  Todos os gateways de conexão estão incluídos na lista de pontos de distribuição nas propriedades do Servidor de Administração.

- Você também pode usar gateways de conexão dentro da rede. Por exemplo, pontos de distribuição atribuídos automaticamente também se tornam gateways de conexão em seu próprio escopo. No entanto, em uma rede interna, os gateways de conexão não oferecem benefícios consideráveis. Eles reduzem o número de conexões de rede recebidas pelo Servidor de Administração, mas não reduzem o volume de dados de entrada. Mesmo sem gateways de conexão, todos os dispositivos ainda podem se conectar ao Servidor de Administração.

Sobre o Kaspersky Security Center

A seção contém informações sobre a finalidade do Kaspersky Security Center, seus respectivos recursos e componentes principais e maneiras de comprá-lo.

As informações fornecidas na Ajuda online podem diferenciar-se das informações fornecidas em documentos fornecidos com o aplicativo; neste caso, considera-se a Ajuda online como a versão mais atualizada. Você pode prosseguir à Ajuda on-line clicando nos links na interface do aplicativo, ou clicando no link da Ajuda on-line nos documentos. A Ajuda on-line pode ser atualizada sem prévio aviso. É possível alternar entre a Ajuda on-line e a Ajuda offline, caso necessário.

O Kaspersky Security Center foi concebido para a execução centralizada de tarefas de administração e manutenção básicas na rede de uma organização. O aplicativo fornece o acesso ao administrador para obter informações detalhadas sobre o nível de segurança da rede corporativa; isso permite configurar todos os componentes de proteção criados usando os aplicativos Kaspersky.

O Kaspersky Security Center é um aplicativo que se destina aos administradores de redes corporativas e funcionários responsáveis pela proteção de dispositivos em diversos tipos de organizações.

Com o uso do Kaspersky Security Center, você pode fazer o seguinte:

- Crie uma hierarquia de Servidores de Administração para gerenciar a rede corporativa, assim como redes em escritórios remotos e organizações cliente.

  A *organização cliente* é uma organização, cuja proteção antivírus é garantida pelo provedor de serviços.

- Crie uma hierarquia de grupos de administração para gerenciar uma seleção de dispositivos cliente como um todo.

- Gerenciar um sistema de proteção antivírus criado com base nos aplicativos Kaspersky.
- Crie imagens de sistemas operacionais e implemente-as em dispositivos cliente na a rede, assim como executar uma instalação remota de aplicativos Kaspersky e de outros fornecedores de software.
- Remotamente gerenciar os aplicativos Kaspersky e de outros fornecedores instalados em dispositivos cliente. Instale as atualizações e encontre e corrija as vulnerabilidades.
- Realizar implementações centralizadas de chaves de licença para aplicativos Kaspersky em dispositivos cliente, monitorar seu uso e renovar licenças.
- Receber estatísticas e relatórios sobre a operação dos aplicativos e dispositivos.
- Receber notificações sobre eventos críticos durante a operação dos aplicativos Kaspersky.
- Gerenciar dispositivos móveis.
- Gerenciar criptografia de informações armazenadas nos discos rígidos de dispositivos e unidades removíveis e acesso de usuários aos dados criptografados.
- Realizar inventário de hardware conectado à rede corporativa.
- Gerencie centralizadamente os arquivos colocados em Quarentena ou em Backup pelos aplicativos de segurança, assim como gerencie os arquivos para os quais o processamento pelos aplicativos antivírus foi adiado.

É possível comprar o Kaspersky Security Center pela Kaspersky (por exemplo, no site https://www.kaspersky.com) ou por meio de empresas parceiras.

Caso o Kaspersky Security Center seja adquirido por meio da Kaspersky, será possível copiar o aplicativo de nosso site. As informações necessárias para ativação do aplicativo são enviadas para o usuário por e-mail após o pagamento ser processado.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Requisitos de hardware e software

- Requisitos do Servidor de Administração
- Requisitos do Web Console
- Requisitos de servidores móveis
- Requisitos do Console de Administração
- Requisitos do Agente de Rede

Requisitos do Servidor de Administração

Requisitos mínimos de hardware:

- CPU com uma frequência operacional de 1 GHz ou superior. Para um sistema operacional de 64 bits, a frequência mínima de CPU é de 1.4 GHz.
- RAM: 4 GB.
- Espaço disponível em disco: 10 GB. Quando o Gerenciamento de sistemas for usado, pelo menos 100 GB de espaço livre em disco deve estar disponível.

Para implementação em ambientes de nuvem, os requisitos do Servidor de Administração e do servidor de banco de dados são idênticos aos requisitos do Servidor de Administração físico (dependendo de quantos dispositivos você deseja gerenciar).

Requisitos de software:

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

Os seguintes sistemas operacionais são compatíveis:

- Windows Server 2008 R2 Standard com Service Pack 1 e versões posteriores de 64 bits
- Windows Server 2012 Server Core 64 bits
- Windows Server 2012 Datacenter 64 bits
- Windows Server 2012 Essentials 64 bits
- Windows Server 2012 Foundation 64 bits
- Windows Server 2012 Standard 64 bits
- Windows Server 2012 R2 Server Core 64-bit
- Windows Server 2012 R2 Datacenter 64-bit
- Windows Server 2012 R2 Essentials 64 bits
- Windows Server 2012 R2 Foundation 64-bit
- Windows Server 2012 R2 Standard 64-bit
- Windows Server 2016 Datacenter (LTSB) 64 bits
- Windows Server 2016 Standard (LTSB) 64 bits
- Microsoft Windows Server 2016 Server Core (opção de Instalação) (LTSB) 64 bits

- Windows Server 2019 Standard 64 bits
- Windows Server 2019 Datacenter 64 bits
- Windows Server 2019 Core 64 bits
- Windows Server 2022 Standard 64 bits
- Windows Server 2022 Datacenter 64 bits
- Windows Server 2022 Core 64 bits
- Windows Storage Server 2012 64 bits
- Windows Storage Server 2012 R2 64 bits
- Windows Storage Server 2016 64 bits
- Windows Storage Server 2019 64 bits

As seguintes plataformas para virtualização são suportadas:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64 bits
- Microsoft Hyper-V Server 2012 R2 64 bits
- Microsoft Hyper-V Server 2016 64 bits
- Microsoft Hyper-V Server 2019 64 bits
- Microsoft Hyper-V Server 2022 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 17
- Oracle VM VirtualBox 6.x

Os seguintes servidores de banco de dados são compatíveis (podem ser instalados em um dispositivo diferente):

- Microsoft SQL Server® 2012 Express 64-bit com limitações
- Microsoft SQL Server 2014 Express 64 bits com limitações
- Microsoft SQL Server 2016 Express 64 bits com limitações
- Microsoft SQL Server 2017 Express 64 bits com limitações

- Microsoft SQL Server 2019 Express 64 bits com limitações
- Microsoft SQL Server 2014 (todas edições) 64 bits
- Microsoft SQL Server 2016 (todas edições) 64 bits
- Microsoft SQL Server 2017 (todas as edições) no Windows 64 bits
- Microsoft SQL Server 2017 (todas as edições) no Linux 64 bits
- Microsoft SQL Server 2019 (todas as edições) no Windows 64 bits (requer ações adicionais)
- Microsoft SQL Server 2019 (todas as edições) no Linux 64 bits (requer ações adicionais)
- Microsoft Azure SQL Database
- Todas as edições do SQL Server suportadas nas plataformas na nuvem Amazon RDS e Microsoft Azure
- MySQL 5.7 Community 32 bits/64 bits
- MySQL Standard Edition 8.0 (versão 8.0.20 e mais recentes) 32 bits/64 bits
- MySQL Enterprise Edition 8.0 (versão 8.0.20 e mais recentes) 32 bits/64 bits
- MariaDB 10.1 (compilação 10.1.30 e posterior) 32 bits/64 bits
- MariaDB 10.3 (modelo 10.3.22 e posterior) 32 bits/64 bits
- MariaDB 10.4 (modelo 10.4.26 e posterior) 32 bits/64 bits
- MariaDB 10.5 (compilação 10.5.27 e posterior) 32 bits/64 bits
- MariaDB Galera Cluster 10.3 32 bits/64 bits com mecanismo de armazenamento InnoDB
- PostgreSQL 13.x 64 bits
- PostgreSQL 14.x 64 bits
- Postgres Pro 13.x (todas as edições)
- Postgres Pro 14.x (todas as edições)

Consulte este tópico para obter detalhes e limitações: Selecionar um DBMS.

> Recomenda-se usar o MariaDB 10.3.22; ao usar uma versão anterior, a tarefa Executar o Windows Update poderá levar mais de um dia para funcionar.

SIEM e outros sistemas de gerenciamento de informações:

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

Requisitos do Web Console

Kaspersky Security Center Web Console Server

Requisitos mínimos de hardware:

- CPU: 4 núcleos, frequência operacional de 2,5 GHz
- RAM: 8 GB
- Espaço disponível em disco: 40 GB

Sistemas operacionais compatíveis com o Kaspersky Security Center Web Console Server

Sistemas operacionais. Microsoft Windows (somente as versões 64 bits):	Windows Server 2012 Server Core Windows Server 2012 Datacenter Windows Server 2012 Essentials Windows Server 2012 Foundation Windows Server 2012 Standard Windows Server 2012 R2 Server Core Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Essentials Windows Server 2012 R2 Foundation Windows Server 2012 R2 Standard Windows Server 2016 Datacenter (LTSB) Windows Server 2016 Standard (LTSB) Windows Server 2016 Server Core (opção de Instalação) (LTSB) Windows Server 2019 Standard Windows Server 2019 Datacenter Windows Server 2019 Core Windows Server 2022 Standard Windows Server 2022 Datacenter Windows Server 2022 Core Windows Storage Server 2012 Windows Storage Server 2012 R2 Windows Storage Server 2016 Windows Storage Server 2019
Sistemas operacionais. Linux (apenas versões de 64 bits)	Debian GNU/Linux 9.x (Stretch) Debian GNU/Linux 10.x (Buster) Debian GNU/Linux 11.x (Bullseye) Ubuntu Server 18.04 LTS (Bionic Beaver) Ubuntu Server 20.04 LTS (Focal Fossa) Ubuntu Server 22.04 LTS (Jammy Jellyfish) CentOS 7.x Red Hat Enterprise Linux Server 7.x Red Hat Enterprise Linux Server 8.x Red Hat Enterprise Linux Server 9.x SUSE Linux Enterprise Server 12 (todos os Service Packs) SUSE Linux Enterprise Server 15 (todos os Service Packs) Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.6) Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.7) Astra Linux Common Edition (atualização operacional 2.12)

	ALT Server 9.2 ALT Server 10 ALT 8 SP Server (LKNV.11100-01) ALT 8 SP Server (LKNV.11100-02) ALT 8 SP Server (LKNV.11100-03) Oracle Linux 7 Oracle Linux 8 Oracle Linux 9 RED OS 7.3 Server RED OS 7.3 Certified Edition Máquina virtual baseada em kernel (todos os sistemas operacionais Linux compatíveis com o Kaspersky Security Center Web Console Server)

Dispositivos cliente

Em um dispositivo cliente, o uso do Kaspersky Security Center Web Console requer apenas um navegador.

A resolução mínima da tela é de 1366x768 pixels.

Os requisitos de hardware e software para o dispositivo são idênticos aos requisitos do navegador utilizado com o Kaspersky Security Center Web Console.

Navegadores:

- Mozilla Firefox Extended Support Versão 91.8.0 ou posterior (91.8.0 lançada em 5 de abril de 2022)
- Google Chrome 100.0.4896.88 ou posterior (compilação oficial)
- Microsoft Edge 100 ou posterior
- Safari 15 no macOS

Requisitos de servidores móveis

Servidor de gerenciamento de dispositivos móveis do iOS (MDM do iOS)

Requisitos de hardware:

- CPU com uma frequência operacional de 1 GHz ou superior. Para um sistema operacional de 64 bits, a frequência mínima de CPU é de 1.4 GHz.
- RAM: 2 GB.
- Espaço disponível em disco: 2 GB.

Requisitos de software: Microsoft Windows (a versão do sistema operacional compatível é definida pelos requisitos do Servidor de Administração).

Servidor de dispositivos móveis Exchange

Todos os requisitos de software e hardware para o Servidor de dispositivos móveis Exchange estão incluídos nos requisitos para o Microsoft Exchange Server.

Compatibilidade com Microsoft Exchange Server 2007, Microsoft Exchange Server 2010 e Microsoft Exchange Server 2013 suportada.

Requisitos do Console de Administração

Requisitos de hardware:

- CPU com uma frequência operacional de 1 GHz ou superior. Para um sistema operacional de 64 bits, a frequência mínima de CPU é de 1.4 GHz.
- RAM: 512 MB.
- Espaço disponível em disco: 1 GB.

Requisitos de software:

- Microsoft Windows (a versão suportada do sistema operacional é determinada pelos requisitos do Servidor de Administração), exceto para os sistemas operacionais a seguir:
  - Windows Server 2012 Server Core 64 bits
  - Windows Server 2012 R2 Server Core 64-bit
  - Microsoft Windows Server 2016 Server Core (opção de Instalação) (LTSB) 64 bits
  - Windows Server 2019 Core 64 bits
  - Windows Server 2022 Core 64 bits
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 10.0 executando em:
  - Microsoft Windows Server 2008 R2 com Service Pack 1
  - Microsoft Windows Server 2012
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows 7 com Service Pack 1
  - Microsoft Windows 8
  - Microsoft Windows 8.1
  - Microsoft Windows 10

- Microsoft Internet Explorer 11.0 executando em:
  - Microsoft Windows Server 2012 R2
  - Microsoft Windows Server 2012 R2 com Service Pack 1
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2019
  - Microsoft Windows 7 com Service Pack 1
  - Microsoft Windows 8.1
  - Microsoft Windows 10
- Microsoft Edge executando no Microsoft Windows 10

Requisitos do Agente de Rede

Requisitos mínimos de hardware:

- CPU com uma frequência operacional de 1 GHz ou superior. Para um sistema operacional de 64 bits, a frequência mínima de CPU é de 1.4 GHz.
- RAM: 512 MB.
- Espaço disponível em disco: 1 GB.

Requisitos mínimos de hardware para Gerenciamento de vulnerabilidades e patches:

- CPU com frequência operacional de 1.4 GHz ou superior. É necessário um sistema operacional de 64 bits.
- RAM: 8 GB.
- Espaço disponível em disco: 1 GB.

Requisito de software para dispositivos baseados em Linux: o intérprete de linguagem Perl versão 5.10 ou posterior deve estar instalado.

Sistemas operacionais. Microsoft Windows	Microsoft Windows Embedded POSReady 2009 com o Service Pack de 32 bits mais recente Microsoft Windows Embedded POSReady 7 32 bits/64 bits Microsoft Windows Embedded 7 Standard with Service Pack 1 32 bits/64 bits Microsoft Windows Embedded 8 Standard 32 bits/64 bits Microsoft Windows Embedded 8.1 Industry Pro 32 bits/64 bits Microsoft Windows Embedded 8.1 Industry Enterprise 32 bits/64 bits Microsoft Windows Embedded 8.1 Industry Update 32 bits/64 bits Microsoft Windows 10 Enterprise 2015 LTSB 32 bits/64 bits Microsoft Windows 10 Enterprise 2016 LTSB 32 bits/64 bits Microsoft Windows 10 IoT Enterprise 2015 LTSB 32 bits/64 bits Microsoft Windows 10 IoT Enterprise 2016 LTSB 32 bits/64 bits Microsoft Windows 10 Enterprise 2019 LTSC 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1703 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1709 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1803 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1809 32 bits/64 bits Microsoft Windows 10 20H2 IoT Enterprise 32 bits/64 bits Microsoft Windows 10 21H2 IoT Enterprise 32 bits/64 bits Microsoft Windows 10 IoT Enterprise 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1909 32 bits/64 bits Microsoft Windows 10 IoT Enterprise LTSC 2021 32 bits/64 bits Microsoft Windows 10 IoT Enterprise versão 1607 32 bits/64 bits Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32 bits/64 bits Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32 bits/64 bits Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32 bits/64 bits Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32 bits/64 bits Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32 bits/64 bits Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32 bits/64 bits Microsoft Windows 10 Home RS5 (outubro de 2018) 32 bits/64 bits Microsoft Windows 10 Pro RS5 (outubro de 2018) 32 bits/64 bits Microsoft Windows 10 Pro for Workstations RS5 (outubro de 2018) 32 bits/64 bits Microsoft Windows 10 Enterprise RS5 (outubro de 2018) 32 bits/64 bits Microsoft Windows 10 Education RS5 (outubro de 2018) 32 bits/64 bits Microsoft Windows 10 Home 19H1 32 bits/64 bits Microsoft Windows 10 Pro 19H1 32 bits/64 bits Microsoft Windows 10 Pro for Workstations 19H1 32 bits/64 bits Microsoft Windows 10 Enterprise 19H1 32 bits/64 bits Microsoft Windows 10 Education 19H1 32 bits/64 bits Microsoft Windows 10 Home 19H2 32 bits/64 bits Microsoft Windows 10 Pro 19H2 32 bits/64 bits Microsoft Windows 10 Pro for Workstations 19H2 32 bits/64 bits Microsoft Windows 10 Enterprise 19H2 32 bits/64 bits Microsoft Windows 10 Education 19H2 32 bits/64 bits Microsoft Windows 10 Home 20H1 (Atualização de maio de 2020) 32 bits/64 bits Microsoft Windows 10 Pro 20H1 (Atualização de abril de 2020) 32 bits/64 bits Microsoft Windows 10 Enterprise 20H1 (Atualização de maio de 2020) 32 bits/64 bits Microsoft Windows 10 Education 20H1 (Atualização de maio de 2020) 32 bits/64 bits Microsoft Windows 10 Home 20H2 (Atualização de outubro de 2020) 32 bits/64 bits Microsoft Windows 10 Pro 20H2 (Atualização de outubro de 2020) 32 bits/64 bits Microsoft Windows 10 Enterprise 20H2 (Atualização de outubro de 2020) 32 bits/64 bits Microsoft Windows 10 Education 20H2 (Atualização de outubro de 2020) 32 bits/64 bits

Microsoft Windows 10 Home 21H1 (Atualização de maio de 2021) 32 bits/64 bits

Microsoft Windows 10 Pro 21H1 (Atualização de abril de 2021) 32 bits/64 bits

Microsoft Windows 10 Enterprise 21H1 (Atualização de maio de 2021) 32 bits/64 bits

Microsoft Windows 10 Education 21H1 (Atualização de maio de 2021) 32 bits/64 bits

Microsoft Windows 10 Home 21H2 (Atualização de outubro de 2021) 32 bits/64 bits

Microsoft Windows 10 Pro 21H2 (Atualização de outubro de 2021) 32 bits/64 bits

Microsoft Windows 10 Enterprise 21H2 (Atualização de outubro de 2021) 32 bits/64 bits

Microsoft Windows 10 Education 21H2 (Atualização de outubro de 2021) 32 bits/64 bits

Microsoft Windows 10 Home 22H2 (atualização de outubro de 2023) 32/64 bits

Microsoft Windows 10 Pro 22H2 (atualização de outubro de 2023) 32/64 bits

Microsoft Windows 10 Enterprise 22H2 (atualização de outubro de 2023) 32/64 bits

Microsoft Windows 10 Education 22H2 (atualização de outubro de 2023) 32/64 bits

Microsoft Windows 11 Home 64 bits

Microsoft Windows 11 Pro 64 bits

Microsoft Windows 11 Enterprise 64 bits

Microsoft Windows 11 Education 64 bits

Microsoft Windows 11 22H2

Microsoft Windows 8.1 Pro 32 bits/64 bits

Microsoft Windows 8.1 Enterprise 32 bits/64 bits

Microsoft Windows 8 Pro 32 bits/64 bits

Microsoft Windows 8 Enterprise 32 bits/64 bits

Microsoft Windows 7 Professional com Service Pack 1 e versões posteriores de 32 bits/64 bits

Microsoft Windows 7 Enterprise/Ultimate com Service Pack 1 e versões posteriores de 32 bits/64 bits

Microsoft Windows 7 Home Basic/Premium com Service Pack 1 e versões posteriores de 32 bits/64 bits

Microsoft Windows XP Professional com Service Pack 2 32 bits/64 bits (compatível apenas com a versão 10.5.1781 do Agente de Rede, que você pode solicitar por meio do Suporte Técnico)

Microsoft Windows XP Professional com Service Pack 3 e superior a 32 bits (compatível com o Agente de Rede versão 14.0.0.20023)

Microsoft Windows XP Professional for Embedded Systems com Service Pack 3 de 32 bits (compatível com o Agente de Rede versão 14.0.0.20023)

Windows Small Business Server 2011 Essentials 64 bits

Windows Small Business Server 2011 Premium Add-on 64 bits

Windows Small Business Server 2011 Standard 64 bits

Windows MultiPoint Server 2011 Standard/Premium 64 bits

Windows MultiPoint Server 2012 Standard/Premium 64 bits

Windows Server 2003 SP1 32 bits/64 bits (compatível apenas com a versão 10.5.1781 do Agente de Rede)

Windows Server 2003 SP2 Standard/Enterprise 32 bits/64 bits (compatível apenas com a versão 10.5.1781 do Agente de Rede)

Windows Server 2003 R2 Standard/Enterprise com SP2 32 bits/64 bits (compatível apenas com a versão 10.5.1781 do Agente de Rede)

Windows Server 2008 Foundation Service Pack 2 de 32 bits/64 bits

Windows Server 2008 com Service Pack 2 (todas as edições) 32 bits/64 bits

Windows Server 2008 R2 Datacenter com Service Pack 1 e versões posteriores 64 bits

Windows Server 2008 R2 Enterprise com Service Pack 1 e versões posteriores 64 bits

Windows Server 2008 R2 Foundation Service Pack 1 e versões posteriores de 64 bits

Windows Server 2008 R2 Core Mode Service Pack 1 e versões posteriores 64 bits

Windows Server 2008 R2 Standard com Service Pack 1 e versões posteriores de 64 bits

Windows Server 2008 R2 com Service Pack 1 (todas as edições) 64 bits

Windows Server 2012 Server Core 64 bits

Windows Server 2012 Datacenter 64 bits

Windows Server 2012 Essentials 64 bits

Windows Server 2012 Foundation 64 bits

Windows Server 2012 Standard 64 bits

Windows Server 2012 R2 Server Core 64-bit

Windows Server 2012 R2 Datacenter 64-bit

Windows Server 2012 R2 Essentials 64 bits

Windows Server 2012 R2 Foundation 64-bit

	Windows Server 2012 R2 Standard 64-bit Windows Server 2016 Datacenter (LTSB) 64 bits Windows Server 2016 Standard (LTSB) 64 bits Microsoft Windows Server 2016 Server Core (opção de Instalação) (LTSB) 64 bits Windows Server 2019 Standard 64 bits Windows Server 2019 Datacenter 64 bits Windows Server 2019 Core 64 bits Windows Server 2022 Standard 64 bits Windows Server 2022 Datacenter 64 bits Windows Server 2022 Core 64 bits Windows Storage Server 2012 64 bits Windows Storage Server 2012 R2 64 bits Windows Storage Server 2016 64 bits Windows Storage Server 2019 64 bits
Sistemas operacionais. Linux	Debian GNU/Linux 9.x (Stretch) 32 bits/64 bits Debian GNU/Linux 10.x (Buster) 32 bits/64 bits Debian GNU / Linux 11.x (Bullseye) 32 bits/64 bits Ubuntu Server 18.04 LTS (Bionic Beaver) 32 bits/64 bits Ubuntu Server 20.04 LTS (Focal Fossa) 32 bits/64 bits Ubuntu Server 20.04.04 LTS (Focal Fossa) ARM 64 bits Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32 bits/64 bits Ubuntu Desktop 20.04 LTS (Focal Fossa) 32 bits/64 bits Ubuntu Server 22.04 LTS (Jammy Jellyfish) 64 bits CentOS 7.x 64 bits CentOS 7.x ARM 64 bits Red Hat Enterprise Linux Server 6.x 32 bits/64 bits Red Hat Enterprise Linux Server 7.x 64 bits Red Hat Enterprise Linux Server 8.x 64 bits Red Hat Enterprise Linux Server 9.x 64 bits SUSE Linux Enterprise Server 12 (todos Service Packs) 64 bits SUSE Linux Enterprise Server 15 (todos os Service Packs) 64 bits SUSE Linux Enterprise Desktop 15 (todos os Service Packs) 64 bits SUSE Linux Enterprise Desktop 15 com Service Pack 3 ARM 64 bits openSUSE 15 64 bits EulerOS 2.0 SP8 ARM Pardus OS 19.1 64 bits Astra Linux Common Edition (atualização operacional 2.12) de 64 bits Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.6) de 64 bits Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.7) de 64 bits Astra Linux Special Edition RUSB.10152-02 (atualização operacional 4.7) ARM de 64 bits ALT Server 9.2 64 bits ALT Server 10 64 bits ALT Workstation 9.2 32 bits/64 bits ALT Workstation 10 32 bits/64 bits ALT 8 SP Server (LKNV.11100-01) 64 bits ALT 8 SP Server (LKNV.11100-02) 64 bits ALT 8 SP Server (LKNV.11100-03) 64 bits ALT 8 SP Workstation (LKNV.11100-01) 32 bits/64 bits ALT 8 SP Workstation (LKNV.11100-02) 32 bits/64 bits ALT 8 SP Workstation (LKNV.11100-03) 32 bits/64 bits Mageia 4 32 bits Oracle Linux 7 64 bits Oracle Linux 8 64 bits Oracle Linux 9 64 bits Linux Mint 19.x 32 bits Linux Mint 20.x 64 bits

	AlterOS 7.5 e versões posteriores de 64 bits GosLinux IC6 64 bits RED OS 7.3 Server 64 bits RED OS 7.3 Certified Edition 64 bits ROSA COBALT 7.9 64 bits ROSA CHROME 12 64 bits Lotos (Linux core versão 4.19.50, DE: MATE) 64 bits
Sistemas operacionais macOS	Para obter a lista de sistemas operacionais compatíveis, consulte a Ajuda do Kaspersky Endpoint Security for Mac.

Para o Agente de Rede, a arquitetura Apple Silicon (M1) também é compatível, assim como Intel.

As seguintes plataformas para virtualização são suportadas:

- VMware vSphere 6.7
- VMware vSphere 7.0
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64 bits
- Microsoft Hyper-V Server 2012 R2 64 bits
- Microsoft Hyper-V Server 2016 64 bits
- Microsoft Hyper-V Server 2019 64 bits
- Microsoft Hyper-V Server 2022 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Máquina virtual baseada em kernel (todos os sistemas operacionais Linux compatíveis com o Agente de Rede)

Em dispositivos executando o Windows 10 versão RS4 ou RS5, o Kaspersky Security Center pode não ser capaz de detectar algumas vulnerabilidades em pastas onde a diferenciação de maiúsculas e minúsculas estiver ativada.

Antes de instalar o Agente de Rede nos dispositivos que executam o Windows 7, Windows Server 2008, Windows Server 2008 R2 ou Windows Small Business Server 2011 Premium Add-on, verifique e confirme se a atualização de segurança KB3063858 para SO Windows foi instalada: Atualização de segurança para Windows 7 (KB3063858), Atualização de segurança para Windows 7 para sistemas baseados em x64 (KB3063858), Atualização de segurança para Windows Server 2008 (KB3063858), Atualização de segurança para Windows Server 2008 x64 Edition (KB3063858), Atualização de segurança para Windows Server 2008 R2 x64 Edition (KB3063858).

No Microsoft Windows XP, o Agente de Rede poderá não executar algumas operações corretamente.

É possível instalar ou atualizar o Agente de Rede para Windows XP somente no Microsoft Windows XP. As edições compatíveis do Microsoft Windows XP e suas versões correspondentes do Agente de Rede estão indicadas na lista de sistemas operacionais compatíveis. É possível baixar a versão necessária do Agente de Rede para Microsoft Windows XP nesta página.

Recomendamos a instalação da mesma versão ou mais recente do Agente de Rede para Linux que o Kaspersky Security Center.

O Kaspersky Security Center é totalmente compatível com o Agente de Rede da mesma versão ou de versões mais recentes.

O Agente de Rede para macOS é fornecido com o aplicativo de segurança Kaspersky para este sistema operacional.

Aplicativos e soluções da Kaspersky compatíveis

O Kaspersky Security Center é compatível com a implementação e o gerenciamento centralizados de todos os aplicativos e soluções da Kaspersky que são compatíveis atualmente. A tabela abaixo mostra quais aplicativos e soluções da Kaspersky são compatíveis com o Console de Administração baseado em MMC e o Kaspersky Security Center Web Console. Para conhecer as versões dos aplicativos e soluções, consulte a página da Web de ciclo de vida de suporte ao produto.

Lista de aplicativos e soluções Kaspersky compatíveis com o Kaspersky Security Center

Nome do aplicativo ou solução da Kaspersky	Compatível com o Console de Administração baseado em MMC	Compatível com o Kaspersky Security Center Web Console
Para estações de trabalho		
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 Embedded Systems Security for Linux	—	✓
Para soluções industriais		
Kaspersky Industrial CyberSecurity for Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Linux Nodes	✓	✓
Kaspersky Industrial CyberSecurity for Networks (não é compatível com implementação centralizada)	✓	✓
Para dispositivos móveis		
Kaspersky Endpoint Security for Android	✓	✓
Kaspersky Security for iOS	—	✓
Para servidores de arquivos		
Kaspersky Security for Windows Server	✓	✓

Nome do aplicativo ou solução da Kaspersky	Compatível com o Console de Administração baseado em MMC	Compatível com o Kaspersky Security Center Web Console
Kaspersky Endpoint Security for Windows	✓	✓
Kaspersky Endpoint Security for Linux	✓	✓
Para ambientes virtuais		
Kaspersky Security for Virtualization Light Agent	✓	✓
Kaspersky Security for Virtualization Agentless	✓	—
Para servidores de correio e colaboração		
Kaspersky Security para Linux Mail Server	✓	—
Kaspersky Security for Microsoft Exchange Servers	✓	—
Para detecção de ataques direcionados		
Kaspersky Sandbox Server	—	✓
Kaspersky Endpoint Detection and Response Optimum	—	✓
Kaspersky Managed Detection and Response	—	✓
Para dispositivos KasperskyOS		
Kaspersky IoT Secure Gateway	—	✓
Kaspersky Thin Client	—	✓

Licenças e recursos do Kaspersky Security Center 14.2

O Kaspersky Security Center requer uma licença para o uso de alguns recursos.

A tabela abaixo mostra qual licença cobre quais recursos do Kaspersky Security Center.

Para ativar os recursos do Kaspersky Security Center, é necessário ativar o Servidor de Administração com a adição de uma chave de licença do Servidor de Administração.

É necessário adicionar manualmente uma chave de licença para cada Servidor de Administração.

Licenciamentos e recursos do Kaspersky Security Center

Recursos do Kaspersky Security Center	Gerenciamento de patches e vulnerabilidades 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
Avaliação de vulnerabilidade	✓	✓	✓	✓	✓	✓	✓
Gerenciamento de patches	✓	—	✓	✓	—	✓	✓
Controle de acesso baseado em função	✓	✓	✓	✓	✓	✓	✓
Instalação de sistemas operacionais e aplicativos	✓	—	✓	✓	—	✓	✓

Recursos do Kaspersky Security Center	Gerenciamento de patches e vulnerabilidades 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
Gerenciamento de Dispositivos Móveis (ou seja os dispositivos iOS e Android dos usuários)	✓	✓	✓	✓	–	–	✓
Configurar o ambiente em nuvem para trabalhar em ambientes em nuvem, como AWS, Microsoft Azure ou Google Cloud	–	–	–	–	✓	✓	–
Exportando eventos para os sistemas SIEM: Syslog	✓	✓	✓	✓	✓	✓	✓
Exportação de eventos para sistemas SIEM: QRadar da IBM e ArcSight da Micro Focus	✓	✓	✓	✓	✓	✓	✓

Sobre a compatibilidade do Servidor de Administração e Kaspersky Security Center Web Console

É recomendável usar a versão mais recente do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center Web Console; caso contrário, a funcionalidade do Kaspersky Security Center estará limitada.

Você pode instalar e fazer o upgrade do Servidor de Administração do Kaspersky Security Center e o Kaspersky Security Center Web Console de forma independente. Neste caso, garanta que a versão do Kaspersky Security Center Web Console instalado seja compatível com a versão do Servidor de Administração ao qual você se conecta:

- O Web Console incluído no Kaspersky Security Center 14.2 Windows é compatível com o Servidor de Administração do Kaspersky Security Center para as seguintes versões: 14.2, 14 e 13.2.
- O Servidor de Administração incluído no Kaspersky Security Center 14.2 Windows é compatível com o Kaspersky Security Center Web Console nas seguintes versões: 14.2, 14 e 13.2 para Windows e 15 para Linux.

Comparativo do Kaspersky Security Center: baseado em Windows X baseado em Linux

A Kaspersky fornece o Kaspersky Security Center como uma solução local para duas plataformas: Windows e Linux. Na solução baseada em Windows, você instala o Servidor de Administração em um dispositivo Windows e a solução baseada em Linux tem a versão do Servidor de Administração projetada para ser instalada em um dispositivo Linux. Esta Ajuda on-line contém informações sobre o Kaspersky Security Center Windows. Para obter informações detalhadas sobre a solução baseada em Linux, consulte a Ajuda on-line do Kaspersky Security Center Linux.

A tabela abaixo permite comparar os principais recursos do Kaspersky Security Center como uma solução baseada no Windows e como uma solução baseada no Linux.

Comparativo de recursos do Kaspersky Security Center funcionando como uma solução baseada em Windows e uma solução baseada em Linux

Recurso ou propriedade	Kaspersky Security Center 14.2	
	Solução baseada em Windows	**Solução baseada em Linux**
Localização do Servidor de Administração	No local	No local
Localização do sistema de gerenciamento de banco de dados (DBMS)	No local	No local
Sistema operacional para instalar o Servidor de Administração	Windows	Linux
Tipo de console de administração	Local e baseado na web	Baseado na web
Sistema operacional para instalar o Console de Administração baseado na web no	Windows ou no Linux	Linux
Hierarquia de Servidores de Administração	✓	✓
Hierarquia do grupo de administração	✓	✓
Sondagem da rede	✓	✓ (apenas por intervalos de IP)
Número máximo de dispositivos gerenciados	100.000	20.000
Proteção de dispositivos gerenciados Windows, macOS e Linux	✓	✓ (proteção apenas para dispositivos Linux e Windows)
Proteção de dispositivos móveis	✓	—
Proteção de máquinas virtuais	✓	—
Proteção da infraestrutura de nuvem pública	✓	—
Gerenciamento de segurança centrada no dispositivo	✓	✓
Gerenciamento de segurança centrada no usuário	✓	✓
Políticas do aplicativo	✓	✓
Tarefas para aplicativos da Kaspersky	✓	✓
Kaspersky Security Network	✓	✓
Proxy da KSN	✓	✓
Kaspersky Private Security Network	✓	✓
Implementação centralizada de chaves de licença para aplicativos da Kaspersky	✓	✓
Atualização automática dos bancos de dados de antivírus	✓	✓
Suporte para Servidores de administração virtuais	✓	✓

Recurso ou propriedade	Kaspersky Security Center 14.2	
	Solução baseada em Windows	Solução baseada em Linux
Instalar atualizações de softwares de terceiros e corrigir vulnerabilidades de softwares de terceiros	✓	— (usando apenas uma tarefa de instalação remota)
Notificações sobre eventos ocorridos em dispositivos gerenciados	✓	✓
Criação e gerenciamento de contas de usuário	✓	✓
Entrar no console usando a autenticação do domínio	✓	—
Integração com sistemas SIEM	✓	✓ (usando apenas o Syslog)
Monitoramento do status de políticas e tarefas	✓	✓
Implementação do cluster de failover do Kaspersky Security Center	✓	✓
Instalação do Servidor de Administração em um cluster de failover da Microsoft	✓	—
Uso do SNMP para enviar estatísticas ao Servidor de Administração aos aplicativos de terceiros	✓	—
Diagnóstico remoto de dispositivos cliente	✓	—
Conexão remota na área de trabalho de um dispositivo cliente	✓	—
Gerenciar revisões de objeto	✓	—
Atualização automática dos aplicativos Kaspersky	✓	—
Implementação de sistemas operacionais em dispositivos cliente	✓	—
Servidor Web para publicação de pacotes de instalação e outros arquivos	✓	—
Exibir e trabalhar com alertas detectados pelo Kaspersky Endpoint Detection and Response Optimum	✓	—
Usar Servidor de Administração como servidor WSUS	✓	—
Integração com o Kaspersky Managed Detection and Response	✓	—
Suporte ao Controle Adaptativo de Anomalia	✓	—
Suporte a clusters e matrizes de servidores em grupos de administração	✓ (apenas no Console de Administração baseado em MMC)	—
Gerenciamento de licenças de terceiros	✓	—

Sobre o Kaspersky Security Center Cloud Console

Usar o Kaspersky Security Center como um aplicativo local significa que o usuário instala o Kaspersky Security Center, incluindo o Servidor de Administração, em um dispositivo local e gerencia o sistema de segurança de rede por meio do Console de Administração baseado no console de gerenciamento Microsoft (disponível somente no Kaspersky Security Center Windows) ou no Kaspersky Security Center Web Console.

No entanto, é possível usar o Kaspersky Security Center como um serviço de nuvem. Nesse caso, o Kaspersky Security Center é instalado e mantido no ambiente em nuvem pelos especialistas da Kaspersky, e a Kaspersky fornece o acesso ao Servidor de Administração como um serviço. Você gerencia o sistema de segurança da rede através do Console de Administração baseado na nuvem chamado Kaspersky Security Center Cloud Console. Esse console tem uma interface semelhante à interface do Kaspersky Security Center Web Console.

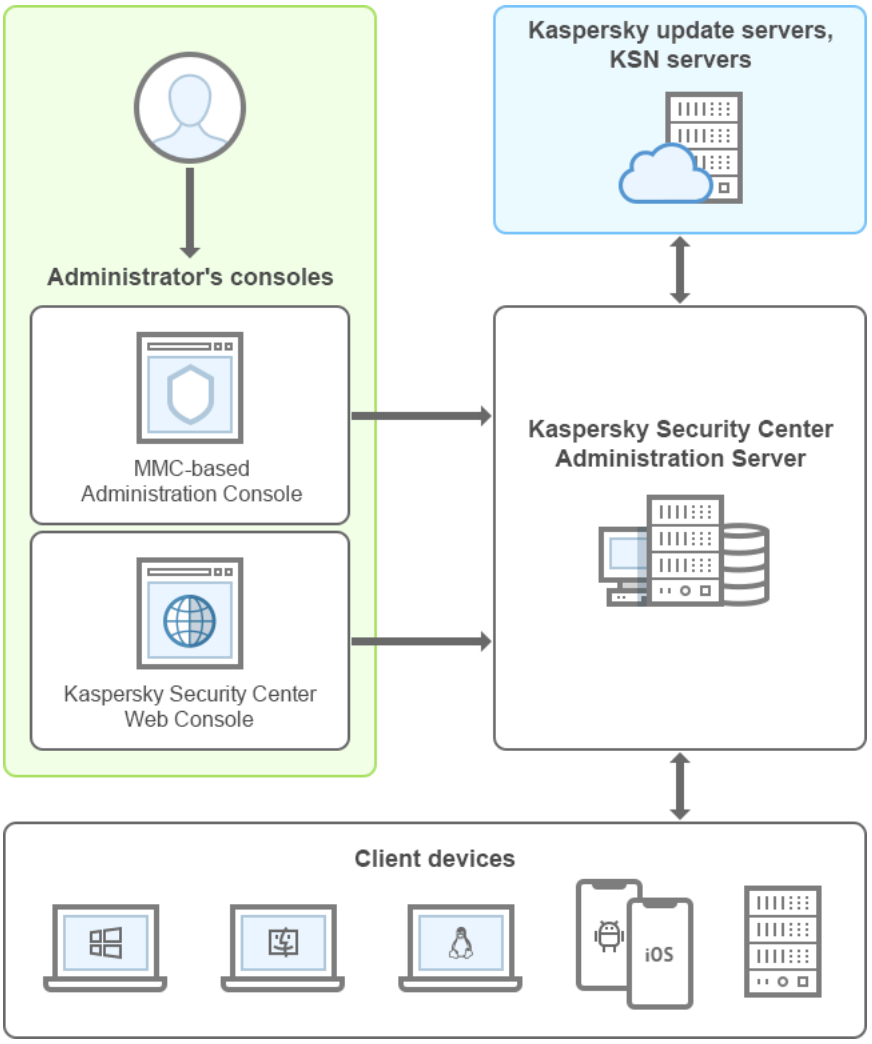
A interface e a documentação do Kaspersky Security Center Cloud Console estão disponíveis nos seguintes idiomas:

- Inglês
- Francês
- Alemão
- Italiano
- Japonês
- Português (Brasil)
- Russo
- Chinês simplificado
- Espanhol
- Espanhol (LATAM)
- Chinês tradicional

Mais informações sobre o Kaspersky Security Center Cloud Console e os seus recursos estão disponíveis na documentação do Kaspersky Security Center Cloud Console e na documentação do Kaspersky Endpoint Security for Business.

Arquitetura

Esta seção fornece uma descrição dos componentes do Kaspersky Security Center e sua interação.



Arquitetura do Kaspersky Security Center

O Kaspersky Security Center inclui os seguintes componentes básicos:

- *Console de Administração* (aqui também referido como *Console*). Fornece uma interface de usuário para os serviços de administração do Servidor de Administração e do Agente de Rede. O Console de Administração é implementado como um snap-in do Microsoft Management Console (MMC). O Console de Administração permite a conexão remota ao Servidor de Administração pela Internet.

- *Kaspersky Security Center Web Console*. Fornece uma interface Web para criar e manter o sistema de proteção da rede de uma organização cliente gerenciada pelo Kaspersky Security Center.

- *Servidor de Administração do Kaspersky Security Center* (também chamado de *Servidor*). Centraliza o armazenamento das informações sobre os aplicativos instalados na rede da organização e a forma como é possível gerenciá-los.

- *Servidores de atualização Kaspersky*. Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

- *Servidores da KSN*. Servidores que contêm informações o banco de dados da Kaspersky com informações constantemente atualizadas sobre a reputação de arquivos, recursos da Web e software. O Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky quanto a ameaças, aprimora o desempenho de alguns componentes de proteção e reduz a probabilidade ocorrerem falsos positivos.

- *Dispositivos cliente*. Dispositivos da empresa cliente protegidos pelo Kaspersky Security Center. Cada dispositivo que precisa ser protegido deve ter um dos aplicativos de segurança da Kaspersky instalado.

Cenário principal de implementação

Seguindo este cenário, você pode implementar o Servidor de Administração, bem como instalar Agente de Rede e aplicativos de segurança nos dispositivos na rede. Você pode usar este cenário para um exame mais próximo no aplicativo e como para a instalação do aplicativo para trabalho adicional.

A instalação do Kaspersky Security Center consiste nas seguintes etapas:

1. Trabalho de preparação

2. Instalação do Kaspersky Security Center e de um aplicativo de segurança Kaspersky no Servidor de Administração

3. Implementação centralizada de aplicativos de segurança Kaspersky em dispositivos clientes

A implementação do Kaspersky Security Center no ambientes de nuvem e a implementação do Kaspersky Security Center para provedores de serviços é descrita em outras seções da Ajuda.

Recomendamos que você atribua um mínimo de uma hora para a instalação do Servidor de Administração e um mínimo de um dia útil para a conclusão do cenário. Também recomendamos que você instale um aplicativo de segurança, tal como o Kaspersky Security for Windows Server ou o Kaspersky Endpoint Security, no computador que atuará como o Servidor de Administração do Kaspersky Security Center.

Quando houver a conclusão do cenário, a proteção será implementada na rede da organização da seguinte forma:

- O DBMS será instalado para o Servidor de Administração.

- O Servidor de Administração do Kaspersky Security Center será instalado.

- Todas as políticas e tarefas necessárias serão criadas; as configurações padrão das políticas e tarefas serão especificadas.

- Os aplicativos de segurança (por exemplo, o Kaspersky Endpoint Security for Windows) e o Agente de Rede serão instalados nos dispositivos gerenciados.

- Os grupos de administração serão criados (possivelmente combinados em uma hierarquia).

- A proteção do dispositivo móvel será implementada, se necessário.

- Os pontos de distribuição serão atribuídos, se necessário.

A instalação do Kaspersky Security Center é feita em fases:

Trabalho de preparação

1 Obtendo os arquivos necessários

Certifique-se de possuir uma chave de licença (código de ativação) para o Kaspersky Security Center ou para os aplicativos de segurança Kaspersky.

Descompacte o arquivo recebido do fornecedor. Este arquivo contém as chaves de licença (arquivos KEY), códigos de ativação e a lista de aplicativos Kaspersky que podem ser ativados por cada chave de licença.

Se deseja experimentar o Kaspersky Security Center primeiro, você pode obter uma avaliação gratuita de 30 dias no site da Kaspersky.

Para obter informações detalhadas sobre o licenciamento dos aplicativos de segurança Kaspersky que não estão incluídos no Kaspersky Security Center, você pode consultar a documentação desses aplicativos.

2 Selecionar uma estrutura para a proteção de uma organização

Saiba mais sobre os componentes do Kaspersky Security Center. Selecione a estrutura de proteção e configuração de rede que se adeque melhor à sua organização. Com base na configuração da rede e na produtividade dos canais de comunicação, defina o número de Servidores de Administração a serem usados e como eles devem ser distribuídos entre seus escritórios (se você executar uma rede distribuída).

Para obter e manter o desempenho ótimo sob a variação de condições operacionais, leve em conta o número de dispositivos na rede, a topologia da rede e o conjunto de recursos do Kaspersky Security Center que você necessita (para obter mais detalhes, consulte o Guia de Dimensionamento do Kaspersky Security Center).

Defina se uma hierarquia de Servidores de Administração será usada na sua organização. Para fazer isto, você deve avaliar se é possível e conveniente cobrir todos os dispositivos clientes com um único Servidor de Administração ou se é necessário criar uma hierarquia de Servidores de Administração. Você também deveria criar uma hierarquia de Servidores de Administração que seja idêntica à estrutura organizacional da sua organização cuja rede você pretende proteger.

Se você tiver que assegurar a proteção de dispositivos móveis, execute todas as ações de pré-requisito necessárias para a configuração de um Servidor de dispositivos móveis Exchange e Servidor de MDM do iOS.

Assegure-se de que os dispositivos que você selecionou como Servidores de Administração, assim como aqueles para a instalação do Console de Administração, atendam todos os requisitos de hardware e software.

3 Preparação para o uso de certificados personalizados

Se a infraestrutura de chave pública (PKI) da sua organização exige que você use certificados personalizados emitidos por uma autoridade de certificação (CA) específica, prepare esses certificados e garanta que eles atendam a todos os requisitos.

4 Preparação para licenciamento do Kaspersky Security Center

Se você planeja usar uma versão do Kaspersky Security Center com o Gerenciamento de Dispositivos Móveis, com a Integração com os sistemas SIEM, e/ou com o suporte ao Gerenciamento de patches e vulnerabilidades, assegure-se de que tenha um arquivo de chave ou um código de ativação para o licenciamento do aplicativo.

5 Preparação para licenciamento de aplicativos de segurança gerenciados

Durante a implementação da proteção, você precisa fornecer à Kaspersky as chaves de licença ativas para os aplicativos que pretende gerenciar por meio do Kaspersky Security Center (consulte a lista de aplicativos de segurança gerenciáveis). Para obter informações detalhadas sobre o licenciamento de cada aplicativo de segurança, consulte a documentação deste aplicativo.

6 Selecionar a configuração de hardware do Servidor de Administração e DBMS

Planejar a configuração de hardware para o DBMS e Servidor de Administração, considerando o número de dispositivos na sua rede.

7 Selecionar um DBMS

Ao selecionar um DBMS, leve em conta o número de dispositivos gerenciados a ser cobertos por este Servidor de Administração. Se sua rede incluir menos de 10.000 dispositivos e você não planeja aumentar esta quantidade, poderá selecionar um DBMS gratuito, tal como o SQL Express ou MySQL, e instalá-lo no mesmo dispositivo que o do Servidor de Administração. Outra opção é escolher o MariaDB DBMS, que permite gerenciar até 20.000 dispositivos. Se a sua rede incluir mais de 10.000 dispositivos (ou se você planejar expandir a sua rede até aquele número de dispositivos), recomendamos que você selecione um DBMS SQL pago e o instale em um dispositivo dedicado. Um DBMS pago pode funcionar com múltiplos Servidores de Administração, enquanto que um DBMS gratuito somente pode funcionar com um.

Se você selecionar o SQL Server DBMS, observe que você pode migrar os dados armazenados no banco de dados para MySQL, MariaDB ou Azure SQL DBMS. Para fazer a migração, faça o backup dos dados e restaure-os no novo DBMS.

8. **Instalar o DBMS e criar o banco de dados**

Saiba mais sobre as contas de trabalho com o DBMS e instale o seu DBMS.

Antes da instalação, escolha um DBMS compatível. Você pode selecionar, por exemplo, PostgreSQL, Postgres Pro, Microsoft SQL Server, MySQL ou MariaDB.

Para obter informações sobre como instalar o DBMS selecionado, consulte a sua documentação.

Se você instalar MariaDB, MySQL, PostgreSQL ou Postgre Pro, use as configurações recomendadas para garantir que o DBMS funcione corretamente.

Anote e salve as configurações do DBMS porque precisará delas durante a instalação do Servidor de Administração. Estas configurações incluem o nome do servidor SQL, o número da porta usada para conectar-se ao SQL Server e o nome da conta e senha para acessar o SQL Server.

> Se você decidir instalar o DBMS PostgreSQL ou Postgres Pro, certifique-se de ter especificado uma senha para o superusuário. Se a senha não for especificada, o Servidor de Administração pode não conseguir se conectar ao banco de dados.

Por padrão, o Instalador do Kaspersky Security Center cria o banco de dados para o armazenamento das informações do Servidor de Administração, mas você pode optar por não criar este banco de dados e usar um banco de dados diferente em vez deste. Neste caso, assegure-se de que o banco de dados tenha sido criado, você saiba o nome dele e de que a conta a partir da qual o Servidor de Administração acessará esse banco de dados tenha a função db_owner para ele.

Se necessário, contate seu administrador de DBMS para obter mais informações.

9. **Configuração de portas**

Assegure-se de que todas as portas necessárias estão abertas para a interação entre os componentes de acordo com a sua estrutura de segurança selecionada.

Se tiver que de fornecer acesso à Internet para o Servidor de Administração, configure as portas e especifique as configurações de conexão, dependendo da configuração da rede.

10. **Verificação de contas**

Assegure-se de que você tenha todos os direitos de administrador local necessários para a instalação bem-sucedida do Servidor de Administração do Kaspersky Security Center para a implementação da proteção adicional nos dispositivos. Os direitos de administrador local em dispositivos cliente são necessários para a instalação do Agente de Rede nestes dispositivos. Após a instalação do Agente de Rede, você pode usá-lo para instalar aplicativos nos dispositivos remotamente sem usar a conta com os direitos de administrador de dispositivo.

Por padrão, no dispositivo selecionado para a instalação do Servidor de Administração, o Instalador do Kaspersky Security Center cria três contas locais abaixo sob as quais o Servidor de Administração e os serviços do Kaspersky Security Center serão executados:

- KL-AK-*: Conta do serviço do Servidor de Administração

- NT Service/KSC*: Contas para outros serviços do grupo de Servidores de Administração
- KlPxeUser: Conta para a implementação de sistemas operacionais

Você pode optar por não criar contas dos serviços do Servidor de Administração e outros serviços. Você usará as suas contas existentes em vez das contas de domínio, tal como contas de domínio, se planejar instalar o Servidor de Administração em um cluster de correção de falhas ou planejar usar contas de domínio em vez de contas locais por algum outro motivo. Nesse caso, certifique-se de que as contas destinadas a executar o Servidor de Administração e os serviços do Kaspersky Security Center tenham sido criadas, não são privilegiadas e possuam todas as permissões necessárias para acessar o DBMS. (Se você planeja uma implementação adicional de sistemas operacionais em dispositivos por meio do Kaspersky Security Center, não desative a criação de contas.)

Instalação do Kaspersky Security Center e de um aplicativo de segurança Kaspersky no Servidor de Administração

1. **Instalar o Servidor de Administração, Console de Administração, Kaspersky Security Center Web Console e plugins de gerenciamento para os aplicativos de segurança**

   Faça o download do Kaspersky Security Center no site da Kaspersky. Você pode fazer o download do pacote completo, apenas do Console da Web ou do Console de Administração.

   Instale o Servidor de Administração no dispositivo selecionado (ou vários dispositivos, se planejar usar múltiplos Servidores de Administração). Você pode selecionar a instalação padrão ou personalizada do Servidor de Administração. O Console de Administração será instalada junto com o Servidor de Administração. Recomenda-se instalar o Servidor de Administração em um servidor dedicado em vez de um controlador de domínio.

   Instalação padrão é recomendada se você quiser testar o Kaspersky Security Center ao, por exemplo, testar a sua operação em uma pequena área dentro sua rede. Durante a instalação padrão, você somente configura o banco de dados. Você também pode instalar somente o conjunto padrão de plugins de gerenciamento de aplicativos Kaspersky. Você também poderá usar a instalação padrão se já tiver alguma experiência em trabalhar com o Kaspersky Security Center e conseguir especificar todas as configurações relevantes após a instalação padrão.

   A instalação personalizada será recomendada se você planejar modificar as configurações do Kaspersky Security Center, como o caminho para a pasta compartilhada, contas, e portas para a conexão ao Servidor de Administração e as configurações do banco de dados. A instalação personalizada permite especificar quais plugins de gerenciamento da Kaspersky devem ser instalados. Caso necessário, é possível iniciar a instalação personalizada no modo silencioso.

   O Console de Administração e a versão do servidor do Agente de Rede são instaladas em conjunto com o Servidor de Administração. Você também pode optar por instalar o Kaspersky Security Center Web Console durante a instalação.

   Se quiser, instale o Console de Administração e/ou Kaspersky Security Center Web Console na estação de trabalho do administrador separadamente para gerenciar o Servidor de Administração pela rede.

2. **Configuração inicial e licenciamento**

   Quando a instalação de Servidor de Administração estiver concluída, na primeira conexão ao Servidor de Administração o Assistente de início rápido inicia automaticamente. Execute a configuração inicial do Servidor de Administração de acordo com os requisitos existentes. Durante a etapa de configuração inicial, o assistente usa as configurações padrão para criar as políticas e tarefas que são necessárias para implementar a proteção. No entanto, as configurações padrão podem ser menos ótimas para as necessidades da sua organização. Se necessário, é possível editar as configurações de políticas e tarefas (Configurar a proteção em uma rede da organização cliente, Cenário: configurar a proteção da rede).

   Se planejar usar os recursos que estão fora da funcionalidade básica, licencie o aplicativo. Você pode fazer isso em uma das etapas do Assistente de início rápido.

3. **Verificar instalação do Servidor de Administração para obter êxito**

Quando todas as etapas anteriores estiverem concluídas, o Servidor de Administração é instalado e está pronto para uso adicional.

Assegure-se de que o Console de Administração esteja em execução e que você possa conectar-se ao Servidor de Administração através do Console de Administração. Também, assegure-se de que a tarefa Baixar atualizações para o repositório do Servidor de Administração esteja disponível no Servidor de Administração (na pasta **Tarefas** da árvore do console), assim como a política para o Kaspersky Endpoint Security (na pasta **Políticas** da árvore do console).

Quando a verificação estiver concluída, prossiga para as etapas abaixo.

Implementação centralizada de aplicativos de segurança Kaspersky em dispositivos clientes

1. **Localizar dispositivos na rede**

   Esta etapa faz parte do Assistente de início rápido. Você também pode iniciar a localização dos dispositivos manualmente. O Kaspersky Security Center recebe os endereços e os nomes de todos os dispositivos detectados na rede. Você então pode usar o Kaspersky Security Center para instalar aplicativos Kaspersky e software de outros fornecedores nas dispositivos detectados. O Kaspersky Security Center regularmente inicia uma descoberta de dispositivos, o que significa que se alguma nova instância aparecer na rede, elas serão detectadas automaticamente.

2. **Instalar o Agente de Rede e aplicativos de segurança em dispositivos na rede**

   A implementação da proteção (Configurar a proteção em uma rede da organização cliente, Cenário: configurar a proteção da rede) da rede de uma organização engloba a instalação do Agente de Rede e de aplicativos de segurança (por exemplo, o Kaspersky Endpoint Security) nos dispositivos detectados pelo Servidor de Administração durante a descoberta de dispositivos.

   Os aplicativos de segurança protegem os dispositivos contra vírus e/ou outros programas que apresentem uma ameaça. O Agente de Rede assegura a comunicação entre o dispositivo e o Servidor de Administração. As configurações do Agente de Rede são definidas automaticamente por padrão.

   Se desejar, você pode instalar o Agente de Rede no modo silencioso com um arquivo de resposta ou sem um arquivo de resposta.

   Antes de iniciar a instalação do Agente de Rede e dos aplicativos de segurança nos dispositivos na rede, assegure-se de que estes dispositivos estejam acessíveis (ligados). Você pode instalar o Agente de Rede em máquinas virtuais e em dispositivos físicos.

   Aplicativos de segurança e o Agente de Rede podem ser instalados remotamente ou localmente.

   Instalação remota – usando o Assistente de implementação da proteção, você pode instalar remotamente o aplicativo de segurança (por exemplo, Kaspersky Endpoint Security for Windows) e o Agente de Rede em dispositivos que foram detectados pelo Servidor de Administração na rede da organização. Normalmente, a tarefa Instalação remota com êxito, implementa a proteção na maioria dos dispositivos na rede. Contudo, ele pode retornar um erro em alguns dispositivos se, por exemplo, um dispositivo estiver desligado ou não puder ser acessado por qualquer outro motivo. Neste caso, recomendamos que você se conecte ao dispositivo manualmente e use a instalação local.

   A Instalação local – Usada em dispositivos na rede nos quais a proteção não pôde ser implementada usando a tarefa de instalação remota. Para instalar a proteção em tais dispositivos, crie um pacote de instalação independente que possa ser executado localmente naqueles dispositivos.

   A instalação do Agente de Rede em dispositivos que executam os sistemas operacionais Linux e macOS é descrita na documentação do Kaspersky Endpoint Security for Linux e do Kaspersky Endpoint Security for Mac, respectivamente. Embora os dispositivos que executam os sistemas operacionais Linux e macOS sejam considerados menos vulneráveis do que os dispositivos que executam o Windows, recomendamos que você mesmo assim instale aplicativos de segurança.

   Após a instalação, assegure-se de que o aplicativo de segurança esteja instalado nos dispositivos gerenciados. Execute um relatório de versões de software da Kaspersky e exiba os seus resultados.

3. **Implementação de chaves de licença para dispositivos clientes**

   Implemente chaves de licença em dispositivos clientes para ativar aplicativos de segurança gerenciados naqueles dispositivos.

4. **Configurar a proteção de dispositivo móvel**

   Esta etapa faz parte do Assistente de início rápido.

   Se você deseja gerenciar dispositivos móveis corporativos, execute as etapas necessárias para a preparação e implementação do Gerenciamento de Dispositivos Móveis.

5. **Crie uma estrutura de um grupo de administração**

   Em alguns casos, implementar a proteção em dispositivos na rede no modo mais conveniente pode necessitar que você divida todo o conjunto de dispositivos em grupos de administração, considerando a estrutura da organização. Você pode criar regras para mover para distribuir dispositivos entre grupos, ou pode distribuir os dispositivos manualmente. Você pode atribuir tarefas de grupo para grupos de administração, definir o escopo das políticas e atribuir pontos de distribuição.

   Assegure-se de que todos os dispositivos gerenciados foram corretamente atribuídos aos grupos de administração apropriados, e que não mais haja dispositivos não atribuídos na rede.

6. **Atribuir os pontos de distribuição**

   O Kaspersky Security Center atribui pontos de distribuição aos grupos de administração automaticamente, mas você pode atribui-los manualmente, se necessário. Recomendamos que você use pontos de distribuição em redes de larga escala para reduzir a carga no Servidor de Administração, e em redes que têm uma estrutura distribuída para fornecer ao Servidor de Administração o acesso aos dispositivos (ou grupos de dispositivos) comunicado através de canais com baixas taxas de produtividade. Você pode usar dispositivos que executam Linux como pontos de distribuição, bem como dispositivos que executam Windows.

Portas usadas pelo Kaspersky Security Center

As tabelas abaixo mostram as portas padrão utilizadas pelos Servidores de Administração e pelos dispositivos clientes. Se desejar, poderá modificar os números de porta padrão.

Se o Servidor de Administração e o banco de dados forem instalados em dispositivos diferentes, será necessário disponibilizar as portas necessárias no dispositivo no qual o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server; porta 1433 para Microsoft SQL Server ou porta 5432 para PostgreSQL e Postgres Pro). Consulte a documentação do DBMS para obter informações relevantes.

Portas utilizadas pelo Servidor de Administração

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
8060	klcsweb	TCP	Transmissão de pacotes de instalação publicados aos dispositivos cliente	Publicando pacotes de instalação. Você pode alterar o número da porta padrão na seção **Servidor da Web** da janela de propriedades do Servidor de Administração no Console de Administração ou no Kaspersky Security Center Web Console. Esta porta é opcional. Por razões de segurança, recomendamos usar a porta TCP 8061.
8061	klcsweb	TCP (TLS)	Transmitindo pacotes de instalação publicados aos dispositivos cliente	Publicando pacotes de instalação. Você pode alterar o número da porta padrão na seção **Servidor da Web** da janela de propriedades do Servidor de Administração no Console de Administração ou no Kaspersky Security Center Web Console.

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
13000	klserver	TCP (TLS)	Receber conexões de Agentes de Rede e Servidores de Administração secundários; também usado em Servidores de Administração secundários para receber conexões do Servidor de Administração principal (por exemplo, se o Servidor de Administração secundário estiver na DMZ)	Gerenciando dispositivos cliente e Servidores de Administração secundários. Você pode alterar o número da porta padrão para receber conexões do Agentes de Rede ao configurar portas de conexão. Você pode alterar o número da porta padrão para receber conexões de Servidores de Administração secundários ao criar uma hierarquia de Servidores de Administração no Console de Administração ou no Kaspersky Security Center Web Console.
13000	klserver	UDP	Recebendo informações sobre dispositivos que foram desativados a partir de Agentes de Rede	Gerenciamento de dispositivos clientes. Você pode alterar o número da porta padrão nas configurações de política do Agente de Rede no Console de Administração ou no Kaspersky Security Center Web Console.
13291	klserver	TCP (TLS)	Configurar as conexões do Console de Administração ao Servidor de Administração	Gerenciando Servidor de Administração. Você pode alterar o número da porta padrão na janela de propriedades do Servidor de Administração no Console de Administração.
13299	klserver	TCP (TLS)	Receber conexões do Kaspersky Security Center Web Console para o Servidor de Administração; receber conexões para o Servidor de Administração através do OpenAPI	Kaspersky Security Center Web Console, OpenAPI. Você pode alterar o número da porta padrão na janela de propriedades do Servidor de Administração (na seção **Configurações de conexão do Servidor de Administração**→ subseção **Portas de conexão**) no Console de Administração ou ao criar uma hierarquia de Servidores de Administração no Console de Administração ou no Kaspersky Security Center Web Console.
14000	klserver	TCP	Receber conexões dos Agentes de Rede	Gerenciando dispositivos cliente. Você pode alterar o número da porta padrão ao configurar portas de conexão durante a instalação do Kaspersky Security Center ou ao conectar manualmente um dispositivo cliente ao Servidor de Administração. Esta porta é opcional. Por razões de segurança, recomendamos usar a porta TCP 1300.
13111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	TCP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela Propriedades do Servidor de Administração.
15111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	UDP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela Propriedades do Servidor de Administração.
17000	klactprx	TCP (TLS)	Receber conexões para a ativação do aplicativo de dispositivos gerenciados (exceto dispositivos móveis)	Servidor proxy de ativação usado por dispositivos não móveis para ativar aplicativos da Kaspersky com códigos de ativação. Você pode alterar o número da porta padrão na janela Propriedades do Servidor de Administração.
17100 (apenas se você gerencia dispositivos móveis)	klactprx	TCP (TLS)	Recebendo conexões para a ativação do aplicativo de dispositivos móveis	Servidor proxy de ativação para dispositivos móveis. Você pode alterar o número da porta padrão na janela Propriedades do Servidor de Administração.
19170	klserver	HTTPS (TLS)	Tunelamento das conexões com dispositivos gerenciados usando o utilitário klsctunnel	Conexão remota a dispositivos gerenciados com o uso do Kaspersky Security Center Web Console. Você só pode alterar o número de portas padrão na janela de propriedades do Servidor de Administração do Console de Administração (seção **Configurações de conexão do Servidor de Administração**→ subseção **Portas de conexão**→ **opção Abrir porta RDP para o Kaspersky Security Center Web Console**).

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
13292 (apenas se você gerencia dispositivos móveis)	klserver	TCP (TLS)	Receber conexões de dispositivos móveis	Gerenciamento de Dispositivos Móveis. Você pode alterar o número da porta padrão na janela de propriedades do Servidor de Administração no Console de Administração ou no Kaspersky Security Center Web Console.
13294 (apenas se você gerencia dispositivos móveis)	klserver	TCP (TLS)	Receber conexões de dispositivos de proteção UEFI	Gerenciando dispositivos cliente de proteção UEFI. Você pode alterar o número da porta padrão ao conectar dispositivos móveis ou, posteriormente, na janela de propriedades do Servidor de Administração (seção **Configurações de conexão do Servidor de Administração** → subseção **Portas de conexão**) no Console de Administração ou no Kaspersky Security Center Web Console.
13296	klserver	TCP (TLS)	Publicação de métricas do Kaspersky Security Center para Prometheus	Publicação de métricas do Kaspersky Security Center que serão obtidas posteriormente pelo Prometheus. É possível visualizar as métricas no seguinte link: https://<`endereço_do_servidor`>:13296/metrics. Em <`endereço_do_servidor`>, especifique o endereço IP ou nome de domínio do Servidor de Administração. Você pode alterar o número da porta padrão na janela de propriedades do Servidor de Administração no Console de Administração.
30522, 30523 (portas na interface localhost)	klnagent	TCP	Recepção de atualizações do aplicativo da Kaspersky do Servidor de Administração usando o componente FileTransferBridge	O dispositivo do Servidor de Administração que recebe as atualizações do aplicativo da Kaspersky.

A tabela abaixo mostra a porta utilizada pelo Servidor de MDM do iOS (somente se você gerencia dispositivos móveis).

Porta usada pelo Servidor de MDM do iOS

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
443	kliosmdmservicesrv	TCP (TLS)	Receber conexões de dispositivos móveis iOS	Gerenciamento de Dispositivos Móveis. Você pode alterar o número da porta padrão ao instalar o MDM do iOS Server.

A tabela abaixo mostra a porta utilizada pelo Kaspersky Security Center Web Console Server. Pode ser o mesmo dispositivo no qual o Servidor de Administração está instalado ou em outro.

Porta usada pelo Kaspersky Security Center Web Console

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
8080	Node.js: JavaScript do lado do servidor	TCP (TLS)	Receber conexões do navegador no Kaspersky Security Center Web Console	Kaspersky Security Center Web Console. Você pode alterar o número da porta padrão ao instalar o Kaspersky Security Center Web Console em um dispositivo executando o Windows ou em uma plataforma Linux. Ao instalar o Kaspersky Security Center Web Console no sistema operacional Linux ALT, é necessário especificar um número de porta diferente de 8080, pois essa porta é usada pelo sistema operacional.

A tabela abaixo mostra a porta utilizada pelos dispositivos gerenciados nos quais o Agente de Rede está instalado.

Portas usadas pelo Agente de Rede

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
15000	klnagent	UDP	Sinais de gerenciamento do Servidor de Administração ou ponto de distribuição para os Agentes de Rede	Gerenciamento de dispositivos clientes. Você pode alterar o número da porta padrão nas configurações de política do Agente de Rede no Console de Administração ou no Kaspersky Security Center Web Console.
15000	klnagent	Transmissão UDP	Obtendo dados sobre outros Agentes de Rede no mesmo domínio de transmissão (os dados são enviados ao Servidor de Administração)	Fornecendo atualizações e pacotes de instalação.
15001	klnagent	UDP	Recebendo solicitações de multicast de um ponto de distribuição (se estiver em uso)	Recebendo atualizações e pacotes de instalação de um ponto de distribuição. Você pode alterar o número da porta padrão na janela de propriedades do ponto de distribuição no Console de Administração ou no Kaspersky Security Center Web Console.
30522, 30523 (portas na interface localhost)	klnagent	TCP	Recepção de atualizações do aplicativo da Kaspersky do Servidor de Administração usando o componente FileTransferBridge	Dispositivos gerenciados que recebem atualizações do aplicativo da Kaspersky do Servidor de Administração especificado como uma fonte de atualização de bancos de dados.
161	klnagent	SNMP	Monitoramento e descoberta de dispositivos em rede.	Descoberta do dispositivo.

Observe que o processo klnagent também pode solicitar portas livres do intervalo de portas dinâmicas de um sistema operacional de endpoint. Essas portas são alocadas automaticamente para o processo klnagent pelo sistema operacional. Assim, o processo klnagent poderá usar algumas portas que são usadas por outro software. Caso o processo klnagent afete as operações desse software, altere suas configurações da porta ou altere o intervalo padrão de porta dinâmica no sistema operacional para excluir a porta usada pelo software afetado.

Também é preciso levar em consideração que as recomendações sobre a compatibilidade do Kaspersky Security Center com software de terceiros são descritas apenas como referência e podem não ser aplicáveis a novas versões de software de terceiros. As recomendações descritas para configurar as portas são baseadas nas experiências do Suporte Técnico e em nossas práticas recomendadas.

A tabela abaixo mostra a porta utilizada pelos dispositivos gerenciados nos quais o Agente de Rede instalado atua como um ponto de distribuição. As portas listadas são utilizadas pelos dispositivos do ponto de distribuição, além das portas utilizadas pelos Agentes de Rede (consulte a tabela acima).

Portas usadas pelo Agente de Rede funcionando como ponto de distribuição

Número da porta	Nome do processo que abre a porta	Protocolo	Propósito da porta	Escopo
13000	klnagent	TCP (TLS)	Receber conexões de Agentes de Rede e do Kaspersky Security Center quando o ponto de distribuição atuar como um gateway de conexão na DMZ. Caso seja um dispositivo com o Servidor de Administração instalado especificado como ponto de distribuição, a porta 13001 será usada para conexão SSL por padrão em vez de 13000.	Gerenciar dispositivos cliente, entregar atualizações e pacotes de instalação. Consulte o seguinte tópico para obter detalhes: Servidor de Administração, um gateway de conexão em um segmento de rede e um dispositivo cliente. Você pode alterar o número da porta padrão na janela de propriedades do ponto de distribuição no Console de Administração ou no Kaspersky Security Center Web Console.
13111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	TCP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela de propriedades do ponto de distribuição no Console de Administração ou no Kaspersky Security Center Web Console.
15111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	UDP	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela de propriedades do ponto de distribuição no Console de Administração ou no Kaspersky Security Center Web Console.
17111 (apenas se o serviço de proxy KSN for executado no dispositivo)	ksnproxy	HTTPS	Receber solicitações de dispositivos gerenciados para o servidor proxy da KSN	Servidor Proxy da KSN. Você pode alterar o número da porta padrão na janela de propriedades do ponto de distribuição no Console de Administração ou no Kaspersky Security Center Web Console.
13295 (apenas se você usar o ponto de distribuição como um servidor push)	klnagent	TCP (TLS)	Receber conexões de dispositivos cliente	Servidor push. Você pode alterar o número da porta padrão na janela de propriedades do ponto de distribuição no Console de Administração ou no Kaspersky Security Center Web Console.

Certificados para trabalhar com o Kaspersky Security Center

Essa seção contém informações sobre os certificados do Kaspersky Security Center e descreve como emitir um certificado personalizado para o Servidor de Administração.

Sobre os certificados do Kaspersky Security Center

O Kaspersky Security Center usa os seguintes tipos de certificados para permitir uma interação segura entre os componentes do aplicativo:

- Certificado do Servidor de Administração
- Certificado móvel
- Certificado do Servidor de MDM do iOS
- Certificado do Servidor Web do Kaspersky Security Center
- Certificado do Kaspersky Security Center Web Console

Por padrão, o Kaspersky Security Center usa certificados autoassinados (ou seja, emitidos pelo próprio Kaspersky Security Center), mas você pode substituí-los por certificados personalizados para melhor atender aos requisitos da rede da sua organização e cumprir os padrões de segurança. Depois que o Servidor de Administração verifica se um certificado personalizado atende a todos os requisitos aplicáveis, este certificado assume o mesmo escopo funcional de um certificado autoassinado. A única diferença é que um certificado personalizado não é reemitido automaticamente após o término. Os certificados são substituídos por certificados personalizados por meio do utilitário klsetsrvcert ou por meio da seção de propriedades do Servidor de Administração no console de administração, dependendo do tipo de certificado. Ao usar o utilitário klsetsrvcert, é preciso especificar um tipo de certificado usando um dos seguintes valores:

- C (certificado comum para as portas 13000 e 13291).
- CR (certificado de reserva comum para as portas 13000 e 13291).
- M (certificado móvel para porta 13292).
- MR (certificado de reserva móvel para a porta 13292).
- MCA (autoridade de certificação móvel para certificados de usuário gerados automaticamente).

Não é preciso baixar o utilitário klsetsrvcert. Ele está incluído no kit de distribuição do Kaspersky Security Center. Não é compatível com versões anteriores do Kaspersky Security Center.

O período de validade máximo para qualquer um dos certificados do Servidor de Administração deve ser de 397 dias ou menos.

Certificados do Servidor de Administração

Um certificado do Servidor de Administração é necessário para autenticação do Servidor de Administração, bem como para interação segura entre o Servidor de Administração e o Agente de Rede em dispositivos gerenciados ou entre o Servidor de Administração principal e Servidores de Administração secundários. Ao conectar o Console de Administração ao Servidor de Administração pela primeira vez, é solicitado que você confirme o uso do certificado do Servidor de Administração atual. Essa confirmação também é necessária toda vez que o certificado do Servidor de Administração é substituído, após cada reinstalação do Servidor de Administração e ao conectar um Servidor de Administração secundário ao Servidor de Administração principal. Este certificado é chamado comum ("C").

O certificado comum ("C") é criado automaticamente quando o componente Servidor de Administração é instalado. O certificado consiste em duas partes:

- Arquivo klserver.cer; por padrão, está localizado no dispositivo no qual o componente Servidor de Administração está instalado na pasta C:\ProgramData\KasperskyLab\adminkit\1093\cert.
- Chave de licença secreta localizada no Armazenamento Protegido do Windows.

Existe ainda um certificado de reserva comum ("CR"). O Kaspersky Security Center gera automaticamente este certificado 90 dias antes do término do certificado comum. O certificado de reserva comum é subsequentemente usado para a substituição perfeita do certificado do Servidor de Administração. Quando o certificado comum está prestes a expirar, o certificado de reserva comum é usado para manter a conexão com as instâncias do Agente de Rede instaladas nos dispositivos gerenciados. Com esta finalidade, o certificado de reserva comum torna-se automaticamente o novo certificado comum 24 horas antes de o antigo certificado comum expirar.

Você também pode fazer backup do certificado do Servidor de Administração separadamente de outras configurações do Servidor de Administração para mover o Servidor de Administração de um dispositivo para outro, sem perda de dados.

Certificados móveis

Um certificado móvel ("M") é necessário para autenticação do Servidor de Administração em dispositivos móveis. Você pode configurar o uso do certificado de dispositivos móveis na etapa dedicada do Assistente de início rápido.

Além disso, existe um certificado de reserva móvel ("MR"), que é usado para a substituição perfeita do certificado móvel. Quando o certificado móvel está prestes a expirar, o certificado de reserva móvel é usado para manter a conexão com instâncias do Agente de Rede instaladas em dispositivos móveis gerenciados. Com esta finalidade, o certificado de reserva móvel torna-se automaticamente o novo certificado móvel 24 horas antes de o antigo certificado comum expirar.

A reemissão automática de certificado de dispositivos móveis não é compatível. Recomendamos especificar um novo certificado de dispositivos móveis quando o existente estiver prestes a expirar. Caso o certificado de dispositivos móveis expirar e o certificado de dispositivos móveis reserva não for especificado, a conexão entre o Servidor de Administração e as instâncias do Agente de Rede instaladas em dispositivos móveis gerenciados será perdida. Nesse caso, para reconectar dispositivos móveis gerenciados, é necessário especificar um novo certificado de dispositivos móveis e reinstalar o Kaspersky Security for Mobile em cada dispositivo móvel gerenciado.

Se o cenário de conexão exigir o uso de um certificado de cliente em dispositivos móveis (conexão envolvendo autenticação SSL bidirecional), você gera esses certificados através da autoridade de certificação para certificados de usuário gerados automaticamente ("MCA"). Além disso, o Assistente de início rápido permite que você comece a usar certificados de cliente personalizados emitidos por uma autoridade de certificação diferente, enquanto a integração com a infraestrutura de chave pública (PKI) do domínio de sua organização permite que você emita certificados de cliente por meio de sua autoridade de certificação de domínio.

Certificado do Servidor de MDM do iOS

Um certificado de servidor MDM iOS é necessário para autenticação do Servidor de Administração em dispositivos móveis executando o sistema operacional iOS. A interação com esses dispositivos é realizada por meio do protocolo de Gerenciamento de Dispositivos Móveis (MDM) da Apple que não envolve o Agente de Rede. Em vez disso, você instala um perfil MDM do iOS especial, contendo um certificado de cliente, em cada dispositivo, para garantir a autenticação SSL bidirecional.

Além disso, o Assistente de início rápido permite que você comece a usar certificados de cliente personalizados emitidos por uma autoridade de certificação diferente, enquanto a integração com a infraestrutura de chave pública (PKI) do domínio de sua organização permite que você emita certificados de cliente por meio de sua autoridade de certificação de domínio.

Os certificados do cliente são transmitidos para dispositivos iOS quando você baixa os perfis MDM do iOS. Um certificado de cliente do Servidor de MDM do iOS é exclusivo para cada dispositivo iOS gerenciado. Você gera todos os certificados cliente do servidor MDM do iOS através da autoridade de certificação para certificados de usuário gerados automaticamente ("MCA").

Certificado do Servidor Web do Kaspersky Security Center

O Servidor da Web do Kaspersky Security Center (Servidor da Web), um componente do Servidor de Administração do Kaspersky Security Center, usa um tipo especial de certificado. Este certificado é necessário para publicar pacotes de instalação do Agente de Rede que você baixou posteriormente para dispositivos gerenciados, bem como para publicar perfis MDM do iOS, aplicativos iOS e pacotes de instalação do Kaspersky Endpoint Security for Mobile. Para isso, o Servidor Web pode usar vários certificados.

Se a compatibilidade para dispositivo móvel estiver desativada, o Servidor Web usa um dos seguintes certificados, em ordem de prioridade:

1. Certificado de Servidor Web personalizado que você especificou manualmente no Console de Administração
2. Certificado do Servidor de Administração Comum ("C")

Se a compatibilidade para dispositivo móvel estiver habilitada, o Servidor Web usa um dos seguintes certificados, em ordem de prioridade:

1. Certificado de Servidor Web personalizado que você especificou manualmente no Console de Administração
2. Certificado móvel personalizado
3. Certificado móvel autoassinado ("M")
4. Certificado do Servidor de Administração Comum ("C")

Certificado do Kaspersky Security Center Web Console

O Servidor do Kaspersky Security Center Web Console (aqui referido como Web Console) tem seu próprio certificado. Quando você abre um site, um navegador verifica se sua conexão é confiável. O certificado do Web Console permite autenticar o Web Console e é usado para criptografar o tráfego entre um navegador e o Web Console.

Quando o Web Console é aberto, o navegador pode informar que a conexão com o Web Console não é privada e o certificado do Web Console é inválido. Essa advertência aparece porque o certificado do Web Console é autoassinado e gerado automaticamente pelo Kaspersky Security Center. Para remover essa advertência, é possível fazer o seguinte:

- Substitua o certificado do Web Console por um personalizado (opção recomendada). Crie um certificado confiável na infraestrutura e que atenda aos requisitos para certificados personalizados.
- Adicione o certificado do Web Console na lista de certificados de navegador confiáveis. Recomendamos usar essa opção somente se não puder criar um certificado personalizado.

Sobre o certificado do Servidor de Administração

Duas operações são realizadas com base no *certificado do Servidor de Administração:* autenticação do Servidor de Administração durante a conexão pelo Console de Administração e troca de dados com dispositivos. O certificado também é usado para autenticação quando os Servidores de Administração principais são conectados aos Servidores de Administração secundários.

Certificado emitido pela Kaspersky

O certificado do Servidor de Administração é criado automaticamente durante a instalação do componente do Servidor de Administração e é armazenado na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

O certificado do Servidor de Administração é válido por cinco anos, caso o certificado tenha sido gerado pelo Servidor de Administração versão 12.2 ou anterior. Caso contrário, o prazo de validade do certificado é limitado a 397 dias. Um novo certificado é gerado pelo Servidor de Administração 90 dias antes da data de expiração do certificado atual. Posteriormente, o novo certificado automaticamente substitui o certificado atual um dia antes da data de vencimento. Todos os Agentes de Rede nos dispositivos cliente são automaticamente reconfigurados para autenticar o Servidor de Administração com o novo certificado.

Certificados personalizados

Se necessário, você pode atribuir um certificado personalizado ao Servidor de Administração. Por exemplo, isso pode ser necessário melhorar a integração com o PKI existente da sua empresa ou para a configuração personalizada dos campos do certificado.

O período de validade máximo para qualquer um dos certificados do Servidor de Administração deve ser de 397 dias ou menos.

Ao substituir o certificado, todos os Agentes de Rede que estiveram conectados anteriormente ao Servidor de Administração por SSL perderão a conexão e retornarão "Erro de autenticação do Servidor de Administração". Para eliminar o erro, será necessário restaurar a conexão após a substituição do certificado.

Caso o certificado do Servidor de Administração tenha se perdido, é preciso reinstalar o componente Servidor de Administração e restaurar os dados para poder recuperá-lo.

Se o Kaspersky Security Center Web Console for aberto em navegadores diferentes e for baixado o arquivo de certificado do Servidor de Administração na janela de propriedades do Servidor de Administração, os arquivos baixados terão nomes diferentes.

Requisitos para certificados personalizados usados no Kaspersky Security Center

A tabela abaixo mostra os requisitos para certificados personalizados especificados para diferentes componentes do Kaspersky Security Center.

Requisitos para certificados do Kaspersky Security Center

Tipo de certificado	Requisitos	Comentário
Certificado comum, certificado de reserva comum ("C", "CR")	Comprimento mínimo da chave: 2048. Restrições básicas: • Restrição de comprimento do caminho: nenhuma Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Utilização estendida de chave (opcional): autenticação de servidor, autenticação de cliente.	O parâmetro Utilização estendida de chave é opcional. O valor da Restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhum", mas não inferior a "1".
Certificado de dispositivo móvel, certificado de reserva de dispositivo móvel ("M", "MR")	Comprimento mínimo da chave: 2048. Restrições básicas: • CA: true • Restrição de comprimento do caminho: nenhuma Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Utilização estendida de chave (opcional): autenticação do servidor.	O parâmetro Utilização estendida de chave é opcional. O valor da Restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhum" se o certificado comum tiver um valor de Restrição do comprimento do caminho não inferior a "1".

Tipo de certificado	Requisitos	Comentário
Certificado CA para certificados de usuário gerados automaticamente ("MCA")	Comprimento mínimo da chave: 2048. Restrições básicas: • CA: true • Restrição de comprimento do caminho: nenhuma Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Utilização estendida de chave (opcional): autenticação de servidor, autenticação de cliente.	O parâmetro Utilização estendida de chave é opcional. O valor da Restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhum" se o certificado comum tiver um valor de Restrição do comprimento do caminho não inferior a "1".
Certificado do servidor da Web	Utilização estendida de chave: autenticação do servidor. O contêiner PKCS # 12 / PEM do qual o certificado é especificado inclui toda a cadeia de chaves públicas. O nome alternativo do assunto (SAN) do certificado está presente; ou seja, o valor do campo `subjectAltName` é válido. O certificado atende aos requisitos em vigor dos navegadores impostos aos certificados do servidor, bem como aos requisitos básicos atuais do Fórum do navegador/CA.	–
Certificado do Kaspersky Security Center Web Console	O contêiner PEM do qual o certificado é especificado inclui toda a cadeia de chaves públicas. O nome alternativo do assunto (SAN) do certificado está presente; ou seja, o valor do campo `subjectAltName` é válido. O certificado atende aos requisitos em vigor de navegadores para certificados de servidor, bem como os requisitos básicos atuais do Fórum do navegador/CA.	Certificados criptografados não são compatíveis com o Kaspersky Security Center Web Console.

Cenário: especificação do certificado personalizado do Servidor de Administração

É possível atribuir o certificado personalizado do Servidor de Administração, por exemplo, para melhor integração com a infraestrutura de chave pública (PKI) existente de sua empresa ou para configuração personalizada dos campos de certificado. É útil substituir o certificado imediatamente após a instalação do Servidor de Administração e antes que o Assistente de início rápido for concluído.

O período de validade máximo para qualquer um dos certificados do Servidor de Administração deve ser de 397 dias ou menos.

Pré-requisitos

As seguintes condições devem ser atendidas:

- O novo certificado deve ser criado no formato PKCS#12 (por exemplo, por meio da PKI da organização).
- Para o novo certificado, os requisitos listados na tabela abaixo devem ser atendidos.

  Na tabela abaixo, preste atenção ao requisito "CA: true" que significa que o novo certificado deve ser emitido por uma autoridade de certificação (CA) confiável. O novo certificado com o requisito "CA: true" deve incluir toda a cadeia de confiança e uma chave privada que deve ser armazenada em um arquivo com a extensão pfx ou p12.

  Requisitos para os certificados do Servidor de Administração

Tipo de certificado	Requisitos
Certificado comum, certificado de reserva comum ("C", "CR")	Comprimento mínimo da chave: 2048. Restrições básicas: • Restrição de comprimento do caminho: nenhuma O valor da restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhuma", mas não inferior a "1". Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Uso estendido de chave (EKU): autenticação de servidor e autenticação de cliente. O EKU é opcional, mas caso o seu certificado o contenha, os dados de autenticação do servidor e do cliente devem ser especificados no EKU.
Certificado de dispositivo móvel, certificado reserva de dispositivo móvel ("M", "MR")	Comprimento mínimo da chave: 2048. Restrições básicas: • CA: true • Restrição de comprimento do caminho: nenhuma O valor da restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhum" caso o certificado comum tenha um valor de restrição do comprimento do caminho não inferior a 1. Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Uso estendido de chave (EKU): autenticação do servidor. O EKU é opcional, mas caso o seu certificado o contenha, os dados de autenticação do servidor devem ser especificados no EKU.
Certificado CA para certificados de usuário gerados automaticamente ("MCA")	Comprimento mínimo da chave: 2048. Restrições básicas: • CA: true • Restrição de comprimento do caminho: nenhuma O valor da restrição do comprimento do caminho pode ser um número inteiro diferente de "Nenhum" caso o certificado comum tenha um valor de restrição do comprimento do caminho não inferior a 1. Uso da chave: • Assinatura digital • Assinatura de certificado • Criptografia de chave • Assinatura CRL Uso estendido de chave (EKU): autenticação do cliente. O EKU é opcional, mas caso o seu certificado o contenha, os dados de autenticação do cliente devem ser especificados no EKU.

Os certificados emitidos por uma CA pública não têm a permissão de assinatura de certificado. Para usar esses certificados, certifique-se de ter instalado o Agente de Rede versão 13 ou posterior em pontos de distribuição ou gateways de conexão na rede. Caso contrário, não será possível usar os certificados sem a permissão de assinatura.

Fases

A especificação do certificado do Servidor de Administração prossegue em etapas:

1. **Substituição do certificado do Servidor de Administração**

   Use a linha de comando do utilitário klsetsrvcert para este fim.

2. **Especificação de um novo certificado e restauração da conexão de Agentes de Rede com o Servidor de Administração**

   Caso o certificado tenha sido substituído, todos os Agentes de Rede anteriormente conectados ao Servidor de Administração via SSL perderão a conexão e retornarão o "Erro de autenticação do Servidor de Administração". Para especificar o novo certificado e restaurar a conexão, use a linha de comando com o utilitário klmover.

3. **Especificar um novo certificado nas configurações do Kaspersky Security Center Web Console**

   Depois de substituir o certificado, especifique nas configurações do Kaspersky Security Center Web Console. Caso contrário, o Kaspersky Security Center Web Console não será capaz de se conectar ao Servidor de Administração.

Resultados

Ao concluir o cenário, o certificado do Servidor de Administração é substituído e o servidor é autenticado pelos Agentes de Rede nos dispositivos gerenciados.

Substituição do certificado do Servidor de Administração usando o utilitário klsetsrvcert

Para substituir o certificado do Servidor de Administração:

Na linha de comando, execute o seguinte utilitário:

```
klsetsrvcert [-t <tipo de certificado> {-i <caminho para o novo certificado> [-p
<senha>] [-o <parâmetros>] | -g <nome dns>}][-f <horário da substituição>][-r
<certificados raiz>][-l <caminho do arquivo de registro>]
```

Não é preciso baixar o utilitário klsetsrvcert. Ele está incluído no kit de distribuição do Kaspersky Security Center. Não é compatível com versões anteriores do Kaspersky Security Center.

A descrição dos parâmetros do utilitário klsetsrvcert é apresentada na tabela abaixo.

Valores dos parâmetros do utilitário klsetsrvcert

Parâmetro	Valor
`-t < tipo de certificado >`	Tipo de certificado a ser substituído. Valores possíveis do parâmetro `< tipo de certificado >`: • `C` – substitui o certificado para as portas 13000 e 13291. • `CR` – substitui o certificado reserva comum para as portas 13000 e 13291. • `M` – substitui o certificado para dispositivos móveis na porta 13292. • `MR` – substitui o certificado de reserva móvel para a porta 13292. • `MCA` – CA do cliente móvel para certificados de usuário gerados automaticamente.
`-f < horário da substituição >`	Cronograma de alteração do certificado, usando o formato "DD-MM-AAA hh:mm" (para portas 13000 e 13291). Utilize esse parâmetro se quiser substituir o certificado comum pelo certificado de reserva comum antes que o certificado comum expire. Especifique a hora em que os dispositivos gerenciados devem ser sincronizados com o Servidor de Administração em um novo certificado.
`-i < caminho para o novo certificado >`	Contêiner com o certificado e chave privada no formato PKCS#12 (arquivo com a extensão .p12 ou .pfx).
`-p < senha >`	Senha usada para a proteção o contêiner p12. O certificado e uma chave privada são armazenados no contêiner, portanto, a senha é necessária para descriptografar o arquivo com o contêiner.
`-o < parâmetros de validação >`	Parâmetros de validação de certificado (separados por ponto e vírgula). Para usar um certificado personalizado sem a permissão de assinatura, especifique `-o NoCA` no utilitário klsetsrvcert. Isso é útil para certificados emitidos por uma CA pública. Para alterar o comprimento da chave de criptografia para os tipos de certificado C ou CR, especifique `-o RsaKeyLen:< comprimento da chave >` no utilitário klsetsrvcert, em que o parâmetro `< comprimento da chave >` é o valor do comprimento da chave necessário. Caso contrário, o comprimento da chave do certificado atual será usado.
`-g < nome dns >`	Um novo certificado será criado para o nome DNS especificado.
`-r < certificados raiz >`	Lista de autoridades de certificado raiz confiáveis, formato PEM.
`-l < caminho do arquivo de registro >`	Arquivo de saída dos resultados. Por padrão, a saída é redirecionada no fluxo de saída padrão.

Por exemplo, para especificar o certificado personalizado do Servidor de Administração, use o seguinte comando:

```
klsetsrvcert -t C -i <caminho para o novo certificado> -p <senha> -o NoCA
```

Após a substituição do certificado, todos os Agentes de Rede conectados com Servidor de Administração por meio de SSL perdem a conexão. Para restaurá-la, use a linha de comando do utilitário klmover.

Para evitar a perda das conexões dos Agentes de Rede, use os seguintes comandos:

1. Para instalar o novo certificado,

   ```
   klsetsrvcert.exe -t CR -i <caminho para o novo certificado> -p <senha> -o NoCA
   ```

2. Para especificar a data em que o novo certificado será aplicado,

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

em que "`DD-MM-AAAA hh:mm`" é a data 3 a 4 semanas antes da data atual. A mudança de horário para alterar o certificado para um novo permitirá que um novo certificado seja distribuído a todos os Agentes de Rede.

Conexão dos Agentes de Rede ao Servidor de Administração usando o utilitário klmover

Depois de substituir o certificado do Servidor de Administração usando a linha de comando do utilitário klsetsrvcert, é preciso estabelecer a conexão SSL entre os Agentes de Rede e o Servidor de Administração porque a conexão foi interrompida.

Para especificar o novo certificado do Servidor de Administração e restaurar a conexão:

Na linha de comando, execute o seguinte utilitário:

```
klmover [-address <server address>] [-pn <port number>] [-ps <SSL port number>] [-
nossl] [-cert <path to certificate file>]
```

Os direitos de administrador são necessários para executar o utilitário.

O utilitário é copiado automaticamente para a pasta de instalação do agente de rede, quando ele é instalado em um dispositivo cliente.

Caso a opção **Usar senha de desinstalação** esteja ativada nas configurações da política do Agente de Rede e a versão do Agente de Rede usada seja a 15, o utilitário klmover requer a senha correspondente. É possível usar o utilitário klcsngtgui localizado na pasta de instalação do Agente de Rede para verificar a versão do Agente de Rede.

Você não pode usar o utilitário klmover para dispositivos clientes conectados ao Servidor de Administração por meio de gateways de conexão. Para esses dispositivos, você precisa reconfigurar o Agente de Rede ou reinstalar o Agente de Rede e especificar o gateway de conexão.

A descrição dos parâmetros do utilitário klmover é apresentada na tabela abaixo.

Valores dos parâmetros do utilitário klmover

Parâmetro	Valor
`-address < endereço do servidor >`	Endereço do Servidor de Administração para conexão. É possível especificar um endereço IP, o nome NetBIOS ou o nome DNS.
`-pn < número da porta >`	Número da porta pela qual a conexão não criptografada será estabelecida com Servidor de Administração. O número da porta padrão é 14000.
`-ps < número da porta SSL >`	Número da porta SSL pela qual a conexão criptografada será estabelecida com o Servidor de Administração usando o protocolo SSL. O número da porta padrão é 13000.
`-nossl`	Usa a conexão não criptografada com Servidor de Administração. Caso a chave não esteja sendo usada, o agente de rede é conectado ao Servidor de Administração usando o protocolo SSL codificado.
`-cert < caminho para o arquivo do certificado >`	Usa o arquivo de certificado especificado para autenticação de acesso com o Servidor de Administração.
`-virtserv`	Nome do Servidor de Administração virtual.

Parâmetro	Valor
`-cloningmode`	Modo de clonagem do disco do Agente de Rede. Use um dos seguintes parâmetros para configurar o modo de clonagem de disco: • `-cloningmode` – Solicita o status do modo de clonagem de disco. • `-cloningmode 1` – Ativa o modo de clonagem de disco. • `-cloningmode 0` – Desativa o modo de clonagem de disco.
`-nauninstpwd < senha >`	Use este parâmetro para especificar a senha de desinstalação do Agente de Rede. O parâmetro não é obrigatório.

Por exemplo, para conectar o Agente de Rede ao Servidor de Administração, execute o seguinte comando:

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

Reemissão do certificado do servidor da Web

O certificado do Servidor da Web usado no Kaspersky Security Center é necessário para publicar pacotes de instalação do Agente de Rede baixados posteriormente para dispositivos gerenciados, bem como para publicar perfis MDM do iOS, aplicativos iOS e pacotes de instalação do Kaspersky Endpoint Security for Mobile. Dependendo da configuração do aplicativo atual, vários certificados podem funcionar como o certificado do Servidor da Web (para obter mais detalhes, consulte Sobre os certificados do Kaspersky Security Center).

Pode ser necessário emitir o certificado do Servidor da Web novamente para atender aos requisitos de segurança específicos de sua organização ou para manter a conexão contínua dos dispositivos gerenciados antes de iniciar a atualização do aplicativo. O Kaspersky Security Center oferece duas maneiras de reemitir o certificado do servidor da Web. A escolha entre os dois métodos depende se você tem dispositivos móveis conectados e gerenciados por meio do protocolo móvel (ou seja, usando o certificado móvel).

Se você nunca especificou seu próprio certificado personalizado como o certificado do Servidor da Web na seção **Servidor da Web** da janela de propriedades do Servidor de Administração, o certificado móvel atua como o certificado do Servidor Web. Nesse caso, a reemissão do certificado do Web Server é realizada por meio da reemissão do próprio protocolo móvel.

Para reemitir o certificado do Servidor da Web quando você não tiver nenhum dispositivo móvel gerenciado por meio do protocolo móvel:

1. Na árvore do console, clique com o botão direito no nome do Servidor de Administração relevante e no menu contextual selecione **Propriedades**.

2. Na janela aberta de propriedades do Servidor de Administração, selecione a seção **Configurações de conexão do Servidor de Administração**.

3. Na lista de dispositivos, selecione a subseção **Certificados**.

4. Se você planeja continuar usando o certificado emitido pelo Kaspersky Security Center, faça o seguinte:

   a. No painel direito, no grupo de configurações **Autenticação do Servidor de Administração por dispositivos móveis**, selecione a opção **Certificado emitido através do Servidor de Administração** e clique no botão **Reemitir**.

   b. Na janela aberta **Reemitir o certificado** no grupo de configurações **Endereço de conexão** e **Termo de ativação**, selecione as opções pertinentes e clique em **OK**.

   c. Na janela de confirmação, clique em **Sim**.

   Como alternativa, se você planeja usar seu próprio certificado personalizado, faça o seguinte:

   a. Verifique se o seu certificado personalizado atende aos requisitos do Kaspersky Security Center e aos requisitos para certificados confiáveis da Apple. Se necessário, modifique o certificado.

   b. Selecione a opção **Outro certificado** e clique no botão **Procurar**.

   c. Na janela aberta **Certificado**, no campo **Tipo de certificado**, selecione o tipo de seu certificado e, em seguida, especifique o local do certificado e as configurações:

      - Se você selecionou **Contêiner PKCS#12**, clique no botão **Procurar** ao lado do campo **Arquivo de certificado** e especifique o arquivo de certificado em seu disco rígido. Se o arquivo do certificado for protegido por senha, digite a senha no campo **Senha (caso exista)**.

      - Se você selecionou **Certificado X.509**, clique no botão **Procurar** ao lado do campo **Chave privada (.prk, .pem)** e especifique a chave privada no seu disco rígido. Se a chave privada for protegida por senha, digite a senha no campo **Senha (caso exista)**. Em seguida, clique no botão **Procurar** ao lado do campo **Chave pública (.cer)** e especifique a chave privada no seu disco rígido.

   d. Na janela **Certificado** clique em **OK**.

   e. Na janela de confirmação, clique em **Sim**.

   O certificado móvel é reemitido para ser usado como o certificado do Servidor da Web.

Para reemitir o certificado do Servidor da Web se você algum dispositivo móvel gerenciado por meio do protocolo móvel:

1. Gere seu certificado personalizado e prepare-o para uso no Kaspersky Security Center. Verifique se o seu certificado personalizado atende aos requisitos do Kaspersky Security Center e aos requisitos para certificados confiáveis da Apple. Se necessário, modifique o certificado.

   > Você pode usar o utilitário kliossrvcertgen.exe para geração de certificado.

2. Na árvore do console, clique com o botão direito no nome do Servidor de Administração relevante e no menu contextual selecione **Propriedades**.

3. Na janela aberta de propriedades do Servidor de Administração, selecione a seção **Servidor da Web**.

4. No menu **Via HTTPS**, selecione a opção **Especificar outro certificado**.

5. No menu **Via HTTPS**, clique no botão **Alterar**.

6. Na janela aberta **Certificado**, no campo **Tipo de certificado**, selecione o tipo de seu certificado:

   - Se você selecionou **Contêiner PKCS#12**, clique no botão **Procurar** ao lado do campo **Arquivo de certificado** e especifique o arquivo de certificado em seu disco rígido. Se o arquivo do certificado for protegido por senha, digite a senha no campo **Senha (caso exista)**.

   - Se você selecionou **Certificado X.509**, clique no botão **Procurar** ao lado do campo **Chave privada (.prk, .pem)** e especifique a chave privada no seu disco rígido. Se a chave privada for protegida por senha, digite a senha no campo **Senha (caso exista)**. Em seguida, clique no botão **Procurar** ao lado do campo **Chave pública (.cer)** e especifique a chave privada no seu disco rígido.

7. Na janela **Certificado**, clique em **OK**.

8. Se necessário, na janela de propriedades do Servidor de Administração, no campo **Porta HTTPS do Servidor da Web**, altere o número da porta HTTPS para o servidor web. Clique em **OK**.

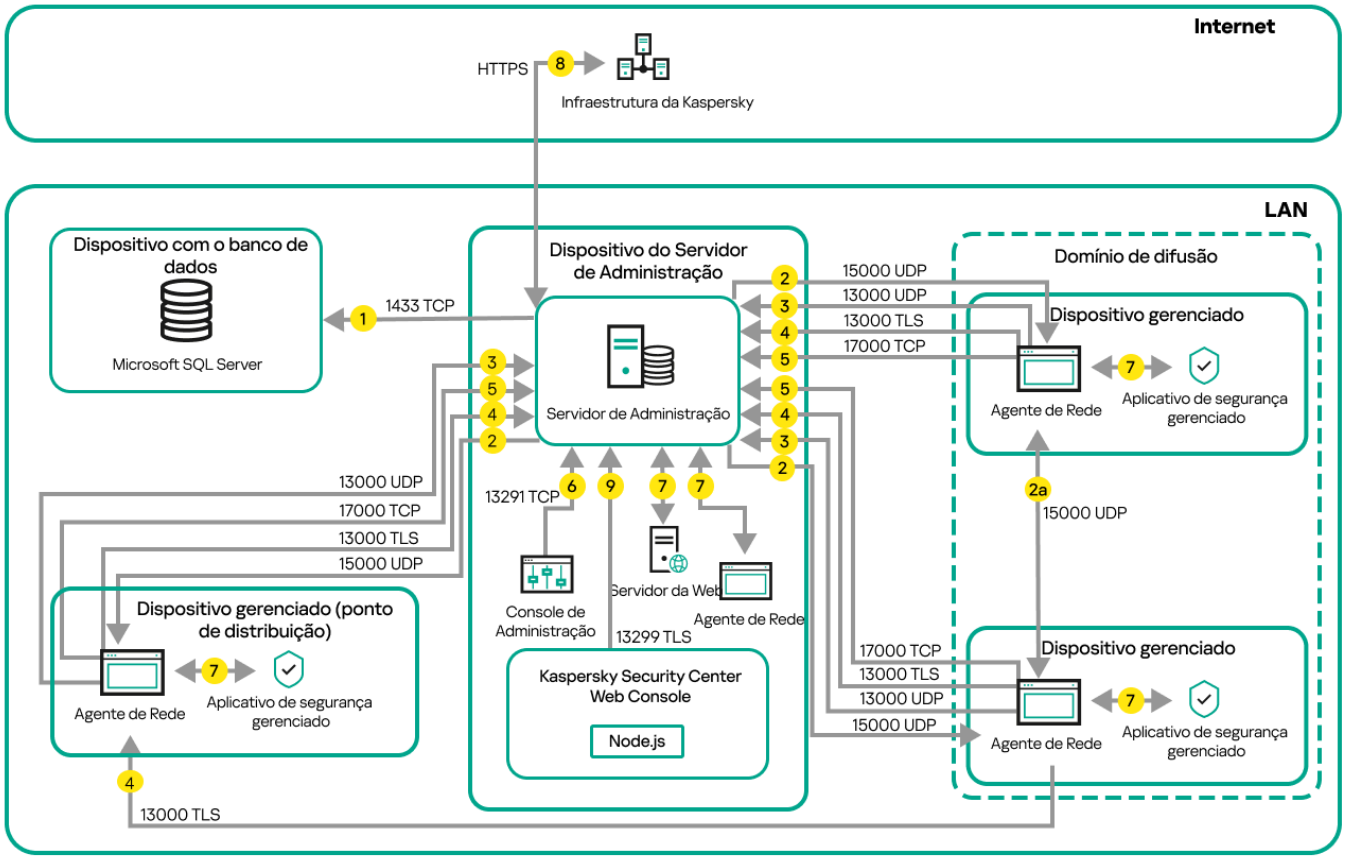
   O certificado do Servidor da Web é emitido novamente.

Esquemas para o tráfego de dados e uso de porta

Esta seção fornece esquemas para o tráfego de dados entre os componentes do Kaspersky Security Center, aplicativos de segurança gerenciados e servidores externos sob diversas configurações. Os esquemas são fornecidos com o número de portas que precisam estar disponíveis nos dispositivos locais.

Servidor de Administração e dispositivos gerenciados dentro de uma rede de área local

A figura abaixo mostra o tráfego dos dados se o Kaspersky Security Center estiver implementado somente em uma rede de área local (LAN).



Servidor de Administração e dispositivos gerenciados em uma rede de área local (LAN)

A figura mostra como diferentes dispositivos gerenciados conectam-se ao Servidor de Administração de diferentes maneiras: diretamente ou via um ponto de distribuição. Os pontos de distribuição reduzem a carga no Servidor de Administração durante a distribuição da atualização e otimizam o tráfego de rede. No, entanto, os pontos de distribuição somente são necessários se o número de dispositivos gerenciados for suficientemente grande. Se o número de dispositivos gerenciados for pequeno, todos os dispositivos gerenciados recebem as atualizações diretamente do Servidor de Administração.

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração e o banco de dados sejam instalados em dispositivos diferentes, será necessário disponibilizar as portas pertinentes no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server ou porta 1433 para Microsoft SQL Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

   > O ponto de distribuição era chamado de "Agente de atualização" nas versões anteriores do Kaspersky Security Center.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. Os dados do Console de Administração baseado em MMC são transferidos para o Servidor de Administração através da porta 13291. (O Console de Administração pode ser instalado no mesmo ou em um dispositivo diferente.)

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

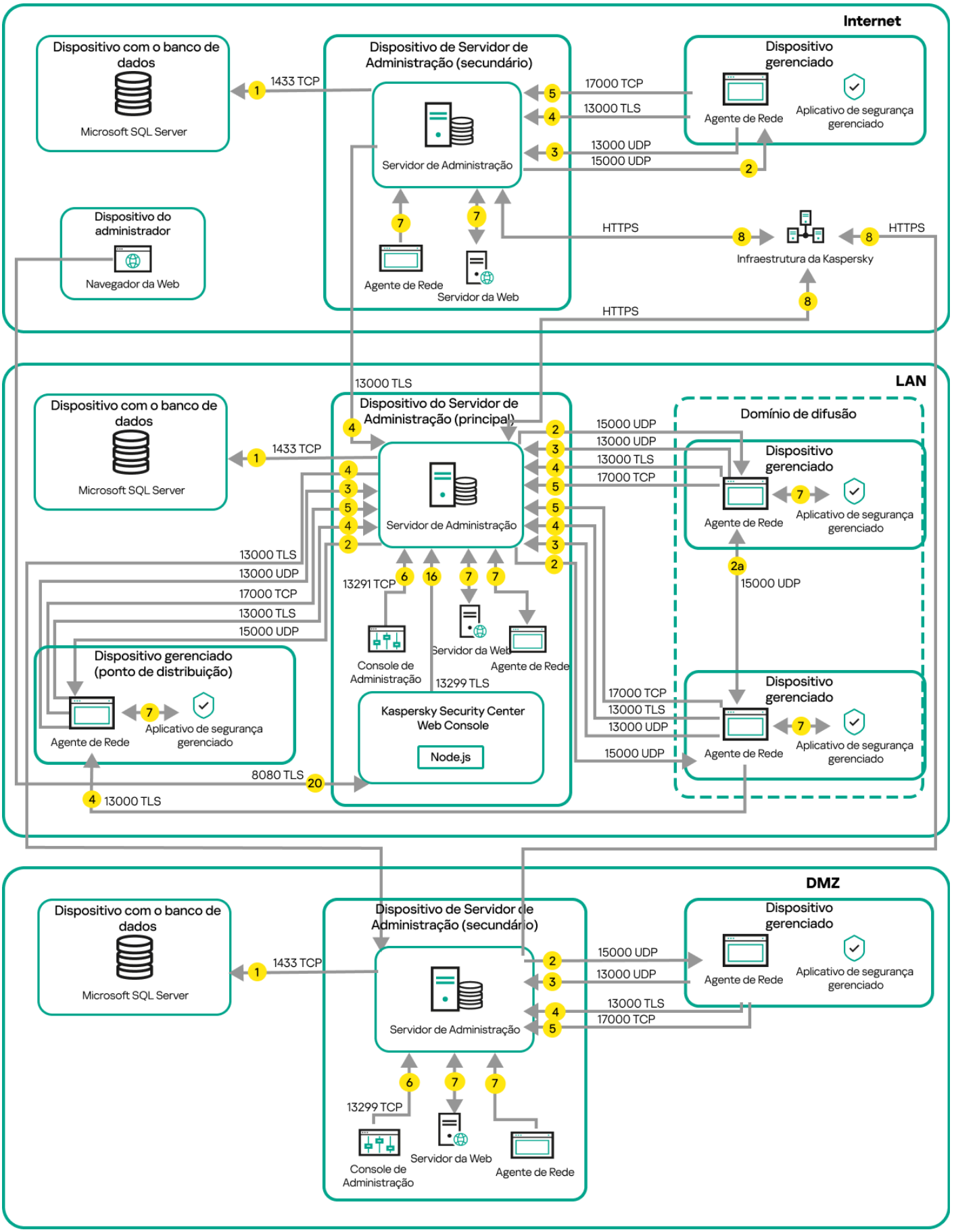
8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. O Kaspersky Security Center Web Console envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

Servidor de Administração principal dentro da rede de área local e dois Servidores de Administração secundários

A figura abaixo mostra a hierarquia dos Servidores de Administração: o Servidor de Administração principal está na rede de área local (LAN). Um Servidor de Administração secundário encontra-se na zona desmilitarizada (DMZ); outros Servidores de Administração secundários estão na Internet.



Hierarquia de Servidores de Administração: Servidor de Administração principal e dois Servidores de Administração secundários

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração e o banco de dados sejam instalados em dispositivos diferentes, será necessário disponibilizar as portas pertinentes no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server ou porta 1433 para Microsoft SQL Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

   > O ponto de distribuição era chamado de "Agente de atualização" nas versões anteriores do Kaspersky Security Center.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. Os dados do Console de Administração baseado em MMC são transferidos para o Servidor de Administração através da porta 13291. (O Console de Administração pode ser instalado no mesmo ou em um dispositivo diferente.)

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

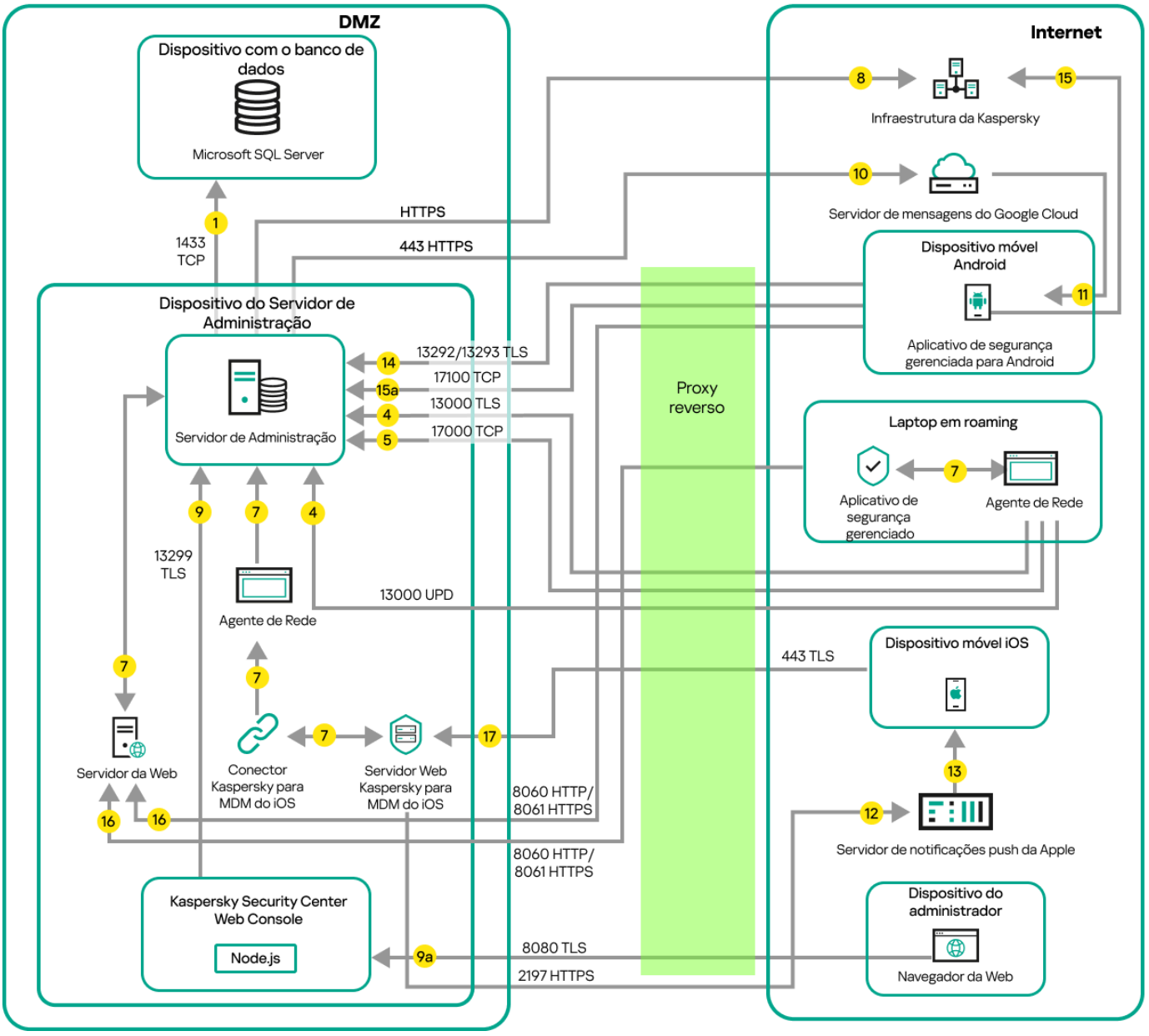
   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. O Kaspersky Security Center Web Console Server envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

   9a. O dados do navegador, que está instalado em um dispositivo separado do administrador, são transferidos ao Kaspersky Security Center Web Console Server através da porta 8080 TLS. O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

Servidor de Administração na LAN, dispositivos gerenciados na Internet, proxy reverso em uso

A figura abaixo exibe o tráfego de dados caso o Servidor de Administração esteja dentro da rede de área local (LAN), e se os dispositivos gerenciados (incluindo os dispositivos móveis) estiverem na Internet. Nesta figura, um proxy reverso de sua escolha está em uso. Consulte a documentação dos aplicativos correspondentes para saber mais detalhes.



Servidor de Administração em uma rede local; dispositivos gerenciados estabelecem conexão com o Servidor de Administração por meio de um proxy reverso

Este esquema de implementação é recomendado se você não deseja que os dispositivos móveis se conectem ao Servidor de Administração diretamente e não deseja atribuir um gateway de conexão na DMZ.

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração e o banco de dados sejam instalados em dispositivos diferentes, será necessário disponibilizar as portas pertinentes no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server ou porta 1433 para Microsoft SQL Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

   > O ponto de distribuição era chamado de "Agente de atualização" nas versões anteriores do Kaspersky Security Center.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. Os dados do Console de Administração baseado em MMC são transferidos para o Servidor de Administração através da porta 13291. (O Console de Administração pode ser instalado no mesmo ou em um dispositivo diferente.)

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. O Kaspersky Security Center Web Console Server envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

   9a. O dados do navegador, que está instalado em um dispositivo separado do administrador, são transferidos ao Kaspersky Security Center Web Console Server através da porta 8080 TLS. O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

10. Somente para dispositivos Android: os dados do Servidor de Administração são transferidos para os servidores da Google. Esta conexão é usada para notificar os dispositivos móveis Android de que precisam se conectar ao Servidor de Administração. As notificações push são enviadas para os dispositivos móveis.

11. Somente para dispositivos móveis Android: as notificações push dos servidores da Google são enviadas para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis de que precisam se conectar ao Servidor de Administração.

12. Somente para dispositivos móveis iOS: os dados do Servidor de MDM do iOS são transferidos para os servidores Apple Push Notification. As notificações push são enviadas para os dispositivos móveis.

13. Somente para dispositivos móveis iOS: as notificações push são enviadas dos servidores da Apple para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis iOS de que precisam se conectar ao Servidor de Administração.

14. Somente para dispositivos móveis: os dados do aplicativo gerenciado são transferidos para o Servidor de Administração (ou para o gateway de conexão) por meio da porta TLS 13292/13293, diretamente ou por um proxy reverso.

15. Somente para dispositivos móveis: os dados do dispositivo móvel são transferidos para a infraestrutura da Kaspersky.

    Se o dispositivo móvel não tiver acesso à Internet, os dados são transferidos para o Servidor de Administração pela porta 17100, e o Servidor de Administração os envia para a infraestrutura da Kaspersky; no entanto, este cenário é raramente usado.

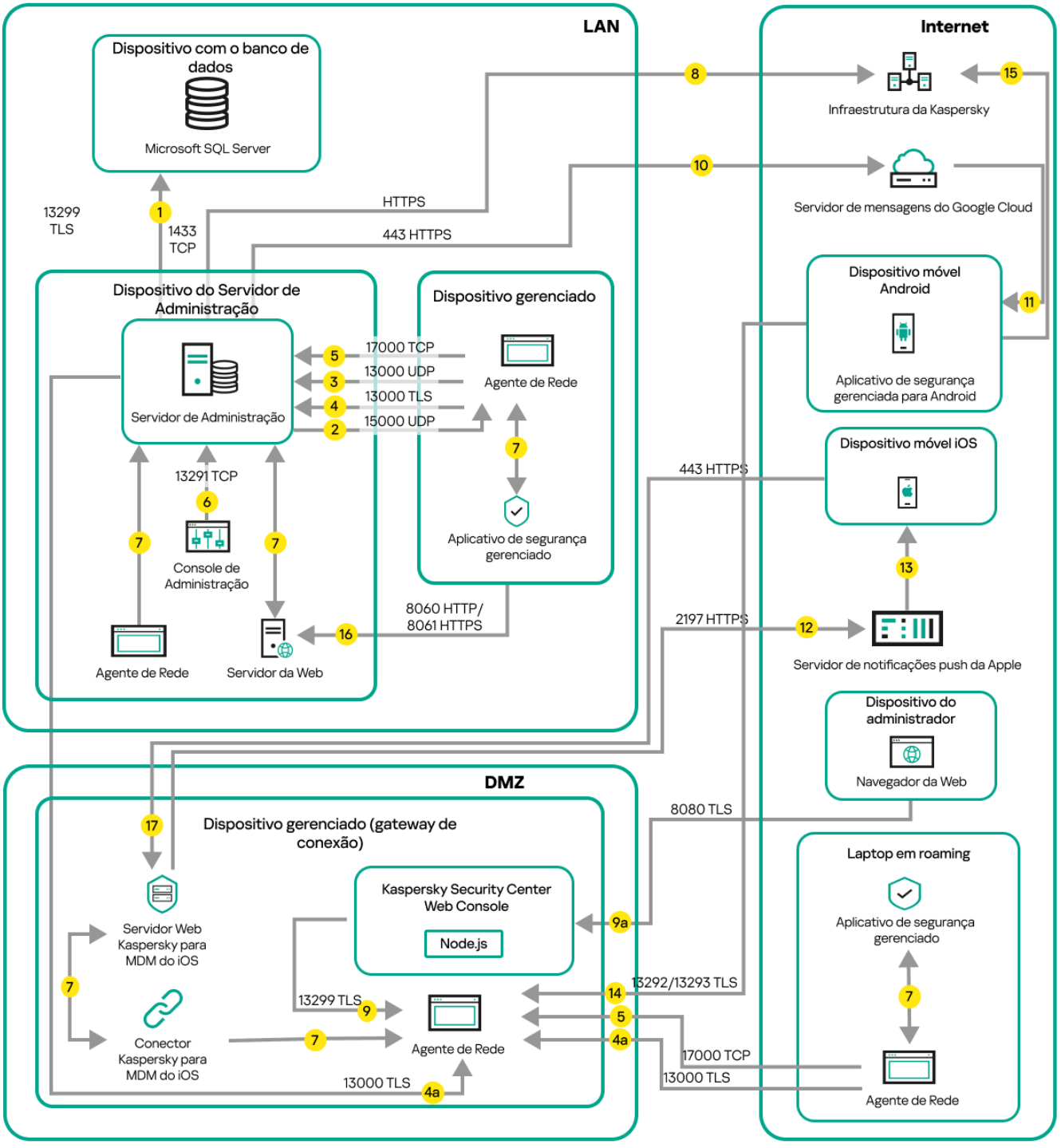
16. Solicitações por pacotes feitas por dispositivos gerenciados, incluindo dispositivos móveis, são transferidas para o Servidor Web, que está no mesmo dispositivo onde está o Servidor de Administração.

17. Somente para dispositivos iOS: os dados do dispositivo móvel são transferidos através da porta 443 TLS para o Servidor de MDM do iOS, que está no mesmo dispositivo que o Servidor de Administração.

Servidor de Administração dentro da LAN, dispositivos gerenciados na Internet, e o gateway de conexão em uso

A figura abaixo exibe o tráfego de dados caso o Servidor de Administração esteja dentro da rede de área local (LAN), e se os dispositivos gerenciados (incluindo os dispositivos móveis) estiverem na Internet. O gateway de conexão está em uso.

Este esquema de implementação é recomendado caso não se queira que os dispositivos móveis se conectem diretamente ao Servidor de Administração e não se deseje usar um proxy reverso ou firewall corporativo.



Gerenciar dispositivos móveis conectados com o Servidor de Administração através de um gateway de conexão

Nesta figura, os dispositivos gerenciados estão conectados com o Servidor de Administração através de um gateway de conexão que está localizado na DMZ. Nenhum proxy reverso ou firewall corporativo está em uso.

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração e o banco de dados sejam instalados em dispositivos diferentes, será necessário disponibilizar as portas pertinentes no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server ou porta 1433 para Microsoft SQL Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

   > O ponto de distribuição era chamado de "Agente de atualização" nas versões anteriores do Kaspersky Security Center.

   4a. Um gateway de conexão na DMZ também recebe a conexão do Servidor de Administração por meio da porta TLS 13000. Como um gateway de conexão na DMZ não pode alcançar as portas do Servidor de Administração, o Servidor de Administração cria e mantém uma conexão de sinal permanente com um gateway de conexão. A conexão de sinal não é usada para transferência de dados, mas apenas para enviar um convite para a interação de rede. Quando o gateway de conexão precisa se conectar ao Servidor, notifica o Servidor por meio dessa conexão de sinal e, em seguida, o Servidor cria a conexão necessária para a transferência de dados.

   Os dispositivos externos também se conectam ao gateway de conexão por meio da porta TLS 13000.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. Os dados do Console de Administração baseado em MMC são transferidos para o Servidor de Administração através da porta 13291. (O Console de Administração pode ser instalado no mesmo ou em um dispositivo diferente.)

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. O Kaspersky Security Center Web Console Server envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

   9a. O dados do navegador, que está instalado em um dispositivo separado do administrador, são transferidos ao Kaspersky Security Center Web Console Server através da porta 8080 TLS. O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

10. Somente para dispositivos Android: os dados do Servidor de Administração são transferidos para os servidores da Google. Esta conexão é usada para notificar os dispositivos móveis Android de que precisam se conectar ao Servidor de Administração. As notificações push são enviadas para os dispositivos móveis.

11. Somente para dispositivos móveis Android: as notificações push dos servidores da Google são enviadas para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis de que precisam se conectar ao Servidor de Administração.

12. Somente para dispositivos móveis iOS: os dados do Servidor de MDM do iOS são transferidos para os servidores Apple Push Notification. As notificações push são enviadas para os dispositivos móveis.

13. Somente para dispositivos móveis iOS: as notificações push são enviadas dos servidores da Apple para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis iOS de que precisam se conectar ao Servidor de Administração.

14. Somente para dispositivos móveis: os dados do aplicativo gerenciado são transferidos para o Servidor de Administração (ou para o gateway de conexão) por meio da porta TLS 13292/13293, diretamente ou por um proxy reverso.

15. Somente para dispositivos móveis: os dados do dispositivo móvel são transferidos para a infraestrutura da Kaspersky.

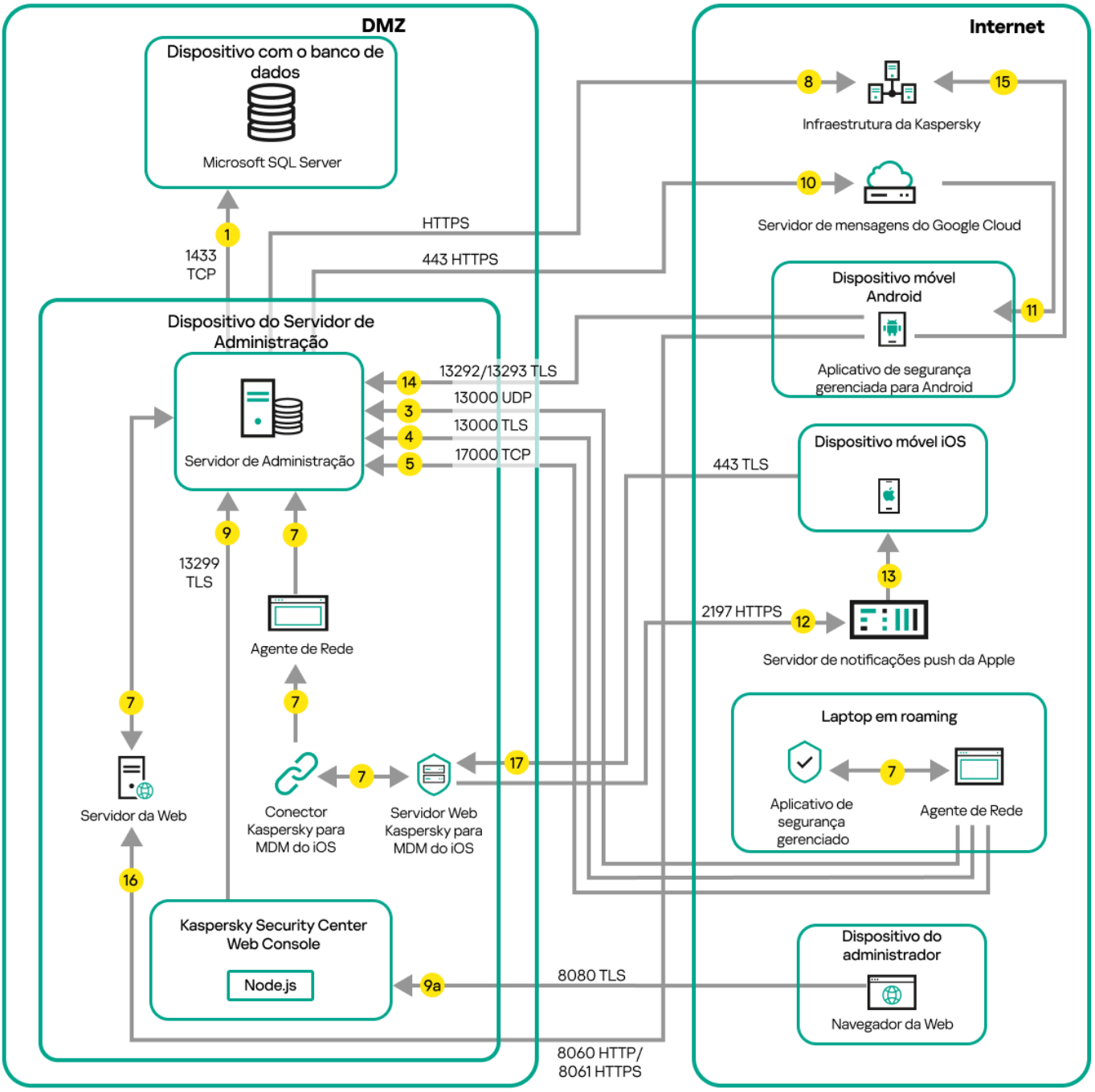
    Se o dispositivo móvel não tiver acesso à Internet, os dados são transferidos para o Servidor de Administração pela porta 17100, e o Servidor de Administração os envia para a infraestrutura da Kaspersky; no entanto, este cenário é raramente usado.

16. Solicitações por pacotes feitas por dispositivos gerenciados, incluindo dispositivos móveis, são transferidas para o Servidor Web, que está no mesmo dispositivo onde está o Servidor de Administração.

17. Somente para dispositivos iOS: os dados do dispositivo móvel são transferidos através da porta 443 TLS para o Servidor de MDM do iOS, que está no mesmo dispositivo que o Servidor de Administração.

Servidor de Administração dentro do DMZ, dispositivos gerenciados na Internet

A figura abaixo mostra o tráfego de dados se o Servidor de Administração estiver dentro da zona desmilitarizada (DMZ), e os dispositivos gerenciados, incluindo os dispositivos móveis, estiverem na Internet.



O Servidor de Administração na DMZ, dispositivos móveis gerenciados na Internet

Nesta figura, nenhum gateway de conexão está em uso: os dispositivos móveis se conectam diretamente ao Servidor de Administração.

As setas indicam a iniciação do tráfego: cada seta aponta de um dispositivo que inicia a conexão para o dispositivo que "responde" a chamada. O número da porta e o nome do protocolo usado para a transferência dos dados são fornecidos. Cada seta tem uma legenda de número e os detalhes sobre o tráfego de dados correspondente são como segue:

1. O Servidor de Administração envia dados para o banco de dados. Caso o Servidor de Administração e o banco de dados sejam instalados em dispositivos diferentes, será necessário disponibilizar as portas pertinentes no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server ou porta 1433 para Microsoft SQL Server). Consulte a documentação do DBMS para obter informações relevantes.

2. Solicitações para a comunicação do Servidor de Administração são transferidas para todos os dispositivos gerenciados não móveis através da porta 15000 UDP.

   Os Agentes de Rede enviam solicitações entre si em um domínio de transmissão. Os dados são então enviados ao Servidor de Administração e são usados para definir os limites do domínio de transmissão e para a atribuição automática de pontos de distribuição (se esta opção estiver ativada).

   Caso o Servidor de Administração não tenha acesso direto aos dispositivos gerenciados, as solicitações de comunicação do Servidor de Administração para esses dispositivos não serão enviadas diretamente.

3. As informações sobre o desligamento dos dispositivos gerenciados são transferidas do Agente de Rede para o Servidor de Administração através da porta 13000 UDP.

4. O Servidor de Administração recebe a conexão dos Agentes de Rede e dos Servidores de Administração secundários por meio da porta TLS 13000.

   Caso uma versão anterior do Kaspersky Security Center seja usada, o Servidor de Administração em sua rede pode receber a conexão de Agentes de Rede por meio da porta não TLS 14000. O Kaspersky Security Center também é compatível com a conexão de Agentes de Rede por meio da porta 14000, embora seja recomendável usar a porta TLS 13000.

   > O ponto de distribuição era chamado de "Agente de atualização" nas versões anteriores do Kaspersky Security Center.

5. Os dispositivos gerenciados (excetos os dispositivos móveis) requerem a ativação através da porta 17000 TCP. Isso não é necessário se o dispositivo tiver seu próprio acesso à Internet; neste caso, o dispositivo envia diretamente da Internet os dados para os servidores da Kaspersky.

6. Os dados do Console de Administração baseado em MMC são transferidos para o Servidor de Administração através da porta 13291. (O Console de Administração pode ser instalado no mesmo ou em um dispositivo diferente.)

7. Aplicativos em um único dispositivo trocam o tráfego local (no Servidor de Administração ou em um dispositivo gerenciado). Nenhuma porta precisa ser aberta.

8. Os dados do Servidor de Administração para os servidores da Kaspersky (tal como dados da KSN ou informações sobre licenças) e os dados dos servidores da Kaspersky para o Servidor de Administração (tal como atualizações do aplicativo e atualizações do banco de dados antivírus) são transferidos usando o protocolo HTTPS.

   Se você não desejar que o Servidor de Administração tenha acesso à Internet, precisará gerenciar esses dados manualmente.

9. O Kaspersky Security Center Web Console Server envia os dados para o Servidor de Administração, que pode ser instalado no mesmo dispositivo ou em um outro, através da porta 13299 TLS.

   9a. O dados do navegador, que está instalado em um dispositivo separado do administrador, são transferidos ao Kaspersky Security Center Web Console Server através da porta 8080 TLS. O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

10. Somente para dispositivos Android: os dados do Servidor de Administração são transferidos para os servidores da Google. Esta conexão é usada para notificar os dispositivos móveis Android de que precisam se conectar ao Servidor de Administração. As notificações push são enviadas para os dispositivos móveis.

11. Somente para dispositivos móveis Android: as notificações push dos servidores da Google são enviadas para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis de que precisam se conectar ao Servidor de Administração.

12. Somente para dispositivos móveis iOS: os dados do Servidor de MDM do iOS são transferidos para os servidores Apple Push Notification. As notificações push são enviadas para os dispositivos móveis.

13. Somente para dispositivos móveis iOS: as notificações push são enviadas dos servidores da Apple para o dispositivo móvel. Esta conexão é usada para notificar os dispositivos móveis iOS de que precisam se conectar ao Servidor de Administração.

14. Somente para dispositivos móveis: os dados do aplicativo gerenciado são transferidos para o Servidor de Administração (ou para o gateway de conexão) por meio da porta TLS 13292/13293, diretamente ou por um proxy reverso.

15. Somente para dispositivos móveis: os dados do dispositivo móvel são transferidos para a infraestrutura da Kaspersky.

    Se o dispositivo móvel não tiver acesso à Internet, os dados são transferidos para o Servidor de Administração pela porta 17100, e o Servidor de Administração os envia para a infraestrutura da Kaspersky; no entanto, este cenário é raramente usado.

16. Solicitações por pacotes feitas por dispositivos gerenciados, incluindo dispositivos móveis, são transferidas para o Servidor Web, que está no mesmo dispositivo onde está o Servidor de Administração.

17. Somente para dispositivos iOS: os dados do dispositivo móvel são transferidos através da porta 443 TLS para o Servidor de MDM do iOS, que está no mesmo dispositivo que o Servidor de Administração.

Interação dos componentes e aplicativos de segurança do Kaspersky Security Center: mais informações

Esta seção fornece os esquemas para a interação de componentes do Kaspersky Security Center e aplicativos de segurança gerenciados. Os esquemas fornecem os números das portas que devem estar disponíveis e os nomes dos processos que abrem aquelas portas.

Convenções usadas em esquemas de interação

A tabela a seguir fornece as convenções usadas através dos esquemas.

Convenções de documentos

Ícone	Significado
	Servidor de Administração

	Servidor de Administração secundário
	DBMS
	O dispositivo cliente (que tem o Agente de Rede e um aplicativo da família do Kaspersky Endpoint Security instalado, ou tem um aplicativo de segurança diferente instalado que o Kaspersky Security Center pode gerenciar)
	Gateway de conexão
	Ponto de distribuição
	O dispositivo cliente móvel com o Kaspersky Security for Mobile
	Navegador no dispositivo do usuário
	Processo em execução no dispositivo e abrir uma porta
	Porta e seu número
	Tráfego TCP (a direção da seta mostra a direção do fluxo de tráfego)
	Tráfego UDP (a direção da seta mostra a direção do fluxo de tráfego)
	Chamar o COM
	Transporte de DBMS
	Limite de DMZ

Servidor de Administração e DBMS

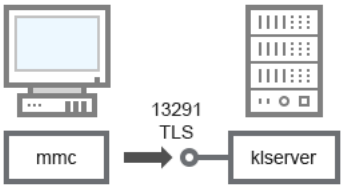
Os dados do Servidor de Administração são inseridos no banco de dados SQL Server, MySQL e MariaDB.



Servidor de Administração e DBMS

Caso o Servidor de Administração e o banco de dados sejam instalados em dispositivos diferentes, será necessário disponibilizar as portas pertinentes no dispositivo onde o banco de dados está localizado (por exemplo, porta 3306 para MySQL Server ou porta 1433 para Microsoft SQL Server). Consulte a documentação do DBMS para obter informações relevantes.

Servidor de Administração e Console de Administração



Servidor de Administração e Console de Administração

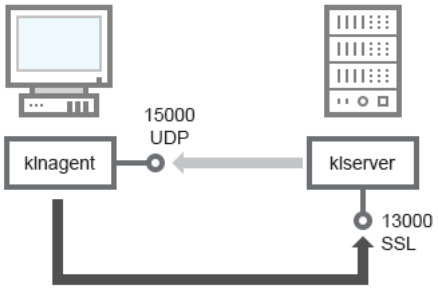
Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Servidor de Administração e Console de Administração (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	TLS	Propósito da porta
Servidor de Administração	13291	klserver	TCP	Sim	Receber conexões do Console de Administração

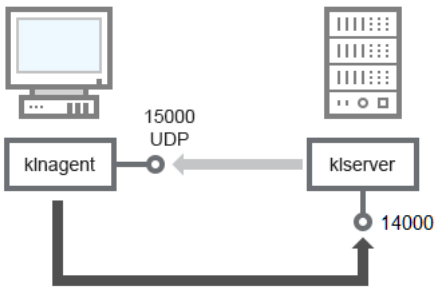
Servidor de Administração e dispositivo cliente: Gerenciar o aplicativo de segurança

O Servidor de Administração recebe a conexão dos Agentes de Rede através da porta SSL 13000 (veja a figura abaixo).



Servidor de Administração e dispositivo cliente: gerenciando o aplicativo de segurança, conexão através da porta 13000 (recomendado)

Se você usou uma versão anterior do Kaspersky Security Center, o Servidor de Administração na sua rede poderá receber conexões de Agentes de Rede através da porta não SSL 14000 (veja a figura abaixo). O Kaspersky Security Center 14.2 também suporta a conexão de Agente de Rede através da porta 14000, embora o uso da porta SSL 13000 é o recomendado.



Servidor de Administração e dispositivo cliente: gerenciando o aplicativo de segurança, conexão através da porta 14000 (segurança mais baixa)

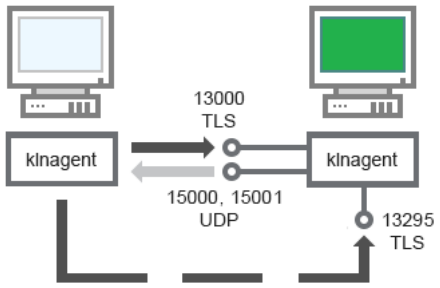
Para obter a clarificação dos esquemas, consulte a tabela abaixo.

Servidor de Administração e dispositivo cliente: Gerenciar o aplicativo de segurança (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	TLS (somente para TCP)	Propósito da porta
Agente de Rede	15000	klnagent	UDP	Null	Multicasting para Agente de Rede
Servidor de Administração	13000	klserver	TCP	Sim	Receber conexões dos Agentes de Rede
Servidor de Administração	14000	klserver	TCP	Não	Receber conexões dos Agentes de Rede

Atualizar o software em um dispositivo cliente através de uma ponto de distribuição

O dispositivos cliente conecta-se ao ponto de distribuição via porta 13000 e, se você estiver usando um ponto de distribuição como servidor push, também via porta 13295. O ponto de distribuição efetua uma transmissão multicast para os Agentes de Rede via port 15000 (ver figura abaixo). Atualizações e pacotes de instalação são recebidos de um ponto de distribuição pela porta 15001.



Atualizar o software em um dispositivo cliente através de uma ponto de distribuição

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Atualizar o software através de um ponto de distribuição (tráfego)

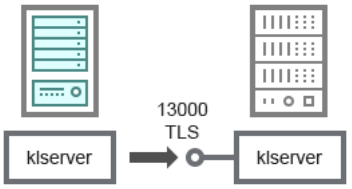
Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	TLS (somente para TCP)	Propósito da porta
Agente de Rede	15000	klnagent	UDP	Null	Multicasting para Agente de Rede
Agente de Rede	15001	klnagent	UDP	Null	Recebendo atualizações e pacotes de instalação de um ponto de distribuição
Ponto de distribuição	13000	klnagent	TCP	Sim	Receber conexões dos Agentes de Rede
Ponto de distribuição	13295	klnagent	TCP	Sim	Recebendo conexões de dispositivos cliente (push do servidor)

Hierarquia de Servidores de Administração: Servidor de Administração principal e Servidor de Administração secundário

O esquema (veja a figura abaixo) mostra como usar a porta 13000 para assegurar a interação entre os Servidores de Administração combinados em uma hierarquia.

Ao combinar dois Servidores de Administração em uma hierarquia, assegure-se de que a porta 13291 esteja acessível em ambos os Servidores de Administração. O Console de Administração conecta-se ao Servidor de Administração através da porta 13291.

Subsequentemente, quando os Servidores de Administração são combinados em uma hierarquia, você pode administrar ambos usando o Console de Administração conectado ao Servidor de Administração principal. Portanto, a acessibilidade da porta 13291 do Servidor de Administração principal é o único prerrequisito.



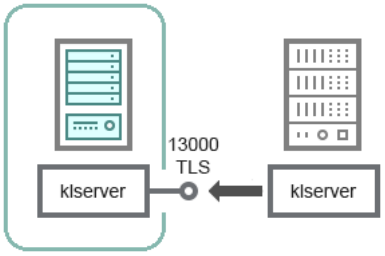
Hierarquia de Servidores de Administração: Servidor de Administração principal e Servidor de Administração secundário

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Hierarquia de Servidores de Administração (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	TLS	Propósito da porta
Servidor de Administração principal	13000	klserver	TCP	Sim	Receber conexões dos Servidores de Administração secundários

Hierarquia de Servidores de Administração com um Servidor de Administração secundário na DMZ



Hierarquia de Servidores de Administração com um Servidor de Administração secundário na DMZ

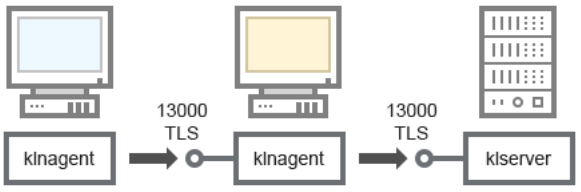
O esquema mostra uma hierarquia de Servidores de Administração nos quais o Servidor de Administração secundário localizado na DMZ recebe uma conexão do Servidor de Administração principal (consulte a tabela abaixo para obter explicações sobre o esquema). Ao combinar dois Servidores de Administração em uma hierarquia, assegure-se de que a porta 13291 esteja acessível em ambos os Servidores de Administração. O Console de Administração conecta-se ao Servidor de Administração através da porta 13291.

Subsequentemente, quando os Servidores de Administração são combinados em uma hierarquia, você pode administrar ambos usando o Console de Administração conectado ao Servidor de Administração principal. Portanto, a acessibilidade da porta 13291 do Servidor de Administração principal é o único prerrequisito.

Hierarquia de Servidores de Administração com um Servidor de Administração de secundário na DMZ (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	TLS	Propósito da porta
Servidor de Administração secundário	13000	klserver	TCP	Sim	Recebendo conexões do Servidor de Administração principal

Servidor de Administração, um gateway de conexão em um segmento da rede e um dispositivo cliente



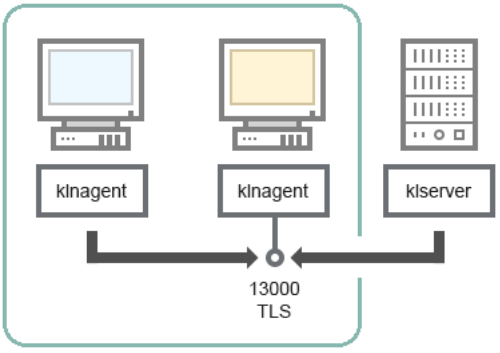
Servidor de Administração, um gateway de conexão em um segmento da rede e um dispositivo cliente

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Servidor de Administração, um gateway de conexão em um segmento da rede e um dispositivo cliente (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	TLS	Propósito da porta
Servidor de Administração	13000	klserver	TCP	Sim	Receber conexões dos Agentes de Rede
Agente de Rede	13000	klnagent	TCP	Sim	Receber conexões dos Agentes de Rede

Servidor de Administração e dois dispositivos na DMZ: um gateway de conexão e um dispositivo cliente



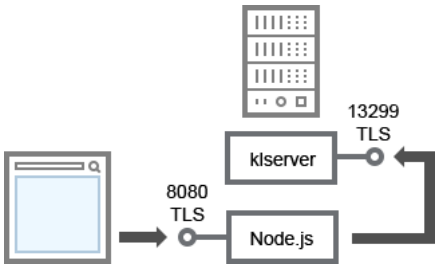
Servidor de Administração com um gateway de conexão e um dispositivo cliente em DMZ

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Servidor de Administração com um gateway de conexão em um segmento da rede e um dispositivo cliente (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	TLS	Propósito da porta
Agente de Rede	13000	klnagent	TCP	Sim	Receber conexões dos Agentes de Rede

Servidor de Administração e Kaspersky Security Center Web Console



Servidor de Administração e Kaspersky Security Center Web Console

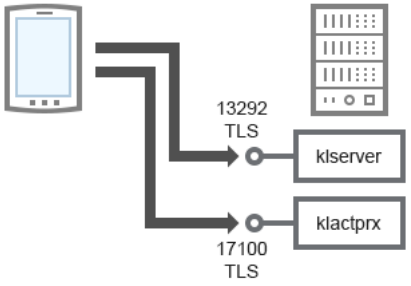
Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Servidor de Administração e Kaspersky Security Center Web Console (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	TLS	Propósito da porta
Servidor de Administração	13299	klserver	TCP	Sim	Receber conexões do Kaspersky Security Center Web Console para o Servidor de Administração através do OpenAPI
Kaspersky Security Center Web Console Server ou Servidor de Administração	8080	Node.js: JavaScript do lado do servidor	TCP	Sim	Receber conexões do Kaspersky Security Center Web Console

O Kaspersky Security Center Web Console pode ser instalado no Servidor de Administração ou em outro dispositivo.

Ativar e gerenciar o aplicativo de segurança em um dispositivo móvel



Ativar e gerenciar o aplicativo de segurança em um dispositivo móvel

Para esclarecimentos sobre o esquema, consulte a tabela abaixo.

Ativar e gerenciar o aplicativo de segurança em um dispositivo móvel (tráfego)

Dispositivo	Número da porta	Nome do processo que abre a porta	Protocolo	TLS	Propósito da porta
Servidor de Administração	13292	klserver	TCP	Sim	Configurar as conexões do Console de Administração ao Servidor de Administração
Servidor de Administração	17100	klactprx	TCP	Sim	Recebendo conexões para a ativação do aplicativo de dispositivos móveis

Implementação de melhores práticas

O Kaspersky Security Center é um aplicativo distribuído. O Kaspersky Security Center suporta os seguintes aplicativos:

- Servidor de Administração – o componente principal, projetado para gerenciar os dispositivos de uma organização e armazenar dados em um DBMS.
- Console de Administração – A ferramenta básica do administrador. A Console de Administração é fornecido junto com o Servidor de Administração, mas também pode ser instalado individualmente em um ou diversos dispositivos executados pelo administrador.
- Agente de Rede – Projetado para gerenciar o aplicativo de segurança instalado em um dispositivo, assim como obter informações sobre esse dispositivo e transferir essas informações para o Servidor de Administração. Os Agentes de Rede são instalados em dispositivos de uma organização.

A implementação do Kaspersky Security Center em uma rede da organização é executada como segue:

- Instalação do Servidor de Administração
- Instalação do Console de Administração no dispositivo do administrador
- Instalação do Agente de Rede e do aplicativo de segurança em dispositivos da empresa

Guia de Proteção

O Kaspersky Security Center foi concebido para a execução centralizada de tarefas de administração e manutenção básicas na rede de uma organização. O aplicativo fornece ao administrador acesso a informações detalhadas sobre o nível de segurança da rede da organização. O Kaspersky Security Center permite configurar todos os componentes de proteção criados com o uso dos aplicativos Kaspersky.

O Servidor de Administração do Kaspersky Security Center tem acesso total ao gerenciamento de proteção de dispositivos clientes, além de ser o componente mais importante do sistema de segurança da organização. Portanto, métodos de proteção aprimorados são necessários para o Servidor de Administração.

Antes de configurar, crie uma cópia de backup do Servidor de Administração do Kaspersky Security Center com o uso da tarefa Backup de dados do Servidor de Administração ou o utilitário klbackup e salve-a em um local seguro.

O Guia de Proteção descreve as recomendações e recursos de configuração do Kaspersky Security Center e seus componentes com o objetivo de reduzir os riscos de seu comprometimento.

O Guia de Proteção contém as seguintes informações:

- Seleção da arquitetura do Servidor de Administração
- Configuração de uma conexão segura com o Servidor de Administração
- Configuração de contas para acesso ao Servidor de Administração

- Gerenciamento da proteção do Servidor de Administração
- Gerenciamento de proteção dos dispositivos cliente
- Configuração da proteção para aplicativos gerenciados
- Manutenção do Servidor de Administração
- Transferência de informações para aplicativos de terceiros
- Recomendações de segurança para sistemas de informações de terceiros

Implementação do Servidor de Administração

Arquitetura do Servidor de Administração

Em geral, a escolha de uma arquitetura de gerenciamento centralizado depende da localização dos dispositivos protegidos, acesso a redes adjacentes, esquemas de entrega de atualizações do banco de dados e assim por diante.

Na fase inicial de desenvolvimento da arquitetura, recomendamos conhecer os componentes do Kaspersky Security Center e sua interação uns com os outros, assim como os esquemas para o tráfego de dados e uso de porta.

De acordo com essas informações, será possível formar uma arquitetura que especifique:

- A localização do Servidor de Administração e as conexões de rede
- Organização dos espaços de trabalho do administrador e métodos de conexão com o Servidor de Administração
- Os métodos de implementação do Agente de Rede e do software de proteção
- Uso dos pontos de distribuição
- Uso de Servidores de Administração virtuais
- Uso de uma hierarquia de Servidores de Administração
- O esquema de atualização do banco de dados de antivírus
- Outros fluxos de informação

Seleção de um dispositivo para a instalação do Servidor de Administração

Recomendamos instalar o Servidor de Administração em um servidor dedicado na infraestrutura da organização. Caso não haja outro software de terceiros instalado no servidor, é possível definir as configurações de segurança de acordo com os requisitos do Kaspersky Security Center sem haver a dependência dos requisitos de software de terceiros.

É possível implementar o Servidor de Administração em um servidor físico ou em um servidor virtual. Verifique e confirme se o dispositivo selecionado atende aos requisitos de hardware e software.

Localização do Servidor de Administração

Os dispositivos gerenciados pelo Servidor de Administração podem ser localizados da seguinte forma:

- Em uma rede local (LAN)
- Na Internet
- Na zona desmilitarizada (DMZ)

Ao mesmo tempo, o Servidor de Administração também pode estar localizado em diferentes segmentos: segmentos industriais, corporativos e DMZ.

Caso o Kaspersky Security Center seja usado para gerenciar a proteção de um segmento de rede isolado, recomendamos implementar o Servidor de Administração em um segmento da zona desmilitarizada (DMZ). Isso permite organizar uma segmentação de rede adequada e minimizar o fluxo de tráfego para o segmento protegido, o que mantém os recursos completos de gerenciamento e entrega de atualizações.

Restrição de implementação do Servidor de Administração em um controlador de domínio, um servidor de terminal ou um dispositivo de usuário

Não recomendamos instalar o Servidor de Administração em um controlador de domínio, um servidor de terminal ou um dispositivo de usuário.

Recomendamos que a separação funcional dos nós de chave de rede seja fornecida. Essa abordagem permite manter a operacionalidade de diferentes sistemas quando um nó falhar ou for comprometido. Ao mesmo tempo, é possível criar diferentes políticas de segurança para cada nó.

Por exemplo, as restrições de segurança geralmente aplicadas a um controlador de domínio podem reduzir significativamente o desempenho do Servidor de Administração e impossibilitar o uso de alguns de seus recursos. Caso um intruso obtenha acesso privilegiado ao controlador de domínio, o banco de dados do Active Directory Domain Services (AD DS) pode ser modificado, danificado ou destruído. Além disso, todos os sistemas e contas gerenciados pelo Active Directory podem ser comprometidos.

Contas para instalar e executar o Servidor de Administração

Recomendamos executar a instalação do Servidor de Administração em uma conta de administrador local para evitar o uso de contas de domínio para acessar o banco de dados do Servidor de Administração. Um conjunto de contas necessárias e seus direitos depende do tipo de DBMS selecionado, localização do DBMS e método de criação do banco de dados do Servidor de Administração.

Os grupos KLAdmins e KLOperators são criados automaticamente durante a instalação do Kaspersky Security Center. Para estes grupos são concedidos os direitos de se conectar-se ao Servidor de Administração e processar os objetos do Servidor de Administração.

Dependendo de qual tipo de conta for usado para a instalação do Kaspersky Security Center, os grupos KLAdmins e KLOperators são criados como segue:

- Caso o aplicativo seja instalado com uma conta de usuário incluída em um domínio, os grupos são criados no Servidor de Administração do dispositivo e no domínio que inclui o Servidor de Administração.
- Caso o aplicativo seja instalado a partir de uma conta de sistema, os grupos são criados somente em um Servidor de Administração.

Para evitar a criação de grupos KLAdmins e KLOperators no domínio e, consequentemente, **fornecer privilégios para gerenciar o Servidor de Administração em uma conta fora do dispositivo do Servidor de Administração**, recomendamos instalar o Kaspersky Security Center em uma conta local.

Durante a instalação do Servidor de Administração, selecione a conta que será usada para iniciá-lo como um serviço. Por padrão, o aplicativo cria uma conta local chamada KL-AK-*, sob a qual o serviço do Servidor de Administração (o serviço klserver) será executado.

Caso seja necessário, o serviço do Servidor de Administração pode ser executado na conta selecionada. Essa conta deve receber os direitos necessários para acessar o DBMS. Por questões de segurança, use uma conta sem privilégios para executar o serviço do Servidor de Administração.

Para evitar o uso de configurações de conta incorretas, recomendamos gerar a conta automaticamente.

Exclusão do Servidor de Administração de um domínio

Caso use o Servidor de Administração para proteger grupos de dispositivos de sistemas de alta importância, não recomendamos incluir o dispositivo do Servidor de Administração no domínio. Isso permite diferenciar os direitos de gerenciamento do Kaspersky Security Center e impedir o acesso ao Servidor de Administração caso a conta do domínio seja comprometida.

Leve em consideração que, caso o Servidor de Administração seja instalado em um dispositivo incluído no grupo de trabalho, os seguintes cenários de trabalho com o Servidor de Administração não estarão disponíveis:

- Uso de um cluster de failover do Kaspersky Security Center
- Uso de um cluster de failover do Windows Server
- Uso do SQL Server for Windows em um dispositivo separado

  Só é possível usar o SQL Server for Windows em um dispositivo separado caso o Servidor de Administração e o SQL Server estiverem no mesmo domínio ou em domínios confiáveis. Se o Servidor de Administração, o SQL Server e um compartilhamento UNC para backups estiverem em um grupo de trabalho, não será possível configurar com segurança os direitos de acesso e leitura/gravação entre o SQL Server e o compartilhamento.
- Instalação remota com as ferramentas do Servidor de Administração pelas políticas de grupo do Active Directory

Caso seja necessário desconectar o Servidor de Administração do domínio do Active Directory, siga as etapas descritas no tópico: Como alterar o nome do Kaspersky Security Center.

Caso seja necessário instalar o Servidor de Administração em um dispositivo incluído no grupo de trabalho, também é possível usar o Kaspersky Security Center Linux em vez do Kaspersky Security Center Windows.

Segurança de conexão

Uso de TLS

Recomendamos proibir as conexões inseguras com o Servidor de Administração. Por exemplo, é possível proibir as conexões que usam HTTP nas configurações do Servidor de Administração.

Observe que, por padrão, várias portas HTTP do Servidor de Administração estão fechadas. A porta restante é usada para o servidor web do Servidor de Administração (8060). Essa porta pode ser limitada pelas configurações do firewall do dispositivo do Servidor de Administração.

Configurações estritas de TLS

Recomendamos usar o protocolo TLS, versão 1.2 e posterior, e restringir ou proibir algoritmos de criptografia inseguros.

Você pode configurar os protocolos de criptografia (TLS) usados pelo Servidor de Administração. Observe que, no momento do lançamento de uma versão do Servidor de Administração, o protocolo de criptografia é configurado por padrão para garantir a transferência segura de dados.

Proibição de autenticação remota usando contas do Windows

É possível usar o sinalizador LP_RestrictRemoteOsAuth para proibir as conexões SSPI de endereços remotos. Esse sinalizador permite proibir a autenticação remota no Servidor de Administração usando contas locais ou de domínio do Windows.

Para mudar o sinalizador LP_RestrictRemoteOsAuth para o modo de proibição de conexões de endereços remotos:

1. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Execute o seguinte comando na linha de comando para especificar o valor do sinalizador LP_RestrictRemoteOsAuth:

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

3. Reinicie o serviço do Servidor de Administração.

O sinalizador LP_RestrictRemoteOsAuth não funciona se a autenticação remota for executada pelo Kaspersky Security Center Web Console ou pelo Console de Administração instalado no dispositivo do Servidor de Administração.

Restrição de acesso ao banco de dados do Servidor de Administração

Recomendamos restringir o acesso ao banco de dados do Servidor de Administração. Por exemplo, conceda acesso apenas ao dispositivo a partir do Servidor de Administração. Isso reduz a probabilidade de o banco de dados do Servidor de Administração ser comprometido devido a vulnerabilidades conhecidas.

É possível configurar os parâmetros de acordo com as instruções de operação do banco de dados usado, assim como fornecer portas fechadas em firewalls.

Autenticação do Microsoft SQL Server

Caso o Kaspersky Security Center use o Microsoft SQL Server como um DBMS, será necessário proteger os dados do Kaspersky Security Center transferidos de ou para o banco de dados e os dados armazenados no banco de dados contra acesso não autorizado. Para fazer isso, é necessário fornecer uma comunicação segura entre o Kaspersky Security Center e o SQL Server. A maneira mais confiável de fornecer comunicação segura é instalando o Kaspersky Security Center e o SQL Server no mesmo dispositivo e usando o mecanismo de memória compartilhada para os dois aplicativos. Em todos os outros casos, recomendamos usar um certificado SSL/TLS para autenticar a instância do SQL Server.

Normalmente, o Servidor de Administração pode tratar o SQL Server usando os seguintes fornecedores:

- SQLOLEDB usando o TCP/IP ou Pipes nomeados

  Esse fornecedor é instalado em um sistema com Windows e utilizado como padrão.

- MSOLEDBSQL usando TCP/IP, Pipes nomeados ou Memória compartilhada

  Se você quiser usar esse fornecedor, precisa instalá-lo em um dispositivo com o Servidor de Administração, definir o valor `1` para a variável do ambiente global `KLDBADO_UseMSOLEDBSQL`.

- MSOLEDBSQL19 usando TCP/IP, Pipes nomeados ou Memória compartilhada

  Se você quiser usar esse fornecedor, precisa instalá-lo no dispositivo com o Servidor de Administração, definir o valor `1` para a variável do ambiente global `KLDBADO_UseMSOLEDBSQL` e o valor `MSOLEDBSQL19` para a variável do ambiente global `KLDBADO_ProviderName`.

Além disso, antes de usar o TCP/IP, Pipes nomeados ou a Memória compartilhada, certifique-se de que o protocolo necessário esteja ativo.

Interação de segurança com um DBMS externo

Se o DBMS for instalado em um dispositivo separado durante a instalação do Servidor de Administração (DBMS externo), recomendamos configurar os parâmetros para interação segura e autenticação com este DBMS. Para mais informações sobre como configurar a autenticação SSL, consulte Autenticação do Servidor PostgreSQL e Cenário: Autenticação do Servidor MySQL.

Configuração de uma lista de permissão de endereços IP para conexão ao Servidor de Administração

Por padrão, os usuários do Kaspersky Security Center podem fazer login nele de qualquer dispositivo em que o Console de Administração baseado em MMC, o Kaspersky Security Center Web Console ou os aplicativos OpenAPI estejam instalados. É possível configurar o Servidor de Administração para que os usuários apenas possam se conectar a ele apenas em dispositivos com endereços IP permitidos. Por exemplo, se um invasor tentar se conectar ao Kaspersky Security Center por meio do servidor do Kaspersky Security Center Web Console instalado em um dispositivo que não está incluído na lista de permissões, não conseguirá fazer login no Kaspersky Security Center.

Configuração de uma lista de permissão de endereços IP para conexão ao Kaspersky Security Center Web Console

Por padrão, os usuários do Kaspersky Security Center podem se conectar ao Kaspersky Security Center Web Console de qualquer dispositivo. Em um dispositivo com o Kaspersky Security Center Web Console instalado, é necessário configurar o firewall (integrado ao sistema operacional ou de terceiros) para que os usuários possam se conectar ao Kaspersky Security Center Web Console apenas usando endereços IP permitidos.

Segurança da conexão com o controlador de domínio durante a sondagem

O Servidor de Administração ou um ponto de distribuição Linux se conecta ao controlador de domínio via LDAPS para pesquisar o domínio. Por padrão, a verificação de certificado não é exigida durante a conexão. Para impor a verificação de certificado, defina o sinalizador `KLNAG_LDAP_TLS_REQCERT` como 1. Além disso, é possível especificar um caminho personalizado para a autoridade certificadora (CA) a fim de conectar a cadeia de certificados, usando o sinalizador `KLNAG_LDAP_SSL_CACERT`.

Contas e autenticação

Antes de executar as etapas abaixo, crie uma cópia backup do Servidor de Administração do Kaspersky Security Center Linux usando a tarefa de backup de dados do Servidor de Administração ou o utilitário klbackup e salve-a em um local seguro.

Uso da verificação em duas etapas com o Servidor de Administração

O Kaspersky Security Center fornece verificação em duas etapas para os usuários do Kaspersky Security Center Web Console e Console de Administração de acordo com o padrão RFC 6238 (TOTP: Algoritmo de Senha Avulsa por Tempo Limitado).

Quando a verificação em duas etapas é ativada para a sua própria conta, toda vez que o login for feito no Kaspersky Security Center Web Console ou no Console de Administração, será necessário inserir o nome de usuário, senha e um código de segurança único adicional. Se você usar autenticação de domínio para sua conta, você só precisa inserir um código de segurança de uso único adicional. Para receber um código de segurança de uso único, é necessário instalar um app autenticador em seu computador ou dispositivo móvel.

Existem autenticadores de software e hardware (tokens) que são compatíveis com o padrão RFC 6238. Por exemplo, autenticadores de software incluem o Google Authenticator, Microsoft Authenticator, FreeOTP.

É altamente recomendável não instalar o app autenticador no mesmo dispositivo no qual a conexão com o Servidor de Administração é estabelecida. É possível instalar um app autenticador no seu dispositivo móvel.

Uso da autenticação de dois fatores para um sistema operacional

Recomendamos o uso de autenticação multifator (MFA) para autenticação no dispositivo do Servidor de Administração com o uso de um token, um cartão inteligente ou outro método (caso seja possível).

Proibição para salvar a senha do administrador

Caso o Console de Administração seja usado, não recomendamos salvar a senha do administrador na caixa de diálogo de conexão do Servidor de Administração.

Caso Kaspersky Security Center Web Console seja usado, não recomendamos salvar a senha do administrador no navegador instalado no dispositivo do usuário.

Autenticação de uma conta de usuário interna

Por padrão, a senha de uma conta de usuário interna do Servidor de Administração deve seguir as seguintes regras:

- A senha deve ter de 8 a 256 caracteres.
- A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
  - Letras maiúsculas (A-Z)
  - Letras minúsculas (a-z)
  - Números (0-9)
  - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
- A senha não deve conter nenhum espaço em branco, caracteres Unicode ou a combinação dos caracteres "." e "@", quando "." estiver colocado antes de "@".

Por padrão, o número máximo permitido de tentativas de entrada da senha é 10. É possível alterar o número permitido de tentativas de inserção de senha.

O usuário do Kaspersky Security Center pode inserir uma senha inválida um número limitado de vezes. Depois que o limite é atingido, a conta de usuário é bloqueada por uma hora.

Grupo de administração dedicado para Servidor de Administração

Recomendamos criar um grupo de administração dedicado para o Servidor de Administração. Conceda direitos de acesso especiais para esse grupo e crie uma política de segurança especial para ele.

Para evitar diminuir intencionalmente o nível de segurança do Servidor de Administração, recomendamos restringir a lista de contas que podem gerenciar o grupo de administração dedicado.

Os grupos KLAdmins e KLOperators

Os grupos KLAdmins e KLOperators são criados automaticamente durante a instalação do Kaspersky Security Center. O grupo KLAdmins recebe todos os direitos de acesso. O grupo KLOperators recebe apenas direitos de leitura e execução. Os direitos concedidos ao grupo KLAdmins são **bloqueados**.

É possível visualizar os grupos KLAdmins e KLOperators e fazer alterações neles usando as ferramentas administrativas padrão do sistema operacional.

Ao desenvolver regulamentos de trabalho do Servidor de Administração, é necessário determinar se o especialista em segurança da informação precisará ter acesso total (e inclusão no grupo KLAdmins) para executar as tarefas padrão.

A maioria das tarefas básicas de administração podem ser distribuídas entre departamentos da empresa (ou diferentes funcionários do mesmo departamento) e, consequentemente, entre diferentes contas. Também é possível configurar a diferenciação de acesso dos grupos de administração no Kaspersky Security Center. Como resultado, é possível implementar um cenário no qual a autorização em contas do grupo KLAdmins seja anômala e possa ser considerada um incidente.

Caso o Kaspersky Security Center tenha sido instalado em uma conta do sistema, os grupos serão criados apenas no dispositivo do Servidor de Administração. Neste caso, recomendamos verificar e confirmar se apenas as entradas criadas durante a instalação do Kaspersky Security Center estão incluídas no grupo. Não recomendamos adicionar nenhum grupo ao grupo KLAdmins (local e/ou domínio) criado automaticamente durante a instalação do Kaspersky Security Center. Também é necessário limitar os direitos para alterar esse grupo. O grupo KLAdmins deve incluir apenas contas únicas sem privilégios.

Caso a instalação tenha sido executada em uma conta de usuário de domínio, os grupos KLAdmins e KLOperators são criados no Servidor de Administração e no domínio que inclui o Servidor de Administração. Recomendamos uma abordagem semelhante, como a instalação de conta local.

Restrição da associação da função de administrador principal

Recomendamos restringir a participação na função de administrador principal.

Por padrão, após a instalação do Servidor de Administração, a função de administrador principal é atribuída ao grupo de administradores locais e ao grupo KLAdmins criado. É útil para o gerenciamento, mas é crítico sob o ponto de vista da segurança, pois a função de administrador principal tem um leque alargado de privilégios, portanto, a atribuição desta função aos usuários deve ser rigorosamente regulamentada.

Os administradores locais podem ser excluídos da lista de usuários com privilégios de administrador do Kaspersky Security Center. A função administrador principal não pode ser removida do grupo KLAdmins. É possível incluir no grupo KLAdmins as contas que serão usadas para gerenciar o Servidor de Administração.

Caso a autenticação do domínio seja usada, recomendamos restringir os privilégios das contas de administrador no Kaspersky Security Center. Por padrão, essas contas têm a função de administrador principal. Além disso, um administrador de domínio pode incluir sua conta no grupo KLAdmins para obter a função de administrador principal. Para evitar isso, nas configurações de segurança do Kaspersky Security Center, é possível adicionar o grupo Domain Admins e definir regras de proibição para ele. Essas regras devem ter precedência sobre as que permitem.

Também é possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado.

Configuração de direitos de acesso aos recursos do aplicativo

Recomendamos usar a configuração flexível de direitos de acesso aos recursos do Kaspersky Security Center para cada usuário ou grupo de usuários.

O controle de acesso baseado em função permite a criação de funções de usuário padrão com um conjunto predefinido de direitos e atribuição dessas funções aos usuários dependendo do seu escopo de obrigações.

As principais vantagens do modelo de controle de acesso baseado em função:

- Facilidade de administração
- Hierarquia de função

- Abordagem de privilégio mínimo
- Segregação de deveres

É possível atribuir funções internas a determinados profissionais de acordo com suas posições ou criar funções completamente novas.

Ao configurar as funções, observe os privilégios associados com a alteração do estado de proteção do dispositivo do Servidor de Administração e com a instalação remota de software de terceiros:

- Gerenciamento de grupos de administração.
- Operações com o Servidor de Administração.
- Instalação remota.
- Alteração dos parâmetros para armazenamento de eventos e envio de notificações.

  Esse privilégio permite definir as notificações que executam um script ou um módulo executável no dispositivo do Servidor de Administração quando um evento ocorrer.

Conta separada para instalação remota de aplicativos

Além da diferenciação básica de direitos de acesso, recomendamos restringir a instalação remota de aplicativos para todas as contas (exceto para o administrador principal ou outra conta especializada).

Recomendamos o uso de uma conta separada para instalação remota de aplicativos. É possível atribuir um papel ou permissões para a conta separada.

Proteção do acesso privilegiado do Windows

Recomendamos levar em consideração as recomendações da Microsoft para fornecer segurança de acesso privilegiado. Para visualizar essas recomendações, acesse o artigo proteção de acesso privilegiado.

Um dos pontos-chave das recomendações é a implementação de estações de trabalho de acesso privilegiado (PAW).

Uso de uma conta de serviço gerenciado (MSA) ou um grupo de contas de serviço gerenciado (gMSA) para executar o serviço do Servidor de Administração

O Active Directory tem um tipo especial de contas para executar serviços com segurança, chamadas conta de serviço gerenciado de grupo (MSA/gMSA). O Kaspersky Security Center dá suporte a contas de serviço gerenciadas (MSA) e contas de serviço gerenciadas em grupo (gMSA). Se esses tipos de contas forem usados no seu domínio, é possível selecionar um deles como a conta para o serviço do Servidor de Administração.

Auditoria periódica de todos os usuários e suas ações

Recomendamos conduzir uma auditoria regular de todos os usuários no dispositivo do Servidor de Administração. Isso permite responder a certos tipos de ameaças de segurança associadas ao possível comprometimento do dispositivo.

Também é possível rastrear as ações dos usuários, como conectar-se e desconectar-se do Servidor de Administração, conectar-se ao Servidor de Administração com um erro e modificação de objetos (para objetos compatíveis com o gerenciamento de revisões).

Gerenciamento da proteção do Servidor de Administração

Seleção de um software de proteção do Servidor de Administração

Dependendo do tipo de implementação do Servidor de Administração e da estratégia de proteção geral, selecione o aplicativo para proteger o dispositivo do Servidor de Administração.

Caso o Servidor de Administração seja implantado em um dispositivo dedicado, recomendamos selecionar o aplicativo Kaspersky Endpoint Security para proteger o dispositivo do Servidor de Administração. Isso permite aplicar todas as tecnologias disponíveis para proteger o dispositivo do Servidor de Administração, inclusive os módulos de análise comportamental.

Caso o Servidor de Administração esteja instalado em um dispositivo existente na infraestrutura e que tenha sido usado anteriormente para outras tarefas, recomendamos considerar o seguinte software de proteção:

- Kaspersky Industrial CyberSecurity for Nodes. Recomendamos instalar esse aplicativo em dispositivos incluídos em uma rede industrial. Kaspersky Industrial CyberSecurity for Nodes é um aplicativo que possui certificados de compatibilidade com diversos fabricantes de softwares industriais.

- Soluções de segurança recomendadas. Caso o Servidor de Administração esteja instalado em um dispositivo com outro software, recomendamos levar em consideração as recomendações desse fornecedor de software sobre a compatibilidade de soluções de segurança (é possível que já haja recomendações para selecionar uma solução de segurança e talvez seja necessário configurar a zona confiável).

Criação de uma política de segurança separada para o aplicativo de proteção

Recomendamos criar uma política de segurança separada para o aplicativo de proteção do dispositivo do Servidor de Administração. Essa política deve ser diferente da política de segurança para dispositivos clientes. Isso permite especificar as configurações de segurança mais apropriadas para o Servidor de Administração, sem afetar o nível de proteção de outros dispositivos.

Recomendamos dividir os dispositivos em grupos e, em seguida, colocar o dispositivo do Servidor de Administração em um grupo separado para o qual será possível criar uma política de segurança especial.

Módulos de proteção

Caso não haja recomendações especiais do fornecedor do software de terceiros instalado no mesmo dispositivo do Servidor de Administração, recomendamos ativar e configurar todos os módulos de proteção disponíveis (depois de verificar a operação desses módulos de proteção por um determinado período).

Configuração do firewall do dispositivo do Servidor de Administração

No dispositivo do Servidor de Administração, recomendamos configurar o firewall para restringir o número de dispositivos a partir dos quais os administradores poderão se conectar ao Servidor de Administração pelo Console de Administração ou Kaspersky Security Center Web Console.

Por padrão, o Servidor de Administração usa a porta 13291 para receber conexões do Console de Administração e a porta 13299 para receber conexões do Kaspersky Security Center Web Console. Recomendamos restringir o número de dispositivos a partir dos quais o Servidor de Administração pode ser gerenciado com o uso dessas portas.

Gerenciamento de proteção dos dispositivos cliente

Restrição de adição de chaves de licença a pacotes de instalação

Os pacotes de instalação são armazenados na pasta compartilhada do Servidor de Administração, na subpasta Pacotes. Caso uma chave de licença seja adicionada a um pacote de instalação, ela pode ser comprometida, pois os direitos de acesso de leitura compartilhados estão ativados no repositório de pacotes de instalação.

Para evitar o comprometimento da chave de licença, não recomendamos adicionar as chaves de licença nos pacotes de instalação.

Recomendamos usar a distribuição automática de chaves de licença para dispositivos gerenciados, a implementação pela tarefa adicionar chave de licença para um aplicativo gerenciado e a adição manual de um código de ativação ou arquivo de chave nos dispositivos.

Regras automáticas para migrar os dispositivos entre os grupos de administração

Recomendamos restringir o uso de regras automáticas para dispositivos móveis entre os grupos de administração.

Caso as regras automáticas para mover dispositivos sejam usadas, isso poderá provocar a propagação de políticas que fornecem mais privilégios ao dispositivo movido antes do que ele tinha no momento da realocação.

Além disso, mover um dispositivo cliente para outro grupo de administração pode causar a propagação das configurações da política. Essas configurações da política podem ser indesejáveis para distribuição entre os dispositivos convidados e não confiáveis.

Essa recomendação não se aplica à alocação inicial única de dispositivos para grupos de administração.

Requisitos de segurança para pontos de distribuição e gateways de conexão

Os dispositivos com o Agente de Rede instalado podem atuar como um ponto de distribuição e executar as seguintes funções:

- Distribuir atualizações e pacotes de instalação recebidos do Servidor de Administração para dispositivos clientes dentro do grupo.
- Executar a instalação remota de software de terceiros e aplicativos Kaspersky em dispositivos cliente.
- Faça a sondagem da rede para detectar novos dispositivos e para atualizar as informações sobre os existentes. O ponto de distribuição pode usar os mesmos métodos de detecção de dispositivos do Servidor de Administração.

Colocação de pontos de distribuição na rede da organização usados para:

- Reduzir a carga no Servidor de Administração
- Otimizar o tráfego
- Fornecer ao Servidor de Administração o acesso aos dispositivos em partes de difícil acesso de uma rede

Tendo em vista as capacidades disponíveis, recomendamos proteger os dispositivos que funcionam como pontos de distribuição de qualquer tipo de acesso não autorizado (inclusive acesso físico).

Restrição da atribuição automática dos pontos de distribuição

Para simplificar a administração e manter a operacionalidade da rede, recomendamos o uso de atribuição automática de pontos de distribuição. Entretanto, para redes industriais e pequenas redes, recomendamos evitar a atribuição de pontos de distribuição automaticamente, pois, por exemplo, as informações privadas das contas usadas para enviar as tarefas de instalação remota podem ser transferidas para os pontos de distribuição pelo sistema operacional.

Para redes industriais e pequenas redes, é possível atribuir os dispositivos manualmente para atuar como pontos de distribuição.

Também é possível visualizar o Relatório de atividades de pontos de distribuição.

Requisitos de segurança para dispositivos de usuários do Kaspersky Security Center

Requisitos especiais de segurança devem ser aplicados aos dispositivos dos usuários do Kaspersky Security Center. Recomendamos proteger esses dispositivos contra qualquer tipo de acesso não autorizado (inclusive físico):

Os dispositivos de usuários do Kaspersky Security Center incluem:

- Dispositivos com os quais os usuários se conectam ao Kaspersky Security Center Web Console suando um navegador.
- Dispositivos com os quais os usuários se conectam ao Kaspersky Security Center usando o Console de Administração baseado em MMC.
- Dispositivos com os quais os aplicativos que interagem com o Servidor de Administração via OpenAPI se conectam ao Kaspersky Security Center.

Requisitos de segurança para dispositivos com o Kaspersky Security Center Web Console instalado

Dispositivos com o Kaspersky Security Center Web Console instalado são usados para gerenciar o Kaspersky Security Center. Por isso, exigem requisitos especiais de segurança. Recomendamos proteger esses dispositivos contra qualquer tipo de acesso não autorizado (inclusive físico).

Configuração da proteção para aplicativos gerenciados

Políticas de aplicativos gerenciados

Recomendamos a criação de uma política para cada tipo de aplicativo e componente usado do Kaspersky Security Center (Agente de Rede, Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Agent e outros). Esta política deve ser aplicada em todos os dispositivos gerenciados (o grupo de administração root) ou em um grupo separado para o qual novos dispositivos gerenciados são movidos automaticamente de acordo com as regras de movimentação configuradas.

Especificação da senha para desativar a proteção e desinstalar o aplicativo

Para evitar que invasores desativem os aplicativos de segurança Kaspersky, recomendamos vivamente ativar a proteção por senha para ativar a proteção e não permitir a desinstalação dos aplicativos de segurança Kaspersky. É possível definir a senha, por exemplo, para o Kaspersky Endpoint Security for Windows, Kaspersky Security for Windows Server, Agente de rede e outros aplicativos Kaspersky. Depois de ativar a proteção por senha, recomendamos bloquear essas configurações com o fechamento do "cadeado".

Especificação da senha para a conexão manual de um dispositivo cliente ao Servidor de Administração (utilitário klmover)

O utilitário klmover permite conectar manualmente um dispositivo cliente ao Servidor de Administração. Ao instalar o Agente de Rede em um dispositivo cliente, o utilitário é copiado automaticamente para a pasta de instalação do Agente de Rede.

Para impedir que intrusos movam dispositivos para fora do controle do Servidor de Administração, é altamente recomendável ativar a proteção por senha para executar o utilitário klmover. Para ativar a proteção por senha, selecione a opção **Usar senha de desinstalação** nas configurações da política do Agente de Rede.

O utilitário klmover requer direitos de administrador local. A proteção por senha para executar o utilitário klmover pode ser omitida para dispositivos operados sem direitos de administrador local.

Ativar a opção **Usar senha de desinstalação** também ativa a proteção por senha para a ferramenta Cleaner (cleaner.exe).

Usar a Kaspersky Security Network

Em todas as políticas de aplicativos gerenciados e nas propriedades do Servidor de Administração, recomendamos ativar o uso da Kaspersky Security Network (KSN) e aceitar a Declaração da KSN. Durante a atualização ou o upgrade do Servidor de Administração, é possível aceitar a Declaração da KSN atualizada. Em alguns casos, quando o uso de serviços em nuvem for proibido por lei ou por outros regulamentos, é possível desativar a KSN.

Verificação regular de dispositivos gerenciados

Para todos os grupos de dispositivos, recomendamos criar uma tarefa que execute periodicamente uma verificação completa dos dispositivos.

Descoberta de novos dispositivos

Recomendamos definir corretamente as configurações de descoberta de dispositivos: configure a integração com o Active Directory e especifique os intervalos de endereços IP para descobrir novos dispositivos.

De acordo com os propósitos de segurança, é possível usar o grupo de administração padrão que inclui todos os novos dispositivos e as políticas padrão que afetam esse grupo.

Seleção de uma pasta compartilhada

Caso o Servidor de Administração seja implementado no dispositivo executando o Windows com a seleção de uma pasta compartilhada existente (que é usada, por exemplo, para colocar pacotes de instalação e armazenamento de bancos de dados atualizados), recomendamos garantir que os direitos de leitura sejam concedidos ao grupo Todos e os direitos de gravação sejam concedidos para o grupo KLAdmins.

Manutenção do Servidor de Administração

Cópia de backup de dados do Servidor de Administração

Backup de dados permite restaurar os dados do Servidor de Administração sem perda de dados.

Por padrão, uma tarefa de backup de dados é criada automaticamente após a instalação do Servidor de Administração e é executada periodicamente ao salvar os backups no diretório apropriado.
As configurações da tarefa de backup de dados podem ser alteradas da seguinte forma:

- A frequência de backup aumenta
- Um diretório especial para salvar cópias é especificado
- As senhas para cópias de backup são alteradas

Caso as cópias de backup sejam armazenadas em um diretório especial, diferentemente do diretório padrão, recomendamos limitar a lista de controle de acesso (ACL) para esse diretório. As contas do Servidor de Administração e as contas do banco de dados do Servidor de Administração devem ter acesso de gravação para esse diretório.

Manutenção do Servidor de Administração

A manutenção do Servidor de Administração permite reduzir o volume do banco de dados e aprimorar o desempenho e a confiabilidade da operação do aplicativo. Recomendamos efetuar a manutenção do Servidor de Administração ao menos uma vez por semana.

A manutenção do Servidor de Administração é executada usando uma tarefa dedicada. O aplicativo executa as seguintes ações ao efetuar a manutenção do Servidor de Administração:

- Verifica o banco de dados quanto a erros
- Reorganiza os índices do banco de dados

- Atualiza as estatísticas do banco de dados
- Compacta o banco de dados (caso seja necessário)

Instalação de atualizações do sistema operacional e atualizações de software de terceiros

Recomendamos com ênfase a instalação regular das atualizações de software do sistema operacional e dos softwares de terceiros no dispositivo do Servidor de Administração.

Os dispositivos cliente não requerem uma conexão contínua com o Servidor de Administração, portanto, é seguro reinicializar o dispositivo do Servidor de Administração após a instalação das atualizações. Todos os eventos registrados nos dispositivos clientes durante o tempo de inatividade do Servidor de Administração são enviados para ele após a conexão ser restaurada.

Transferência de eventos para sistemas de terceiros

Monitoramento e relatórios

Para uma resposta oportuna a incidentes de segurança, recomendamos configurar os recursos de monitoramento e relatórios.

Exportação de eventos para os sistemas SIEM

Para a detecção rápida de incidentes antes que ocorram danos significativos, recomendamos o uso da exportação de eventos em um sistema SIEM.

Notificações por e-mail de eventos de auditoria

O Kaspersky Security Center lhe permite receber informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nestes dispositivos gerenciados. Para uma pronta resposta a emergências, recomendamos configurar o Servidor de Administração para o envio de notificações sobre os eventos de auditoria, eventos críticos, eventos de falha e advertência que ele publica.

Como esses eventos são eventos intrassistema, pode haver um pequeno número deles, o que é bastante pertinente para a correspondência.

Preparação para implementação

Esta seção descreve as etapas que você deve seguir antes de implementar o Kaspersky Security Center.

Planejar a implementação do Kaspersky Security Center

Esta seção fornece informações sobre as opções mais convenientes para a implementação de componentes do Kaspersky Security Center em uma rede da organização dependendo dos seguintes critérios:

- Número total de dispositivos
- As unidades (escritórios locais, filiais) que são separadas de forma organizacional ou geográfica
- Separar as redes conectadas por canais estreitos
- Necessário fornecer acesso à Internet ao Servidor de Administração

Esquemas típicos para implementação do sistema de proteção

Esta seção descreve os esquemas padrão de implementação de um sistema de proteção em uma rede corporativa usando o Kaspersky Security Center.

O sistema deve ser protegido contra qualquer tipo de acesso não autorizado. Recomendamos que você instale todas as atualizações de segurança disponíveis para o sistema operacional antes de instalar o aplicativo em seu dispositivo e de proteger fisicamente o(s) Servidor(es) de Administração e o(s) ponto(s) de distribuição.

Você pode usar o Kaspersky Security Center para implementar um sistema de proteção em uma rede corporativa por meio dos seguintes esquemas de implementação:

- Implemente um sistema de proteção através do Kaspersky Security Center, usando uma das seguintes formas:
  - Através do Console de Administração
  - Através do Kaspersky Security Center Web Console

  Os aplicativos Kaspersky são automaticamente instalados em dispositivos cliente, os quais, por sua vez, são automaticamente conectados ao Servidor de Administração usando o Kaspersky Security Center.

  O esquema de implementação básico é a implementação de um sistema de proteção através do Console de Administração. Usar o Kaspersky Security Center Web Console permite iniciar a instalação de aplicativos Kaspersky a partir de um navegador.
- Implemente um sistema de proteção manualmente usando os pacotes de instalação independentes gerados pelo Kaspersky Security Center.

  A instalação de aplicativos Kaspersky em dispositivos cliente e na estação de trabalho do administrador é executada manualmente; as configurações para a conexão dos dispositivos cliente ao Servidor de Administração são especificadas durante a instalação do Agente de Rede.

  Este método de implementação é recomendado nos casos quando a instalação remota não for possível.

O Kaspersky Security Center também permite implementar seu sistema de proteção usando as políticas de grupo do Microsoft Active Directory®.

Sobre o planejamento da implementação do Kaspersky Security Center em uma rede da organização

Um Servidor de Administração pode suportar um máximo de 100.000 dispositivos. Se o número total de dispositivos na rede de uma organização exceder 100.000, múltiplos Servidores de Administração devem ser implementados na rede e combinados em uma hierarquia para o gerenciamento centralizado conveniente.

Se uma organização incluir escritórios locais remotos de larga escala (filiais) com os seus próprios administradores, é útil implementar Servidores de Administração naqueles escritórios. De outra forma, aqueles escritórios devem ser exibidos como redes desanexadas conectadas por canais de baixa produtividade, consulte a seção "Configuração padrão: alguns escritórios de larga escala dirigidos pelos seus próprios administradores".

Ao usar redes desanexadas conectadas com canais estreitos, o tráfego pode ser poupado ao atribuir um ou diversos Agentes de Rede para atuar como pontos de distribuição (consulte tabela para o cálculo do número de pontos de distribuição). Nesse caso, todos os dispositivos em uma rede desanexada recuperam as atualizações desses centros de atualização locais. Os pontos de distribuição reais podem baixar as atualizações do Servidor de Administração (cenário padrão) e de servidores da Kaspersky na Internet (consulte a seção "Configuração padrão: múltiplos pequenos escritórios remotos").

A seção "Configurações padrão do Kaspersky Security Center" fornece descrições detalhadas das configurações padrão do Kaspersky Security Center. Ao planejar a implementação, selecione a configuração padrão mais adequada, dependendo da estrutura da organização.

Na etapa do planejamento da implementação, a atribuição do certificado especial X.509 ao Servidor de Administração deve considerada. A atribuição do certificado X.509 ao Servidor de Administração pode ser útil nos seguintes casos (lista parcial):

- Inspecionar tráfego da camada do soquete seguro (SSL) por meio de um proxy de terminação SSL ou para usar um proxy reverso
- Integração com a infraestrutura de chaves públicas (PKI) de uma organização
- Especificação dos valores necessários nos campos do certificado
- Fornecer a força de criptografia necessária de um certificado

Selecionar uma estrutura para a proteção de uma empresa

A seleção de uma estrutura para a proteção de uma organização é definida pelos seguintes fatores:

- Topologia de rede da organização.
- Estrutura organizacional.
- Número de funcionários responsáveis pela proteção da rede e alocação de suas responsabilidades.
- Recursos de hardware que podem ser alocados para os componentes de gerenciamento da proteção.

- A produtividade dos canais de comunicação que pode ser alocada para manter a operação dos componentes de proteção na rede da organização.

- Limites de tempo para execução de operações administrativas críticas na rede da organização. As operações administrativas críticas incluem, por exemplo, a distribuição das atualizações para os bancos de dados antivírus e a modificação de políticas para dispositivos cliente.

Ao selecionar uma estrutura de proteção, recomenda-se inicialmente estimar a rede existente e os recursos de hardware disponíveis que podem ser usados para a operação de um sistema de proteção centralizado.

Para analisar a rede e infraestrutura de hardware, recomenda-se que você siga o processo abaixo:

1. Definir as configurações seguintes da rede na qual a proteção será implementada:

   - Número de segmentos de rede.

   - A velocidade dos canais de comunicação entre os segmentos de rede individuais.

   - Número de dispositivos gerenciados em cada um dos segmentos da rede.

   - Informação de cada canal de comunicação que pode ser alocada para manter a operação da proteção.

2. Determinar o tempo máximo permitido para a execução das principais operações administrativas para todos os dispositivos gerenciados.

3. Analisar as informações das etapas 1 e 2, assim como os dados do teste de carga do sistema de administração. Com base na análise, responda às seguintes perguntas:

   - É possível servir todos os clientes com um único Servidor de Administração ou é necessário uma hierarquia de Servidores de Administração?

   - Qual a configuração de hardware dos Servidores de Administração que é necessária para processar todos os clientes dentro dos limites de tempo especificados no etapa 2?

   - É necessário usar pontos de distribuição para reduzir a carga nos canais de comunicação?

Após obter as respostas para a etapa 3 acima, você pode compilar um conjunto de estruturas permitidas de proteção da organização.

Na rede da organização, você pode usar uma das seguintes estruturas de proteção padrão:

- Um Servidor de Administração. Todos os dispositivos cliente são conectados a um único Servidor de Administração. O Servidor de Administração funciona como um ponto de distribuição.

- Um Servidor de Administração com pontos de distribuição. Todos os dispositivos cliente são conectados a um único Servidor de Administração. Alguns dos dispositivos cliente na rede agem como pontos de distribuição.

- Hierarquia de Servidores de Administração. Para cada um dos segmentos de rede um Servidor de Administração individual é alocado e se torna parte de uma hierarquia geral de Servidores de Administração. O Servidor de Administração principal funciona como o ponto de distribuição.

- Hierarquia de Servidores de Administração com pontos de distribuição. Para cada um dos segmentos de rede um Servidor de Administração individual é alocado e se torna parte de uma hierarquia geral de Servidores de Administração. Alguns dos dispositivos cliente na rede agem como pontos de distribuição.

Configurações padrão do Kaspersky Security Center

Esta seção descreve as seguintes configurações padrão usadas para a implementação de componentes do Kaspersky Security Center em uma rede de organização:

- Escritório único
- Alguns escritórios de larga escala que são geograficamente separados e executam por si seus próprios administradores
- Múltiplos pequenos escritórios que são geograficamente separados

Configuração padrão: escritório único

Um ou diversos Servidores de Administração podem ser implementados na rede da organização. O número de Servidores de Administração pode ser selecionado com base no hardware disponível ou no número total de dispositivos gerenciados.

Um Servidor de Administração pode suportar até 100.000 dispositivos. Você deve considerar a possibilidade de aumentar o número de dispositivos gerenciados no futuro próximo: pode ser útil conectar um número ligeiramente menor de dispositivos a um único Servidor de Administração.

Os Servidores de Administração podem ser implementados na rede interna, ou na DMZ, dependendo de se o acesso à Internet aos Servidores de Administração é necessário.

Se múltiplos servidores forem usados, recomenda-se que você os combine em uma hierarquia. Usar uma hierarquia de Servidor de Administração permite evitar políticas e tarefas duplicadas, tratar todo o conjunto de dispositivos gerenciados como se eles fossem gerenciados por um único Servidor de Administração (ou seja, procura por dispositivos, criação de seleções de dispositivos e criação de relatórios).

Configuração padrão: Alguns escritórios de larga escala executam por si seus próprios administradores

Se uma organização tiver escritórios geograficamente separados em ampla escala, considere a opção de implantar Servidores de Administração em cada um dos escritórios. Um ou vários Servidores de Administração podem ser implementados por escritório, dependendo do número de dispositivos e hardware do cliente disponíveis. Neste caso, cada um dos escritórios pode ser visto como uma "Configuração padrão: Escritório único". Para facilitar a administração, é recomendável combinar todos os Servidores de Administração em uma hierarquia (possivelmente em vários níveis).

Caso alguns funcionários façam movimentações entre os escritórios com seus dispositivos (portáteis), crie perfis de conexão do Agente de Rede na política do Agente de Rede. Os perfis de conexão do Agente de Rede são compatíveis apenas com os dispositivos Windows e macOS.

Configuração padrão: múltiplos pequenos escritórios remotos

Esta configuração padrão fornece meios para um escritório de sede e muitos pequenos escritórios remotos que podem se comunicar com o escritório via Internet. Cada um destes escritórios remotos pode estar localizados por trás da Network Address Translation (NAT), assim, nenhuma conexão pode ser estabelecida entre dois escritórios remotos, pois eles estão isolados.

Um Servidor de Administração deve ser implementado no escritório sede e um ou múltiplos pontos de distribuição devem ser atribuídos a todos os outros escritórios. Caso os escritórios estejam ligados pela Internet, pode ser útil criar uma tarefa *baixar atualizações para os repositórios de pontos de distribuição* aos pontos de distribuição para que baixem as atualizações diretamente dos servidores Kaspersky, pasta de rede ou local, e não pelo Servidor de Administração.

Se alguns dispositivos em um escritório remoto não tiverem acesso direto ao Servidor de Administração (por exemplo, o acesso ao Servidor de Administração é fornecido por meio da Internet, mas alguns dispositivos não têm acesso à Internet), os pontos de distribuição devem ser alternados para o modo de gateway de conexão. Neste caso, os Agentes de Rede em dispositivos no escritório remoto serão conectados, para a sincronização adicional, ao Servidor de Administração – mas através do gateway, não diretamente.

Como o Servidor de Administração, muito provavelmente, não conseguirá sondar a rede do escritório remoto, pode ser útil transferir esta função para um ponto de distribuição.

O Servidor de Administração não será capaz de enviar notificações para a porta 15000 UDP em dispositivos gerenciados localizados além da NAT no escritório remoto. Para solucionar este problema, você pode ativar o modo da conexão contínua para o Servidor de Administração nas propriedades dos dispositivos que atuam como pontos de distribuição (caixa de seleção **Não desconectar do Servidor de Administração**). Este modo está disponível se o número total de pontos de distribuição não exceder 300. É possível usar servidores push para garantir que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração. Consulte o seguinte tópico para obter detalhes: Usando um ponto de distribuição como servidor push.

Selecionar um DBMS

Ao selecionar um sistema de gerenciamento de banco de dados (DBMS) a ser usado por um Servidor de Administração, você deve levar em conta o número de dispositivos cobertos por um Servidor de Administração.

A tabela a seguir lista as opções válidas de DBMS, assim como as recomendações e restrições quanto ao seu uso.

Recomendações e restrições no DBMS

DBMS	Recomendações e restrições
SQL Server Express Edition 2012 ou posterior	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 10.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Você pode limitar o número máximo de eventos no repositório de eventos para evitar a sobrecarga do banco de dados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados. O uso simultâneo do SQL Server Express Edition DBMS pelo Servidor de Administração e outro aplicativo é estritamente proibido. O banco de dados Microsoft SQL Express não é compatível com a tarefa **Executar a sincronização com o Windows Update**.
Edição local do SQL Server, que não seja a Express, 2014 ou posterior	Nenhuma limitação.
Edição remota do SQL Server, que não seja a Express, 2014 ou posterior	Válido somente se ambos os dispositivos estiverem no mesmo domínio do Windows®; se os domínios forem diferentes, uma relação de confiança bidirecional deve ser estabelecida entre eles.
MySQL 5.5, 5.6 ou 5.7 local ou remoto (as versões 5.5.1, 5.5.2, 5.5.3, 5.5.4 e 5.5.5 do MySQL não têm mais suporte)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 10.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.
MySQL 8.0.20 remoto ou local, e versões posteriores	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.

DBMS	Recomendações e restrições
MariaDB local ou remoto (visualizar as versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 20.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.
PostgreSQL, Postgres Pro (ver versões compatíveis)	Use um desses DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.

Caso um DBMS PostgreSQL, MariaDB ou MySQL seja usado, a guia **Eventos** poderá exibir uma lista incompleta de eventos para o dispositivo cliente selecionado. Isso ocorre quando o DBMS armazena uma quantidade muito grande de eventos. É possível aumentar o número de eventos exibidos com a execução de um dos seguintes procedimentos:

- Remoção de eventos desnecessários.
- Redução do prazo de armazenamento para eventos desnecessários.

Para ver uma lista completa de eventos registrados no Servidor de Administração para o dispositivo, use Relatórios.

Se estiver usando o SQL Server 2019 como um DBMS e não tiver o patch cumulativo CU12 ou posterior, será necessário fazer o seguinte após instalar o Kaspersky Security Center:

1. Conecte-se ao SQL Server usando o SQL Management Studio.
2. Execute os seguintes comandos (se escolher um nome diferente para o banco de dados, use esse nome em vez do KAV):

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. Reinicie o serviço SQL Server 2019.

Caso contrário, usando Servidor SQL 2019 pode resultar em erros com "Há memória de sistema suficientes no pool de recursos 'internos' para executar esta consulta."

Configurando o servidor MariaDB x64 para trabalhar com o Kaspersky Security Center 14.2

Para configurar com sucesso o servidor MariaDB x64 para trabalhar com o Kaspersky Security Center, você deve usar os parâmetros de servidor padrão, com exceção dos parâmetros de servidor especificados neste artigo.

O Kaspersky Security Center 14.2 é compatível com o DBMS MariaDB. Para obter mais informações sobre as versões compatíveis com MariaDB, consulte a seção Requisitos de hardware e software.

Se você usar o DBMS MariaDB para o Kaspersky Security Center, ative a compatibilidade para armazenamento InnoDB e MEMORY e as codificações UTF-8 e UCS-2.

Configurações recomendadas para o arquivo my.ini

Para configurar o arquivo my.ini:

1. Abra o arquivo my.ini em um editor de texto.

2. Adicione as seguintes linhas na seção `[mysqld]` do arquivo 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=<o valor real não deve ser menor que 80% do tamanho do banco de dados KAV esperado>
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"
```

O valor de `innodb_buffer_pool_size` não deve ser inferior a 80% do tamanho esperado do banco de dados KAV. Observe que a memória especificada será alocada na inicialização do servidor. Caso o tamanho do banco de dados seja menor que o tamanho do buffer especificado, somente a memória necessária será alocada. Caso o MariaDB 10.4.3 ou anterior seja usado, o tamanho real da memória alocada será aproximadamente 10% maior que o tamanho do buffer especificado.

Recomenda-se usar o valor do parâmetro `innodb_flush_log_at_trx_commit=0`, pois os valores "1" ou "2" afetam negativamente a velocidade de operação do MariaDB. Certifique-se de que o parâmetro `innodb_file_per_table` está definido como `1`.

Para o MariaDB 10.1, insira adicionalmente as seguintes linhas na seção [mysqld]:

```
innodb_file_format='Barracuda'
innodb_default_row_format=dynamic
innodb_large_prefix=1
```

Para o MariaDB 10.6, insira adicionalmente as seguintes linhas na seção [mysqld]:

```
optimizer_prune_level=0
optimizer_search_depth=8
```

Por padrão, os complementos do otimizador `join_cache_incremental`, `join_cache_hashed` e `join_cache_bka` estão ativados. Se esses complementos não estiverem ativados, você deve ativá-los.

Para verificar se os complementos do otimizador estão ativados:

1. No console do cliente MariaDB, execute o comando:

   ```
   SELECT @@optimizer_switch;
   ```

2. Verifique se sua saída contém as seguintes linhas:

   ```
   join_cache_incremental=on
   join_cache_hashed=on
   join_cache_bka=on
   ```

   Se essas linhas estiverem presentes e com os valores de `on`, os complementos do otimizador serão ativados.

   Caso estas linhas estejam ausentes ou estejam com o valor `off`, é preciso fazer o seguinte:

   1. Abra o arquivo my.ini em um editor de texto.

   2. Adicione as seguintes linhas na seção `[mysqld]` do arquivo my.ini:

      ```
      optimizer_switch='join_cache_incremental=on'
      optimizer_switch='join_cache_hashed=on'
      optimizer_switch='join_cache_bka=on'
      ```

Os complementos `join_cache_incremental`, `join_cache_hash`, e `join_cache_bka` estão ativados.

Configurando o servidor MySQL x64 para trabalhar com o Kaspersky Security Center 14.2

Para configurar corretamente o servidor MySQL x64 para uso com o Kaspersky Security Center, é preciso utilizar os parâmetros de servidor padrão, exceto os aqueles especificados neste artigo.

Se você usar o MySQL DBMS para o Kaspersky Security Center, ative a compatibilidade para armazenamento InnoDB e MEMORY e as codificações UTF-8 e UCS-2.

Configurações recomendadas para o arquivo my.ini

Para configurar o arquivo my.ini:

1. Abra o arquivo my.ini em um editor de texto.

2. Adicione as seguintes linhas na seção `[mysqld]` do arquivo 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=<o valor real não deve ser menor que 80% do tamanho do banco de dados KAV esperado>
innodb_thread_concurrency=20
innodb_flush_log_at_trx_commit=0 (na maioria dos casos, o servidor usa pequenas transações)
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
```

   Observe que a memória especificada no valor `innodb_buffer_pool_size` é alocado na inicialização do servidor. Caso o tamanho do banco de dados seja menor que o tamanho do buffer especificado, somente a memória necessária será alocada. O tamanho real da memória alocada é aproximadamente 10% maior que o tamanho do buffer especificado. Consulte a documentação do MySQL para obter detalhes.

   Recomenda-se usar o valor do parâmetro `innodb_flush_log_at_trx_commit = 0`, pois os valores "1" ou "2" afetam negativamente a velocidade de operação do MySQL. Certifique-se de que o parâmetro `innodb_file_per_table` está definido como `1`.

Configurar o servidor PostgreSQL ou Postgres Pro para trabalhar com o Kaspersky Security Center 14.2

Para configurar corretamente o servidor PostgreSQL ou Postgres Pro para uso com o Kaspersky Security Center, é preciso utilizar os parâmetros de servidor padrão, exceto os aqueles especificados neste artigo.

Kaspersky Security Center 14.2 compatível com PostgreSQL e Postgres Pro DBMSs. Se você usar um desses DBMSs, considere configurar os parâmetros do servidor DBMS para otimizar o trabalho do DBMS com o Kaspersky Security Center.

O caminho padrão para o arquivo de configuração é: `C:\Program Files\PostgreSQL\<VERSÃO>\data\postgresql.conf`

Parâmetros recomendados para PostgreSQL e Postgres Pro:

- `shared_buffers` = 25% do valor da RAM do dispositivo onde o DBMS está instalado

  Se a RAM for inferior a 1 GB, deixe o valor padrão.

- `max_stack_depth = 2MB`

- `temp_buffers = 24MB`
- `work_mem = 16MB`
- `max_connections = 151`
- `max_parallel_workers_per_gather = 0`
- `maintenance_work_mem = 128MB`

Certifique-se de que o parâmetro `standard_conforming_strings` está definido para o valor padrão `on`. Recarregue a configuração ou reinicie o servidor após atualizar o arquivo postgresql.conf. Consulte a documentação do PostgreSQL para obter detalhes.

Para obter informações detalhadas sobre os parâmetros do servidor PostgreSQL e Postgres Pro, além dos detalhes sobre como especificá-los, consulte a documentação do DBMS correspondente.

Consulte o tópico a seguir para obter detalhes quanto à criação e configuração de contas para PostgreSQL e Postgres Pro: Configuração de contas para trabalhar com PostgreSQL e Postgres Pro.

Gerenciar dispositivos móveis com o Kaspersky Endpoint Security for Android

Os dispositivos móveis com o Kaspersky Endpoint Security for Android™ instalado (aqui referidos como dispositivos KES) são gerenciados por meio do Servidor de Administração. O Kaspersky Security Center oferece suporte aos seguintes recursos para gerenciar dispositivos do KES:

- Tratar dispositivos móveis como dispositivos cliente:
  - Associação em grupos de administração
  - Monitoramento, como visualização de status, eventos e relatórios
  - Modificar as configurações locais e atribuir políticas para o Kaspersky Endpoint Security for Android
- Enviar comandos em modo centralizado
- Instalar pacotes de aplicativos móveis remotamente

O Servidor de Administração gerencia dispositivos KES por meio de TLS, pela porta TCP 13292.

Fornecer acesso à Internet ao Servidor de Administração

Os seguintes casos necessitam do acesso à Internet ao Servidor de Administração:

- Atualização regular dos bancos de dados, módulos de software e aplicativos Kaspersky
- Atualizando software de terceiros

  Por padrão, a conexão com a Internet não é necessária para que o Servidor de Administração instale atualizações de software da Microsoft nos dispositivos gerenciados. Por exemplo, os dispositivos gerenciados podem baixar as atualizações de software da Microsoft diretamente dos servidores de Atualizações da Microsoft ou do Windows Server com o Microsoft Windows Server Update Services (WSUS) implementado na rede da sua organização. O Servidor de Administração deve estar conectado à Internet nos seguintes casos:

  - Ao usar o Servidor de Administração como servidor WSUS
  - Para instalar atualizações de software de terceiros que não sejam da Microsoft
- Corrigindo vulnerabilidades de software de terceiros

  A conexão com a Internet é necessária para que o Servidor de Administração execute as seguintes tarefas:

  - Para fazer uma lista de correções recomendadas para vulnerabilidades em softwares da Microsoft. A lista é criada e atualizada regularmente por especialistas da Kaspersky.
  - Para corrigir vulnerabilidades em software de terceiros que não sejam software da Microsoft.
- Gerenciar dispositivos (computadores portáteis) de usuários fora do escritório
- Gerenciar dispositivos em escritórios remotos
- Interagir com Servidores de Administração principais ou secundários, sediados em escritórios remotos
- Gerenciar dispositivos móveis

Esta seção descreve formas típicas para fornecer o acesso ao Servidor de Administração por meio da Internet. Cada um dos casos com enfoque no fornecimento de acesso à Internet para o Servidor de Administração pode necessitar de um certificado dedicado do Servidor de Administração.

Acesso à Internet: Servidor de Administração em uma rede local

Se o Servidor de Administração estiver localizado na rede interna de uma empresa, convém tornar a porta 13000 TCP do Servidor de Administração acessível do exterior por meio do reencaminhamento de porta. Se o gerenciamento de dispositivos móveis for necessário, convém tornar a porta 13292 TCP acessível.

Acesso à Internet: Servidor de Administração em DMZ

Se o Servidor de Administração estiver localizado em DMZ da rede da organização, ele não terá acesso à rede interna da organização. Por isso, as seguintes limitações aplicam-se:

- O Servidor de Administração não pode detectar novos dispositivos.
- O Servidor de Administração não pode executar a implementação inicial do Agente de Rede através da instalação forçada em dispositivos na rede interna da organização.

Isto somente se aplica à instalação inicial do Agente de Rede. Quaisquer atualizações adicionais do Agente de Rede ou da instalação do aplicativo de segurança pode, no entanto, ser executada pelo Servidor de Administração. Ao mesmo tempo, a implementação inicial dos Agentes de Rede pode ser executada por outros meios, por exemplo, através das políticas de grupo do Microsoft® Active Directory®.

- O Servidor de Administração não pode enviar notificações aos dispositivos gerenciados através da porta 15000 UDP, o que não é crítico para o funcionamento do Kaspersky Security Center.

- O Servidor de Administração não pode amostrar o Active Directory. No entanto, os resultados da sondagem do Active Directory não é necessária na maioria dos cenários.

Se as limitações acima mencionadas forem vistas como críticas, elas podem ser removidas usando pontos de distribuição localizados na rede da organização:

- Para executar a implementação inicial em dispositivos sem Agente de Rede, você primeiro instala o Agente de Rede em um dos dispositivos e, a seguir, o atribui o status de ponto de distribuição. Como resultado, a instalação inicial do Agente de Rede em outros dispositivos será executada pelo Servidor de Administração através deste ponto de distribuição.

- Para detectar novos dispositivos na rede interna da organização e fazer a sondagem do Active Directory, é necessário ativar os métodos relevantes de descoberta de dispositivos em um dos pontos de distribuição.

Para assegurar o envio com êxito de notificações para a porta 15000 UDP em dispositivos gerenciados na rede interna da organização, você precisa cobrir toda a rede com pontos de distribuição. Nas propriedades dos pontos de distribuição que foram atribuídos, selecione a caixa de seleção **Não desconectar do Servidor de Administração**. Como resultado, o Servidor de Administração estabelecerá uma conexão contínua com os pontos de distribuição e eles serão capazes de enviar notificações para a porta 15000 UDP nos dispositivos na rede interna da organização (pode ser uma rede IPv4 ou IPv6).

Acesso à Internet: Agente de Rede como um gateway de conexão no DMZ

O Servidor de Administração pode ser localizado na rede interna da organização, e no DMZ da rede pode haver um dispositivo com o Agente de Rede em execução como gateway de conexão com a conectividade inversa (o Servidor de Administração estabelece uma conexão com o Agente de Rede). Neste caso, as seguintes condições devem ser atendidas para assegurar o acesso à Internet:

- O Agente de Rede deve ser instalado no dispositivo que estiver na DMZ. Quando você instala o Agente de Rede, na janela **Gateway de conexão** do Assistente de instalação, selecione **Usar o Agente de Rede como um gateway de conexão na DMZ**.

- O dispositivo com o gateway de conexão instalado deve ser adicionado como um ponto de distribuição. Ao adicionar o gateway de conexão na janela **Adicionar ponto de distribuição** selecione a opção **Selecionar → Adicionar gateway de conexão na DMZ por endereço**.

- Para usar uma conexão de Internet para conectar dispositivos de desktop externos ao Servidor de Administração é necessário corrigir o pacote de instalação do Agente de Rede. Nas propriedades do pacote de instalação criado, selecione a opção **Avançado → Conectar-se ao Servidor de Administração usando o gateway de conexão** e, em seguida, especifique o gateway de conexão recém-criado.

Para o gateway de conexão no DMZ, o Servidor de Administração cria um certificado assinado com o certificado do Servidor de Administração. Se o administrador decidir atribuir um certificado personalizado ao Servidor de Administração, isso deve ser feito antes que um gateway de conexão seja criado no DMZ.

Se alguns funcionários usarem computadores portáteis que possa se conectar ao Servidor de Administração a parir da rede local ou por meio da Internet, pode ser útil criar uma regra de alternância para o Agente de Rede na política do Agente de Rede.

Sobre os pontos de distribuição

Um dispositivo com o Agente de Rede instalado pode ser usado como um ponto de distribuição. Neste modo, o Agente de Rede pode executar as seguintes funções:

- Distribuir atualizações (estas podem ser recuperadas do Servidor de Administração ou dos servidores da Kaspersky). Nesse caso, a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* deve ser criada para o dispositivo que serve como o ponto de distribuição:
  - Instalar software (incluindo a implementação inicial dos Agentes de Rede) em outros dispositivos.
  - Faça a sondagem da rede para detectar novos dispositivos e para atualizar as informações sobre os existentes. Um ponto de distribuição pode aplicar os mesmos métodos de localização dos dispositivos que os do Servidor de Administração.

A implementação de pontos de distribuição em uma rede da organização tem os seguintes objetivos:

- Reduzir a carga no Servidor de Administração.
- Otimizar o tráfego.
- Fornecer ao Servidor de Administração o acesso aos dispositivos em pontos de difícil acesso de uma rede da organização. A disponibilidade de um ponto de distribuição na rede além da NAT (em relação ao Servidor de Administração) permite ao Servidor de Administração executar as seguintes ações:
  - Enviar notificações para dispositivos por UDP na rede IPv4 ou IPv6
  - Sondar a rede IPv4 ou IPv6
  - Executar a implementação inicial
  - Atuar como um servidor push

Um ponto de distribuição é atribuído para um grupo de administração. Neste caso, o escopo do ponto de distribuição inclui todos os dispositivos dentro do grupo de administração e todos dos seus subgrupos. No entanto, o dispositivo que atua como o ponto de distribuição não pode estar incluído no grupo de administração ao qual foi atribuído.

Você pode criar uma função de ponto de distribuição como um gateway de conexão. Neste caso, os dispositivos no escopo do ponto de distribuição serão conectados ao Servidor de Administração por meio do gateway, não diretamente. Este modo pode ser útil em cenários que não permitem o estabelecimento de uma conexão direta entre o Servidor de Administração e os dispositivos gerenciados.

Se você usar um dispositivo baseado em Linux como um ponto de distribuição, é altamente recomendável aumentar o limite de descritores de arquivo para o serviço klnagent, porque se o escopo do ponto de distribuição incluir muitos dispositivos, o número máximo padrão de arquivos que podem ser abertos pode não ser suficiente.

Aumento do limite de descritores de arquivo para o serviço klnagent

Caso o escopo de um ponto de distribuição baseado em Linux inclua muitos dispositivos, o limite padrão de arquivos que podem ser abertos (descritores de arquivo) pode não ser suficiente. Para evitar isso, é possível aumentar o limite de descritores de arquivo para o serviço klnagent.

Para aumentar o limite de descritores de arquivo para o serviço klnagent:

1. No dispositivo baseado em Linux que atua como um ponto de distribuição, abra o arquivo `/lib/systemd/system/klnagent64.service` e, em seguida, especifique os limites absolutos e flexíveis dos descritores de arquivo no parâmetro `LimitNOFILE` da seção `[Service]`:

   `LimitNOFILE=<limite flexível de recurso>:<limite rígido de recurso>`

   Por exemplo, `LimitNOFILE=32768:131072`. Observe que o limite flexível dos descritores de arquivo deve ser menor ou igual ao limite absoluto.

2. Execute o seguinte comando para garantir que os parâmetros sejam especificados corretamente:

   `systemd-analyze verify klnagent64.service`

   Caso os parâmetros sejam especificados incorretamente, esse comando poderá gerar um dos seguintes erros:

   - `/lib/systemd/system/klnagent64.service:11: Failed to parse resource value, ignoring: 32768:13107`

     Caso ocorra esse erro, os símbolos na linha `LimitNOFILE` foram especificados incorretamente. É necessário verificar e corrigir a linha inserida.

   - `/lib/systemd/system/klnagent64.service:11: Soft resource limit chosen higher than hard limit, ignoring: 32768:13107`

     Se esse erro ocorrer, o limite flexível dos descritores de arquivo inseridos será maior que o limite absoluto. É necessário verificar a linha inserida e garantir que o limite flexível dos descritores de arquivo seja menor ou igual ao limite absoluto.

3. Execute o seguinte comando para recarregar o processo do systemd:

   `systemctl daemon-reload`

4. Execute o seguinte comando para reiniciar o serviço do Agente de Rede:

   `systemctl restart klnagent`

5. Execute o seguinte comando para garantir que os parâmetros especificados sejam aplicados corretamente:

   `less /proc/<ID do processo nagent>/limits`

   em que o parâmetro `<ID do processo nagent>` é o identificador do processo do Agente de Rede. É possível executar o seguinte comando para obter o identificador:

   `ps -ax | grep klnagent`

Para o ponto de distribuição baseado em Linux, o limite de arquivos que podem ser abertos é aumentado.

Calcular o número e a configuração de pontos de distribuição

Quanto mais dispositivos clientes uma rede contiver, mais pontos de distribuição ela exigirá. Recomendamos que você não desative a atribuição automática de pontos de distribuição. Quando a atribuição automática de pontos de distribuição estiver ativada, o Servidor de Administração atribui pontos de distribuição se o número de dispositivos clientes for bastante grande e define a sua configuração.

Usar pontos de distribuição exclusivamente atribuídos

Se você planejar usar determinados dispositivos específicos como pontos de distribuição (ou seja, servidores exclusivamente atribuídos), você pode optar por não utilizar a atribuição automática de pontos de distribuição. Neste caso, assegure-se de que os dispositivos aos quais você pretende tornar pontos de distribuição tenham volume suficiente de espaço livre em disco, não sejam desligados regularmente e estejam com o modo Suspenso desativado.

Número de pontos de distribuição exclusivamente atribuídos em uma rede que contém um segmento de rede único, com base no número de dispositivos na rede

Número de dispositivos clientes no segmento da rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Número de pontos de distribuição exclusivamente atribuídos em uma rede que contém vários segmentos de rede, com base no número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10–100	1
Mais de 100	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Usar dispositivos clientes padrão (estações de trabalho) como pontos de distribuição

Se você planejar usar dispositivos clientes padrão (isto é, estações de trabalho) como pontos de distribuição, recomendamos atribuir pontos de distribuição, como mostrado nas tabelas abaixo, para evitar a carga excessiva dos canais de comunicação e do Servidor de Administração:

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém um segmento de rede único, com base no número de dispositivos na rede

Número de dispositivos clientes no segmento da rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém vários segmentos de rede, com base no número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10–30	1

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
31–300	2
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

Se um ponto de distribuição estiver desativado (ou não disponível por algum outro motivo), os dispositivos gerenciados no escopo poderão acessar o Servidor de Administração para as atualizações.

Hierarquia de Servidores de Administração

Um MSP pode executar múltiplos Servidores de Administração. Pode ser inconveniente administrar diversos Servidores de Administração separados, portanto uma hierarquia pode ser aplicada. Uma configuração de "principal / secundário" para dois Servidores de Administração fornece as seguintes opções:

- Um Servidor de Administração secundário herda as políticas e tarefas do Servidor de Administração principal, prevenindo assim a duplicação das configurações.
- As seleções de dispositivos no Servidor de Administração principal podem incluir dispositivos de Servidores de Administração secundários.
- Os Relatórios no Servidor de Administração principal podem conter dados (incluindo informações detalhadas) de Servidores de Administração secundários.

O Servidor de Administração principal somente recebe dados de Servidores de Administração secundários não virtuais dentro do escopo das opções listadas acima. Essa limitação não se aplica aos Servidores de Administração virtuais, que compartilham o banco de dados com seu Servidor de Administração principal.

Servidores de Administração virtual

Com base em um Servidor de Administração físico, múltiplos Servidores de Administração virtuais podem ser criados, que serão semelhantes a Servidores de Administração secundários. Em comparação com o modelo de acesso discricionário, que tem base em listas de controle de acesso (ACLs), o modelo de Servidor de Administração virtual é mais funcional e fornece um maior grau de isolamento. Além de uma estrutura dedicada de grupos de administração para dispositivos atribuídos com políticas e tarefas, cada Servidor de Administração virtual apresenta seu próprio grupo de dispositivos não atribuídos, conjuntos próprios de relatórios, dispositivos e eventos selecionados, pacotes de instalação, regras de movimentação etc. O escopo funcional dos Servidores de Administração virtuais pode ser usado tanto por provedores de serviços (xSP) para maximizar o isolamento de clientes quanto por organizações de grande porte com fluxos de trabalho sofisticados e vários administradores.

Os Servidores de Administração virtuais são muito semelhantes aos Servidores de Administração secundários, mas com as seguintes distinções:

- Em um Servidor de Administração virtual falta a maior parte das configurações globais e as suas próprias portas TCP.
- Um Servidor de Administração virtual não tem Servidores de Administração secundários.
- Um Servidor de Administração virtual não tem outros Servidores de Administração virtuais.
- Um Servidor de Administração físico exibe dispositivos, grupos, eventos e objetos em dispositivos gerenciados (itens em Quarentena, registro de aplicativos e etc.) de todos os seus Servidores de Administração virtuais.
- Um Servidor de Administração virtual somente pode verificar a rede com pontos de distribuição conectados.

Informações sobre as limitações do Kaspersky Security Center

A tabela a seguir exibe as limitações da versão atual do Kaspersky Security Center.

Limitações do Kaspersky Security Center

Tipo de limitação	Valor
Número máximo de dispositivos gerenciados por Servidor de Administração	100.000
Número máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada	300
Número máximo de grupos de administração	10.000
Número de eventos a armazenar	45.000.000
Número máximo de políticas	2000
Número máximo de tarefas	2000
Número total máximo de objetos do Active Directory (unidades organizacionais, UOs) e contas de usuários, dispositivos e grupos de segurança)	1.000.000
Número máximo de perfis em uma política	100
Número máximo de Servidores de Administração secundários em um Servidor de Administração principal único	500
Número máximo de Servidores de Administração virtuais	500
O número máximo de dispositivos que um ponto de distribuição único pode cobrir (os pontos de distribuição podem cobrir dispositivos não móveis somente)	10.000
Número máximo de dispositivos que podem usar um único gateway de conexão	10.000, incluindo dispositivos móveis
Número máximo de dispositivos móveis por Servidor de Administração	100.000, menos o número de dispositivos gerenciados estacionários

Carga de rede

Essa seção contém informações sobre o volume do tráfego de rede que os dispositivos cliente e o Servidor de Administração trocam durante os principais cenários administrativos.

A carga principal na rede é causada pelos seguintes cenários administrativos em andamento:

- Implementação inicial da proteção antivírus
- Atualização inicial dos bancos de dados antivírus
- Sincronização de um dispositivo cliente com o Servidor de Administração
- Atualizações regulares dos bancos de dados antivírus
- Processamento de eventos em dispositivos cliente pelo Servidor de Administração

Implementação inicial da proteção antivírus

Esta seção fornece informações sobre os valores de volume de tráfego após a instalação do Agente de Rede e Kaspersky Endpoint Security for Windows no dispositivo cliente (consulte a tabela abaixo).

O Agente de Rede é instalado usando a instalação forçada quando os arquivos necessários para a configuração são copiados pelo Servidor de Administração para uma pasta compartilhada no dispositivo cliente. Após a instalação, o Agente de Rede obtém o pacote de distribuição do Kaspersky Endpoint Security for Windows usando uma conexão ao Servidor de Administração.

Tráfego

Cenário	Instalação do Agente de Rede para um dispositivo cliente único	Instalar o Kaspersky Endpoint Security for Windows em um único dispositivo cliente (com bancos de dados atualizados)	Instalação simultânea do Agente de Rede e do Kaspersky Endpoint Security for Windows
Tráfego do dispositivo cliente ao Servidor de Administração, KB	1638,4	7843,84	9707,52
Tráfego do Servidor de Administração ao dispositivo cliente, KB	69.990,4	259.317,76	329.318,4
Tráfego total (para um único dispositivo cliente), KB	71.628,8	267.161,6	339.025,92

Após os Agentes de rede serem instalados nos dispositivos cliente, você pode atribuir que um dos dispositivos no grupo de administração atue como o ponto de distribuição. Ele será usado para distribuição de pacotes de instalação. Neste caso, o volume de tráfego transferido durante a implementação inicial da proteção antivírus variará consideravelmente dependendo se você usa ou não o multicasting de IP.

Se o multicasting de IP for usado, os pacotes de instalação serão enviados uma vez a todos os dispositivos em execução no grupo de administração. Assim, o tráfego total se tornará N vezes menor, onde N significa o número total de dispositivos em execução no grupo de administração. Se você não estiver usando multicasting de IP, o tráfego total é idêntico ao tráfego calculado quando os pacotes de distribuição são baixados do Servidor de Administração. Porém, a fonte do pacote será o ponto de distribuição, não o Servidor de Administração.

Atualização inicial dos bancos de dados antivírus

As taxas de tráfego durante a atualização inicial dos bancos de dados antivírus (ao iniciar a tarefa de atualização do banco de dados pela primeira vez em um dispositivo cliente) são as seguintes:

- Tráfego do dispositivo cliente ao Servidor de Administração: 1.8 MB.
- Tráfego do Servidor de Administração ao dispositivo cliente: 113 MB.
- Tráfego total (para um único dispositivo cliente): 114 MB.

Os dados podem variar ligeiramente dependendo da versão atual do banco de dados antivírus.

Sincronização de um cliente com o Servidor de Administração

Esse cenário descreve o estado do sistema de administração nos casos quando ocorre a sincronização intensiva de dados entre um dispositivo cliente e o Servidor de Administração. Os dispositivos cliente se conectam ao Servidor de Administração com o intervalo definido pelo administrador. O Servidor de Administração compara o status dos dados em um dispositivo cliente com os no Servidor, registra as informações no banco de dados sobre última conexão do dispositivo e sincroniza os dados.

Esta seção contém informações sobre os valores de tráfego para cenários de administração básicos ao conectar um cliente ao Servidor de Administração (consulte a tabela em baixo). Os dados na tabela podem variar ligeiramente dependendo da versão atual do banco de dados antivírus.

Tráfego

Cenário	Tráfego de dispositivos cliente ao Servidor de Administração, KB	Tráfego do Servidor de Administração aos dispositivos cliente, KB	Tráfego total (para um único dispositivo cliente), KB
Sincronização inicial antes da atualização dos bancos de dados em um dispositivo cliente	699,44	568,42	1267,86
Sincronização inicial após atualizar os bancos de dados em um dispositivo cliente	735,8	4474,88	5.210,68
Sincronização sem modificações em um dispositivo cliente e no Servidor de Administração	11,99	6,73	18,72
Sincronização após alterar o valor de uma configuração em uma política de grupo	9,79	11,39	21,18
Sincronização após alterar o valor de uma configuração em uma tarefa de grupo	11,27	11,72	22,99
Sincronização forçada sem modificações em um dispositivo cliente	77,59	99,45	177,04

O volume total de tráfego varia consideravelmente, dependendo do uso do multicasting de IP em grupos de administração. Se a multicasting de IP for usada, o volume de tráfego total diminui aproximadamente por N vezes para o grupo, onde N é o número total de dispositivos incluídos no grupo de administração.

O volume de tráfego na sincronização inicial antes e depois de uma atualização dos bancos de dados é especificada para os seguintes casos:

- Instalar o Agente de Rede e um aplicativo de segurança em um dispositivo cliente
- Mover um dispositivo cliente para um grupo de administração
- Aplicar uma política e tarefas que foram criadas para o grupo por padrão, a um dispositivo cliente

A tabela especifica as taxas de tráfego no caso de modificações de uma das configurações de proteção que estão incluídas nas configurações da política do Kaspersky Endpoint Security. Dados para outras configurações de políticas podem ser diferentes dos dados exibidos na tabela.

Atualização adicional dos bancos de dados antivírus

As taxas de tráfego em caso de atualização incremental dos bancos de dados antivírus, 20 horas após a atualização anterior, são as seguintes:

- Tráfego do dispositivo cliente ao Servidor de Administração: 169 KB.
- Tráfego do Servidor de Administração ao dispositivo cliente: 16 MB.
- Tráfego total (para um único dispositivo cliente): 16,3 MB.

Os dados na tabela podem variar ligeiramente dependendo da versão atual do banco de dados antivírus.

O volume de tráfego varia consideravelmente, dependendo se o multicasting de IP é usado em grupos de administração. Se a multicasting de IP for usada, o volume de tráfego total diminui aproximadamente por N vezes para o grupo, onde N é o número total de dispositivos incluídos no grupo de administração.

Processamento de eventos clientes pelo Servidor de Administração

Esta seção fornece as informações sobre os valores de volume de tráfego quando um dispositivo cliente encontra um evento de "Vírus detectado", o qual é então enviado ao Servidor de Administração e registrado no banco de dados (consulte a tabela abaixo).

Cenário	Transferência de dados para o Servidor de Administração quando um evento de "Vírus detectado" ocorre	Transferência de dados para o Servidor de Administração quando nove eventos de "Vírus detectado" ocorrem
Tráfego do dispositivo cliente ao Servidor de Administração, KB	49,66	64,05
Tráfego do Servidor de Administração ao dispositivo cliente, KB	28,64	31,97
Tráfego total (para um único dispositivo cliente), KB	78,3	96,02

Os dados na tabela podem variar ligeiramente dependendo da versão atual do aplicativo antivírus e os eventos que são definidos nesta política para registro no banco de dados do Servidor de Administração.

Tráfego durante 24 horas

Esta seção contém informações sobre as taxas de tráfego durante as 24 horas da atividade do sistema de administração em uma condição "silenciosa", quando nenhuma modificação aos dados é feita por dispositivos cliente ou pelo Servidor de Administração (consulte a tabela abaixo).

Os dados exibidos na tabela descrevem a condição da rede após a instalação padrão do Kaspersky Security Center e a conclusão do Assistente de início rápido. A frequência de sincronização do dispositivo cliente com o Servidor de Administração foi de 20 minutos; as atualizações foram baixadas no repositório do Servidor de Administração a cada hora.

Taxas de tráfego por 24 horas em estado inativo

Fluxo de tráfego	Valor
Tráfego do dispositivo cliente ao Servidor de Administração, KB	3235,84
Tráfego do Servidor de Administração ao dispositivo cliente, KB	64.378,88
Tráfego total (para um único dispositivo cliente), KB	67.614,72

Preparar para o gerenciamento de dispositivos móveis

Esta seção fornece as seguintes informações:

- Sobre o Servidor de dispositivos móveis Exchange projetado para gerenciamento de dispositivos móveis através do protocolo Exchange ActiveSync
- Sobre o Servidor de MDM do iOS projetado para gerenciar dispositivos iOS ao instalar perfis MDM do iOS dedicados neles
- Sobre o gerenciamento de dispositivos móveis que têm o Kaspersky Endpoint Security for Android instalado

Servidor de dispositivos móveis Exchange

Um Servidor de dispositivos móveis Exchange permite gerenciar dispositivos móveis que estão conectados a um Servidor de Administração usando o protocolo Exchange ActiveSync (dispositivos EAS).

Como implementar um Servidor de dispositivos móveis Exchange

Se múltiplos servidores Microsoft Exchange dentro de uma matriz Servidor de Acesso de Cliente tiverem sido implementados na organização, um Servidor de dispositivos móveis Exchange deve ser instalado em cada um dos servidores naquela matriz. A opção **Modo de cluster** deve ser ativada no Assistente de implementação do servidor de dispositivos móveis do Microsoft Exchange. Neste caso, um conjunto de instâncias do Servidor de dispositivos móveis Exchange instalado em servidores na matriz é chamado de cluster do Servidor de dispositivos móveis Exchange.

Se nenhuma matriz do Servidor Acesso de Cliente do Microsoft Exchange Servers estiver implementado na organização, um Servidor de dispositivos móveis Exchange deve ser instalado em um Microsoft Exchange Server que tenha o Acesso de Cliente. Neste caso, a opção **Modo padrão** deve ser ativada no Assistente de instalação do Servidor de dispositivos móveis do Microsoft Exchange.

Junto com o Servidor de dispositivos móveis Exchange, o Agente de Rede deve ser instalado no dispositivo; isso ajuda a integrar o Servidor de dispositivos móveis Exchange com o Kaspersky Security Center.

O escopo da verificação padrão do Servidor de dispositivos móveis Exchange é o domínio atual do Active Directory no qual foi instalado. Implementar um Servidor de dispositivos móveis Exchange em um servidor com o Microsoft Exchange Server (versões 2010, 2013) instalado, permite à expansão do escopo da verificação para incluir toda a floresta de domínios no Servidor de dispositivos móveis Exchange (consulte a seção "Configurar o escopo da verificação"). As informações solicitadas durante uma verificação incluem as contas dos usuários do Microsoft Exchange Server, políticas do Exchange ActiveSync e os dispositivos móveis de usuários conectados ao Microsoft Exchange Server através do protocolo Exchange ActiveSync.

Múltiplas instâncias de um Servidor de dispositivos móveis do Microsoft Exchange não podem ser instaladas dentro de um domínio único se eles executarem no **Modo padrão** sendo gerenciado por um único Servidor de Administração. Dentro de uma floresta de domínios de um único Active Directory, múltiplas instâncias de um Servidor de dispositivos móveis do Microsoft Exchange (ou múltiplos clusters do Servidores de dispositivos móveis Exchange) não podem ser instaladas – se forem executados no **Modo padrão** com um escopo expandido de verificação que inclui toda a floresta de domínios e se estiverem conectados a um único Servidor de Administração.

Direitos necessários para a implementação de um Servidor de dispositivos móveis Exchange

A implementação de um Servidor de dispositivos móveis do Microsoft Exchange em um Microsoft Exchange Server (2010, 2013) requer os direitos de administrador do domínio e a função Gerenciamento da organização. A implementação de um Servidor de dispositivos móveis do Microsoft Exchange em um Microsoft Exchange Server (2007) requer os direitos de administrador do domínio e a associação ao grupo de segurança de Administradores da Organização do Exchange.

Conta para o serviço Exchange ActiveSync

Quando um Servidor de dispositivos móveis Exchange for instalado, uma conta é automaticamente criada no Active Directory:

- No Microsoft Exchange Server (2010, 2013): KLMDM4ExchAdmin***** conta com a função Grupo de Função KLMDM.
- No Microsoft Exchange Server (2007): Conta KLMDM4ExchAdmin*****, um membro do grupo de segurança KLMDM Secure Group.

O serviço Servidor de dispositivos móveis Exchange é executado sob esta conta.

Se você quiser cancelar a geração automática de uma conta, terá que criar uma conta personalizada com os seguintes direitos:

- Ao usar Microsoft Exchange Server (2010, 2013), é preciso atribuir à conta uma função que tem a permissão de executar os seguintes cmdlets:
  - Get-CASMailbox
  - Set-CASMailbox
  - Remove-ActiveSyncDevice
  - Clear-ActiveSyncDevice
  - Get-ActiveSyncDeviceStatistics
  - Get-AcceptedDomain
  - Set-AdServerSettings
  - Get-ActiveSyncMailboxPolicy
  - New-ActiveSyncMailboxPolicy
  - Set-ActiveSyncMailboxPolicy
  - Remove-ActiveSyncMailboxPolicy
- Ao usar um Microsoft Exchange Server (2007), à conta deve ser concedida os direitos de acesso aos objetos do Active Directory (consulte a tabela abaixo).

Direitos de acesso aos objetos do Active Directory

Acesso	Objeto	Cmdlet
Completo	Thread "CN=Mobile Mailbox Policies,CN=<Nome da organização>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nome do domínio>"	`Add-ADPermission -User <Nome de usuário ou grupo> -Identity "CN=Mobile Mailbox Policies,CN=<Nome da organização>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nome do domínio>" -InheritanceType All -AccessRight GenericAll`
Ler	Thread "CN=<Nome da organização>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nome do domínio>"	`Add-ADPermission -User <Nome do usuário ou grupo> -Identity "CN=<Nome da organização>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nome do domínio>" -InheritanceType All -AccessRight GenericRead`
Ler/gravar	Propriedades msExchMobileMailboxPolicyLink e msExchOmaAdminWirelessEnable para objetos no Active Directory	`Add-ADPermission -User <Nome do usuário ou grupo> -Identity "DC=<Dome do domínio>" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`
Extended right ms-Exch-Store-Active	Repositórios da caixa de correio do servidor Exchange, thread "CN=Databases,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative Groups,CN=<Nome da organização>,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=<Nome do domínio>"	`Get-MailboxDatabase | Add-ADPermission -User <Nome de usuário ou grupo> -ExtendedRights ms-Exch-Store-Admin`

Servidor MDM do iOS

O Servidor de MDM do iOS permite gerenciar dispositivos iOS ao instalar perfis MDM do iOS dedicados neles. Os seguintes recursos são compatíveis:

- Bloquear o dispositivo
- Redefinir a senha
- Limpar os dados
- Instalação ou remoção de aplicativos
- O uso de um perfil de MDM do iOS com configurações avançadas (tal como, configurações de VPN, configurações de e-mail, configurações de Wi-Fi, configurações de câmera, certificados e etc.)

O Servidor de MDM do iOS é um serviço da Web que recebe conexões de entrada de dispositivos móveis através de sua porta TLS (por padrão, porta 443), que é gerenciada pelo Kaspersky Security Center usando o Agente de Rede. O Agente de Rede é instalado localmente em um dispositivo com um Servidor de MDM do iOS implementado.

Ao implementar um Servidor de MDM do iOS, o administrador deve executar as seguintes ações:

- Fornecer ao Agente de Rede o acesso ao Servidor de Administração
- Fornecer aos dispositivos móveis o acesso à porta TCP do Servidor de MDM do iOS

Esta seção aborda duas configurações padrão de um Servidor de MDM do iOS.

Configuração padrão: Kaspersky Device Management for iOS no DMZ

Um Servidor de MDM do iOS é localizado no DMZ da rede local de uma organização com o acesso à Internet. Um recurso especial desta abordagem é a ausência de qualquer problema quando o serviço da Web MDM do iOS for acessado de dispositivos por meio da Internet.

Como o gerenciamento de um Servidor de MDM do iOS necessita que o Agente de Rede seja instalado localmente, você deve assegurar a interação do Agente de Rede com o Servidor de Administração. Você poderá assegurar isso usando um dos seguintes métodos:

- Ao mover o Servidor de Administração para o DMZ.
- Usando um gateway de conexão:
    a. No dispositivo com o Servidor de MDM do iOS implementado, conecte o Agente de Rede ao Servidor de Administração através de uma gateway de conexão.
    b. No dispositivo com o Servidor de MDM do iOS implementado, atribua o Agente de Rede para atuar como um gateway de conexão.

Configuração padrão: Servidor de MDM do iOS na rede local de uma organização

Um Servidor de MDM do iOS está localizado na rede interna de uma organização. A porta 443 (porta padrão) deve ser ativada para acesso externo, por exemplo, publicando o serviço da Web MDM do iOS no proxy reverso que dá suporte à delegação restrita de Kerberos.

Qualquer configuração padrão necessita do acesso aos serviços da Web da Apple para o Servidor de MDM do iOS (faixa 17.0.0.0/8) através da porta TCP 2197. Esta porta é usada para notificar os dispositivos sobre os novos comandos por meio de um serviço dedicado denominado APNs.

Gerenciar dispositivos móveis com o Kaspersky Endpoint Security for Android

Os dispositivos móveis com o Kaspersky Endpoint Security for Android™ instalado (aqui referidos como dispositivos KES) são gerenciados por meio do Servidor de Administração. O Kaspersky Security Center oferece suporte aos seguintes recursos para gerenciar dispositivos do KES:

- Tratar dispositivos móveis como dispositivos cliente:
  - Associação em grupos de administração
  - Monitoramento, como visualização de status, eventos e relatórios
  - Modificar as configurações locais e atribuir políticas para o Kaspersky Endpoint Security for Android
- Enviar comandos em modo centralizado
- Instalar pacotes de aplicativos móveis remotamente

O Servidor de Administração gerencia dispositivos KES por meio de TLS, pela porta TCP 13292.

Informações sobre o desempenho do Servidor de Administração

Esta seção apresenta os resultados do teste de desempenho do Servidor de Administração para diferentes configurações de hardware, assim como as restrições na conexão de dispositivos gerenciados ao Servidor de Administração.

Limitações na conexão a um Servidor de Administração

Um Servidor de Administração é compatível com o gerenciamento de até 100.000 dispositivos sem uma perda no desempenho.

Limitações de conexões a um Servidor de Administração sem uma perda de desempenho:

- Um Servidor de Administração pode suportar até 500 Servidores de Administração virtuais.
- O Servidor de Administração principal comporta no máximo 1000 sessões simultaneamente.
- Os Servidores de Administração virtuais comportam não mais do que 1000 sessões simultaneamente.

Resultados do teste de desempenho do Servidor de Administração

Os resultados do teste de desempenho do Servidor de Administração nos permitiram definir números máximos de dispositivos cliente com os quais o Servidor de Administração pode ser sincronizado dentro do intervalos de tempo especificados. Você pode usar estas informações para selecionar o esquema ideal para a implementação da proteção antivírus em redes de computador.

Os dispositivos com as seguintes configurações de hardware (ver as tabelas abaixo) foram usados para o teste:

Configuração de hardware do Servidor de Administração

Parâmetro	Valor
CPU	Intel Xeon CPU E5630, velocidade de clock de 2.53 GHz, 2 soquete, 8 núcleos, 16 processadores lógicos
RAM	26 GB
Disco rígido	IBM ServeRAID M5014 SCSI Disk Device, 487 GB
Sistema operacional	Microsoft Windows Server 2019 Standard, versão 10.0.17763, build 17763
Rede	QLogic BCM5709C Gigabit Ethernet (NDIS VBD Client)

Configuração de hardware para o dispositivo do SQL Server

Parâmetro	Valor
CPU	Intel Xeon CPU X5570, velocidade de clock de 2,93 GHz, 2 soquetes, 8 núcleos, 16 processadores lógicos
RAM	32 GB
Disco rígido	Dispositivo de disco SCSI Adaptec Array, 2047 GB
Sistema operacional	Microsoft Windows Server 2019 Standard, versão 10.0.17763, build 17763
Rede	Intel 82576 Gigabit

O Servidor de Administração é compatível com a criação de 500 Servidores de Administração virtuais.

O intervalo de sincronização foi de 15 minutos para cada 10.000 dispositivos gerenciados (ver a tabela abaixo).

Resultados resumidos do teste de carga do Servidor de Administração

Synchronization interval (min)	Número de dispositivos gerenciados
15	10.000
30	20.000
45	30.000
60	40.000
75	50.000
90	60.000
105	70.000
120	80.000

Synchronization interval (min)	Número de dispositivos gerenciados
135	90.000
150	100.000

Se você conectar o Servidor de Administração com um servidor de banco de dados MySQL ou SQL Express, recomendamos evitar usar o aplicativo para gerenciar mais do que 10.000 dispositivos. Para o sistema de gerenciamento de banco de dados MariaDB, o número máximo recomendado de dispositivos gerenciados é 20.000.

Resultados do teste de desempenho do Servidor proxy da KSN

Se a sua rede corporativa tiver um grande volume de dispositivos cliente e eles usarem o Servidor de Administração como Servidor proxy da KSN, o hardware do Servidor de Administração deverá atender aos requisitos específicos para poder processar as solicitações dos dispositivos cliente. É possível usar os resultados dos testes abaixo para avaliar a carga do Servidor de Administração na rede e planejar os recursos de hardware para propiciar o funcionamento normal do serviço de proxy da KSN.

As tabelas abaixo mostram a configuração de hardware do Servidor de Administração e do SQL Server. Essa configuração foi usada para testes.

Configuração de hardware do Servidor de Administração

Parâmetro	Valor
CPU	Intel Xeon CPU E5450, velocidade de clock de 3,00 GHz, 2 soquetes, 8 núcleos, 16 processadores lógicos
RAM	32 GB
Sistema operacional	Microsoft Windows Server 2016 Standard

Configuração de hardware do SQL Server

Parâmetro	Valor
CPU	Intel Xeon CPU E5450, velocidade de clock de 3,00 GHz, 2 soquetes, 8 núcleos, 16 processadores lógicos
RAM	32 GB
Sistema operacional	Microsoft Windows Server 2019 Standard

A tabela abaixo mostra os resultados do teste.

Resultados resumidos do teste de desempenho de Servidor proxy da KSN

Parâmetro	Valor
Número máximo de solicitações processadas por segundo	4914
Utilização máxima da CPU	36%

Configurações de rede para interação com serviços externos

O Kaspersky Security Center usa as seguintes configurações de rede para interagir com serviços externos.

Configurações de rede

Configurações de rede	Endereço	Descrição
Porta: 443 Protocolo: HTTPS	activation-v2.kaspersky.com	Ativação do aplicativo.
Porta: 443 Protocolo: 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	Atualização de bancos de dados, módulos de software e aplicativos da Kaspersky.
Porta: 443 Protocolo: HTTPS	https://downloads.upd.kaspersky.com	• Atualização de bancos de dados, módulos de software e aplicativos da Kaspersky. • Verificar se os servidores da Kaspersky estão acessíveis. Antes de baixar os bancos de dados e módulos de software da Kaspersky, o Kaspersky Security Center verifica se os servidores da Kaspersky estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos.

Configurações de rede	Endereço	Descrição
Porta: 80 Protocolo: 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	Atualização de bancos de dados, módulos de software e aplicativos da Kaspersky.
Porta: 443 Protocolo: 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	Uso da Kaspersky Security Network.
Porta: 443, 1443 Protocolo: HTTPS	ksn-a-stat-geo.kaspersky-labs.com 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	Uso da Kaspersky Security Network.

Configurações de rede	Endereço	Descrição
Protocolo: HTTPS	click.kaspersky.com redirect.kaspersky.com	Como seguir os links da interface.
Porta: 80 Protocolo: HTTP	http://crl.kaspersky.com http://ocsp.kaspersky.com	Esses servidores fazem parte da Infraestrutura de Chaves Públicas (PKI) e são necessários para verificar o status de validade dos certificados de assinatura digital da Kaspersky. A CRL é uma lista de certificados revogados. O OCSP permite solicitar o status de um certificado específico em tempo real. Esses servidores ajudam a garantir a segurança da interação com certificados digitais e protegem contra possíveis ataques.
Porta: 443 Protocolo: HTTPS	https://ipm-klca.kaspersky.com	Informativos de marketing.

Para a interação adequada do Kaspersky Security Center com os serviços externos, considere as seguintes recomendações:
- O tráfego de rede não criptografado deve ser permitido nas portas 443 e 1443 no equipamento de rede e no servidor proxy de sua organização.
- Quando o Servidor de Administração interage com os servidores de atualização da Kaspersky e os servidores da Kaspersky Security Network, é necessário evitar o sequestro do tráfego de rede com substituição de certificado (ataques MITM).

Para baixar as atualizações usando o protocolo HTTP ou HTTPS com o utilitário klscflag:

1. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Caso queira baixar as atualizações com o uso do protocolo HTTP, execute um dos seguintes comandos com a conta root:

   - No dispositivo com o Servidor de Administração instalado:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 1
     ```

   - Em um ponto de distribuição:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 1
     ```

   Caso queira baixar as atualizações com o uso do protocolo HTTPS, execute um dos seguintes comandos com a conta root:

   - No dispositivo com o Servidor de Administração instalado:

     ```
     klscflag.exe -fset -pv klserver -s Updater -n DisableKLHttps -t d -v 0
     ```

   - Em um ponto de distribuição:

     ```
     klscflag.exe -fset -pv klnagent -s Updater -n DisableKLHttps -t d -v 0
     ```

Implementar o Agente de Rede e o aplicativo de segurança

Para gerenciar dispositivos em uma organização, você deve instalar o Agente de Rede em cada um deles. A implementação do Kaspersky Security Center distribuído nos dispositivos corporativos normalmente começa com a instalação do Agente de Rede neles.

No Microsoft Windows XP, o Agente de Rede pode não executar as seguintes operações corretamente: baixar atualizações diretamente dos servidores da Kaspersky (como um ponto de distribuição); funcionar como servidor proxy da KSN (como um ponto de distribuição); e detectar vulnerabilidades de terceiros (caso o Gerenciamento de patches e vulnerabilidades seja usado).

Implementação inicial

Para gerenciar dispositivos em uma organização, você deve instalar o Agente de Rede em cada um deles.

A instalação do Agente de Rede nos dispositivos gerenciados que executam Windows pode ser realizada das seguintes formas:

- Com ferramentas de terceiros para a instalação remota de aplicativos.
- Clonando uma imagem do disco rígido do administrador com o sistema operacional e com o Agente de Rede, utilizando ferramentas fornecidas pelo Kaspersky Security Center para tratar imagens do disco ou usando ferramentas de terceiros.
- Com políticas de grupo do Windows, utilizando ferramentas padrão de gestão do Windows para políticas de grupo ou em modo automático, através da opção correspondente e dedicada na tarefa de instalação remota do Kaspersky Security Center.
- No modo forçado, utilizando recursos do sistema operacional por meio da tarefa de instalação remota do Kaspersky Security Center.
- Enviando aos usuários de dispositivo links para pacotes independentes pelo Kaspersky Security Center. Os pacotes independentes são módulos executáveis que contêm os pacotes de distribuição de aplicativos selecionados com as suas configurações definidas.
- Manualmente, executando os instaladores do aplicativo em dispositivos.

A instalação inicial do Agente de Rede nos dispositivos gerenciados que rodam Linux pode ser realizada das seguintes formas:

- Ao se conectar com o dispositivo gerenciado via SSH e que executa a tarefa de instalação remota.
- Ao executar a instalação do pacote no dispositivo gerenciado.

A instalação inicial do Agente de Rede nos dispositivos gerenciados que executam macOS pode ser realizada das seguintes formas:

- Ao executar a tarefa de instalação remota pelo ponto de distribuição do macOS.
- Ao enviar aos usuários do dispositivo links para pacotes autônomos gerados pelo Kaspersky Security Center Geral. Pacotes autônomos são módulos executáveis que contêm os pacotes de distribuição de aplicativos selecionados, com configurações predefinidas.

Depois de instalar o Agente de Rede em um dispositivo, você poderá executar a instalação remota de aplicativos da Kaspersky no mesmo dispositivo através deste Agente de Rede. O pacote de distribuição de um aplicativo a ser instalado é transferido através de canais de comunicação entre Agentes de Rede e o Servidor de Administração, junto com as configurações de instalação definidas pelo administrador. Para transferir o pacote de distribuição, é possível usar nós de distribuição de transmissão, ou seja, pontos de distribuição, entrega multicast, etc.

Ao selecionar um método e uma estratégia para a implementar aplicativos em uma rede gerenciada, é necessário considerar um número de fatores (lista parcial):

- Configuração de rede da organização.
- Número total de dispositivos.
- Presença de dispositivos na rede da organização que não são membros de nenhum domínio do Active Directory, e a presença de contas uniformes com direitos de administrador nesses dispositivos.
- Capacidade do canal entre o Servidor de Administração e os dispositivos.
- Tipo de comunicação entre o Servidor de Administração, sub-redes remotas e a capacidade dos canais de rede nessas sub-redes.
- Configurações de segurança aplicadas nos dispositivos remotos no início da implementação. Esses parâmetros permitem estabelecer a conexão remota com o dispositivo gerenciado e iniciar a instalação.

Configurar os instaladores

Antes da implementação inicial de aplicativos Kaspersky em uma rede, você deve especificar as configurações de instalação, ou seja, as definidas durante a instalação do aplicativo. Ao instalar o Agente de Rede, você deve especificar, no mínimo, um endereço para a conexão ao Servidor de Administração; algumas configurações avançadas também podem ser necessárias. Dependendo do método Instalação que você selecionou, poderá definir configurações de diferentes maneiras. No caso mais simples (instalação interativa manual em um dispositivo selecionado), todas as configurações relevantes podem ser definidas através da interface de usuário do instalador.

Este método de definição das configurações é inadequado para a instalação silenciosa de aplicativos em grupos de dispositivos. Em geral, o administrador deve especificar os valores das configurações no modo centralizado. Os valores podem ser usados posteriormente para a instalação silenciosa em dispositivos em rede selecionados.

Pacotes de instalação

O primeiro e principal método de definir as configurações da instalação de aplicativos é útil para muitas finalidades e assim adequado para todos os métodos de instalação, para os métodos de instalação com as ferramentas do Kaspersky Security Center e com a maior parte de ferramentas de terceiros. Este método consiste na criação de pacotes de instalação de aplicativos no Kaspersky Security Center.

Os pacotes de Instalação são gerados usando os seguintes métodos:

- Automaticamente, a partir de pacotes de distribuição especificados, com base em *descritores* incluídos (arquivos com a extensão .kud que contêm regras para a instalação e análise de resultados e outras informações)

- A partir de arquivos executáveis de instaladores ou a partir de instaladores no formato nativo (.msi, .deb, .rpm), para aplicativos padrão ou compatíveis

Os pacotes de instalação gerados são organizados hierarquicamente como pastas com subpastas e arquivos. Além do pacote de distribuição original, um pacote de instalação contém configurações editáveis (incluindo as configurações do instalador e as regras para processar os casos tal como necessidade de reiniciar o sistema operacional para concluir a instalação), assim como os módulos auxiliares secundários.

Os valores das configurações de instalação que seriam específicos para o aplicativo individual suportado podem ser definidos na interface do usuário do Console de Administração quando o pacote de instalação for criado. Ao executar a instalação remota de aplicativos através das ferramentas do Kaspersky Security Center, os pacotes de instalação são entregues aos dispositivos para que ao executar o instalador de um aplicativo, torna todas as configurações definidas pelo administrador à disposição daquele aplicativo. Ao usar as ferramentas de terceiros para a instalação de aplicativos Kaspersky, você somente tem de assegurar a disponibilidade de todo o pacote de instalação no dispositivo, ou seja, a disponibilidade do pacote de distribuição e de suas configurações. Os pacotes de Instalação são criados e armazenados pelo Kaspersky Security Center em uma subpasta dedicada da pasta compartilhada.

Não especifique nenhum detalhe de contas privilegiadas nos parâmetros dos pacotes de instalação.

Para obter a instrução sobre a utilização deste método de configuração para aplicativos Kaspersky antes da implementação através de ferramentas de terceiros, consulte a seção "Implementar usando políticas de grupo do Microsoft Windows".

Imediatamente após a instalação do Kaspersky Security Center, alguns pacotes de instalação são automaticamente gerados; eles estão prontos para a instalação e incluem pacotes de Agente de Rede e pacotes de aplicativos de segurança para o Microsoft Windows.

Embora a chave de licença para um aplicativo possa ser definida nas propriedades de um pacote de instalação, é aconselhável evitar este método de distribuição da licença porque é fácil obter o acesso de leitura para pacotes de instalação. Você deve usar as chaves automaticamente distribuídas ou as tarefas de instalação para chaves de licença.

Propriedades MSI e arquivos de transformação

Outro modo de configurar a instalação na plataforma Windows é o de definir as propriedades MSI e arquivos de transformação. Este método pode ser aplicado nos seguintes casos:

- Ao instalar através das políticas de grupo do Windows, usando as ferramentas regulares da Microsoft ou outras ferramentas de terceiros para tratar políticas de grupo do Windows.

- Ao instalar aplicativos usando ferramentas de terceiros intencionadas para tratar de instaladores no formato do Microsoft Installer.

Implementação com ferramentas de terceiros para a instalação remota de aplicativos

Quando qualquer ferramenta para a instalação remota de aplicativos (tal como o Microsoft System Center) estiver disponível em uma organização, é conveniente executar a implementação inicial usando estas ferramentas.

As seguintes ações devem ser executadas:

- Selecione o método para configurar a instalação melhor adequada para a ferramenta implementação a ser usada.
- Defina o mecanismo para a sincronização entre a modificação das configurações dos pacotes de instalação (através da interface do Console de Administração) e a operação das ferramentas de terceiros selecionadas e usadas para a implementação de aplicativos a partir dos dados do pacote de instalação.
- Ao executar a instalação a partir de uma pasta compartilhada, você deve assegurar-se de que este recurso de arquivo tenha capacidade suficiente.

Sobre as tarefas de instalação remotas no Kaspersky Security Center

O Kaspersky Security Center fornece vários mecanismos para a instalação remota de aplicativos, que são implementados como tarefas de instalação remotas (instalação forçada, instalação copiando uma imagem de disco rígido, instalação através das políticas de grupo do Microsoft Windows). Você pode criar uma tarefa de instalação remota para um grupo de administração especificado e para dispositivos específicos ou para uma seleção de dispositivos (tais tarefas são exibidas no Console de Administração, na pasta **Tarefas**). Ao criar uma tarefa, você pode selecionar pacotes de instalação (aqueles do Agente de Rede e / ou outro aplicativo) a ser instalado dentro desta tarefa, assim como especificar determinadas configurações que definem o método da instalação remota. Além disso, você pode usar o Assistente de instalação remota, que tem base na criação de uma tarefa de instalação remota e no monitoramento dos resultados.

As tarefas para grupos de administração afetam ambos os dispositivos incluídos em um grupo especificado e todos os dispositivos em todos os subgrupos dentro daquele grupo de administração. Uma tarefa cobre dispositivos de Servidores de Administração secundários incluídos em um grupo ou algum dos seus subgrupos se a configuração correspondente estiver ativada na tarefa.

As tarefas para dispositivos específicos atualizam a lista de dispositivos cliente em cada execução de acordo com o conteúdo da seleção no momento em que a tarefa é iniciada. Se uma seleção incluir dispositivos que foram conectados aos Servidores de Administração secundários, a tarefa também será executada naqueles dispositivos. Para obter detalhes sobre aquelas configurações e métodos de instalação, consulte abaixo nesta seção.

Para certificar-se do sucesso de uma tarefa de instalação remota nos dispositivos conectados aos Servidores de Administração secundários, você deve usar a tarefa de encaminhamento para encaminhar os pacotes de instalação usados por sua tarefa aos Servidores de Administração secundários correspondentes com antecedência.

Implementação ao capturar e copiar a imagem de um dispositivo

Caso necessite instalar o Agente de Rede em dispositivos nos quais um sistema operacional e outro software também devem ser instalados (ou reinstalados), será possível usar o mecanismo de captura e copiar a imagem daquele dispositivo.

Para realizar a implementação capturando e copiando um disco rígido:

1. Crie um dispositivo de referência com um sistema operacional e o software relevante instalado, incluindo o Agente de Rede e um aplicativo de segurança.

2. Capture a imagem de referência no dispositivo e distribua aquela imagem nos novos dispositivos através da tarefa dedicada do Kaspersky Security Center.

   Para capturar e instalar imagens do disco, você pode usar ferramentas de terceiros disponíveis na organização ou recurso fornecido (sob a licença do Gerenciamento de patches e vulnerabilidades) pelo Kaspersky Security Center.

Se você usar alguma ferramenta de terceiros para processar imagens do disco, deverá excluir as informações que o Kaspersky Security Center usa para identificar o dispositivo gerenciado ao executar a implementação em um dispositivo a partir de uma imagem de referência. De outra forma, o Servidor de Administração não será capaz de distinguir adequadamente os dispositivos criados ao copiar a mesma imagem.

Ao capturar uma imagem do disco com ferramentas do Kaspersky Security Center, este problema é solucionado automaticamente.

Copiar uma imagem do disco com ferramentas de terceiros

Ao aplicar ferramentas de terceiros para capturar a imagem de um dispositivo com o Agente de Rede instalado, use um dos seguintes métodos:

- Método recomendado. Ao instalar o Agente de Rede em um dispositivo de referência, capture a imagem do dispositivo antes da primeira execução do serviço Agente de Rede (porque as informações exclusivas que identificam o dispositivo são criadas na primeira conexão do Agente de Rede ao Servidor de Administração). Após isso, recomenda-se que você evite executar o serviço Agente de Rede até a conclusão da operação de captura da imagem.

- No dispositivo de referência, pare o serviço Agente de Rede e execute o utilitário klmover com a chave -dupfix. O utilitário klmover está incluído no pacote de instalação do Agente de Rede. Evite qualquer execuções subsequentes do serviço Agente de Rede até que a operação de captura da imagem seja concluída.

- Assegure-se de que o klmover será executado com a chave -dupfix antes (requisito obrigatório) da primeira execução do serviço Agente de Rede em dispositivos alvo, na primeiro inicialização do sistema operacional após a implementação da imagem. O utilitário klmover está incluído no pacote de instalação do Agente de Rede.

- Use o modo de clonagem do disco do Agente de Rede.

Caso a imagem da unidade de disco rígido tenha sido copiada incorretamente, é possível solucionar o problema.

Também é possível capturar a imagem de um dispositivo sem que o Agente de Rede esteja instalado. Para fazer isso, execute a implementação de imagem em dispositivos de destino e, a seguir, implemente o Agente de Rede. Caso esteja usando esse método, forneça acesso à pasta de rede com os pacotes de instalação independentes a partir de um dispositivo.

Cópia incorreta de uma imagem do disco rígido

Caso uma imagem do disco rígido com o Agente de Rede instalado tenha sido copiada sem que as regras de implementação sejam seguidas, alguns dispositivos podem ser exibidos juntos no Console de Administração sob um ícone único com um nome que muda constantemente.

É possível resolver isso usando um dos seguintes métodos:

- Removendo o Agente de Rede

  Este método é o mais confiável. É necessário remover o Agente de Rede nos dispositivos que foram copiados incorretamente a partir da imagem, usando ferramentas de terceiros, e, a seguir, instalá-lo novamente. O Agente de Rede não pode ser removido por meio das ferramentas do Kaspersky Security Center, porque o Servidor de Administração não pode distinguir entre dispositivos defeituosos (todos compartilham o mesmo ícone no Console de Administração).

- Executando o utilitário klmover com a chave "-dupfix"

  Use ferramentas de terceiros para executar o utilitário klmover, localizado na pasta de instalação do Agente de Rede, com a chave "-dupfix" (klmover -dupfix) uma vez em dispositivos com falha (aqueles copiados incorretamente a partir da imagem). Não é possível executar o utilitário com as ferramentas do Kaspersky Security Center, pois o Servidor de Administração não pode distinguir entre dispositivos defeituosos (todos compartilham o mesmo ícone no Console de Administração).

  Em seguida, exclua o ícone no qual os dispositivos defeituosos foram exibidos antes de executar o utilitário.

- Reforçando a regra para detecção de dispositivos copiados incorretamente.

  > Esse método só é aplicável se o Servidor de Administração e os Agentes de Rede versão 10 Service Pack 1 ou superior estiverem instalados.

  A regra para detecção de Agentes de Rede copiados incorretamente deve ser reforçada para que a alteração do nome NetBIOS de um dispositivo resulte em uma "correção" automática desses Agentes de Rede (com a suposição de que todos os dispositivos copiados tenham nomes NetBIOS exclusivos).

  No dispositivo com o Servidor de Administração, é preciso importar o arquivo reg, mostrado abaixo, para o Registro e, a seguir, reiniciar o serviço do Servidor de Administração.

  - Se um sistema operacional de 32 bits estiver instalado no dispositivo com o Servidor de Administração:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

  - Se um sistema operacional de 64 bits estiver instalado no dispositivo com o Servidor de Administração:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags]
"KLSRV_CheckClones"=dword:00000003
```

Implementar usando políticas de grupo do Microsoft Windows

Recomenda-se que você execute a implementação inicial de Agentes de Rede através da políticas de grupo do Microsoft Windows se as seguintes condições forem atendidas:

- Este dispositivo é membro de um domínio Active Directory.
- O esquema de implementação permite esperar pelo reinício da próxima rotina de dispositivos alvo antes da implementação inicial de Agentes de Rede neles (ou você pode forçar uma política de grupo do Windows a ser aplicada àqueles dispositivos).

Este esquema de implementação consiste no seguinte:

- O pacote de distribuição do aplicativo no formato do Microsoft Installer (pacote MSI) está localizado em uma pasta compartilhada (uma pasta onde as contas de LocalSystem de dispositivos alvo têm permissões de leitura).
- Na política de grupo do Active Directory, um objeto Instalação é criado para o pacote de distribuição.
- O escopo da instalação é definido especificando a unidade organizacional (UO) e/ou o grupo de segurança, que inclua os dispositivos alvo.
- Na próxima vez que um dispositivo alvo se conecta ao domínio (antes que os usuários do dispositivo se conectem ao sistema), todos os aplicativos instalados são verificados quanto a presença do aplicativo necessário. Se o aplicativo não for encontrado, o pacote de distribuição é baixado do recurso especificado na política e então é instalado.

Uma vantagem deste esquema de implementação é que os aplicativos atribuídos são instalados nos dispositivos alvo enquanto o sistema operacional está sendo carregado, ou seja, até antes que o usuário se conecte ao sistema. Mesmo se um usuário com direitos suficientes remova o aplicativo, ele será reinstalado na próxima inicialização do sistema operacional. Este problema do esquema implementação é que as modificações feitas pelo administrador à política de grupo não entrarão em vigor até que os dispositivos sejam reiniciados (se nenhuma ferramenta adicional estiver envolvida).

Você pode usar políticas de grupo para instalar o Agente de Rede assim como outros aplicativos se os seus respetivos instaladores estiverem no formato do Windows Installer.

Quando este esquema de implementação for selecionado, você também deve avaliar a carga do recurso de arquivo do qual os arquivos serão copiados para os dispositivos após aplicar a política de grupo do Windows.

Tratar políticas do Microsoft Windows através da tarefa de instalação remota do Kaspersky Security Center

O modo mais simples de instalar aplicativos por meio das políticas de grupo do Microsoft Windows é de selecionar a opção **Atribuir a instalação do pacote em políticas de grupo do Active Directory** nas propriedades da tarefa de instalação remota do Kaspersky Security Center. Neste caso, o Servidor de Administração automaticamente executa as seguintes ações quando você executa a tarefa:

- Cria os objetos necessários na política de grupo do Microsoft Windows.
- Cria grupos de segurança dedicados, inclui os dispositivos alvo naqueles grupos e atribui a instalação de aplicativos selecionados à eles. O conjunto de grupos de segurança será atualizado a cada tarefa executada, de acordo com o conjunto de dispositivos no momento da execução.

Para tornar este recurso operável, nas propriedades de tarefa, especifique uma conta que tenha permissões de gravação nas políticas de grupo do Active Directory.

Se você pretender instalar o Agente de Rede e outro aplicativo através da mesma tarefa, selecionar a opção **Atribuir a instalação do pacote em políticas de grupo do Active Directory** faz com que o aplicativo crie um objeto de instalação na política do Active Directory somente para o Agente de Rede. O segundo aplicativo selecionado na tarefa será instalado através das ferramentas do Agente de Rede assim que o último seja instalado no dispositivo. Se você desejar instalar um aplicativo que não seja o Agente de Rede através das políticas de grupo do Windows, deverá criar uma tarefa de instalação somente para este pacote de instalação (sem o pacote do Agente de Rede). Nem todo aplicativo pode ser instalado usando políticas de grupo do Microsoft Windows. Para conhecer esta capacidade, você pode referir-se às informações sobre os métodos possíveis para instalar o aplicativo.

Se os objetos necessários forem criados na política de grupo usando as ferramentas do Kaspersky Security Center, a pasta compartilhada do Kaspersky Security Center será usada como a fonte do pacote de instalação. Ao planejar a implementação, você deve correlacionar a velocidade de leitura desta pasta com o número de dispositivos e o tamanho do pacote de distribuição a ser instalado. Pode ser útil localizar a pasta compartilhada do Kaspersky Security Center em um repositório de arquivo dedicado de alto desempenho.

Além da sua facilidade de uso, a criação automática de políticas de grupo do Windows através doo Kaspersky Security Center tem esta vantagem: ao planejar a instalação do Agente de Rede, você pode especificar facilmente o grupo de administração do Kaspersky Security Center no qual os dispositivos serão automaticamente movidos depois que a instalação seja concluída. Você pode especificar este grupo no Assistente para novas tarefas ou na janela de configurações da tarefa de instalação remota.

Ao tratar das políticas de grupo do Windows através do Kaspersky Security Center, você pode especificar dispositivos para um objeto de política de grupo criando um grupo de segurança. O Kaspersky Security Center sincroniza o conteúdo do grupo de segurança com o conjunto atual de dispositivos na tarefa. Usando outras ferramentas para tratar políticas de grupo, você pode associar objetos de políticas de grupo com UOs selecionadas diretamente do Active Directory.

Instalação não assistida de aplicativos através das políticas do Microsoft Windows

O administrador pode criar os objetos necessários para a instalação em uma política de grupo do Windows em seu nome. Neste caso, ele ou ela pode fornecer links para os pacotes armazenados na pasta compartilhada do Kaspersky Security Center, ou carregar aqueles pacotes para um servidor de arquivos dedicado e então fornecer-lhes os links.

Os seguintes cenários de instalação são possíveis:

- O administrador cria um pacote de instalação e define suas propriedades no Console de Administração. O objeto de política de grupo fornece um link para o arquivo MSI deste pacote armazenado na pasta compartilhada do Kaspersky Security Center.

- O administrador cria um pacote de instalação e define suas propriedades no Console de Administração. Então o administrador copia a toda a subpasta EXEC deste pacote da pasta compartilhada do Kaspersky Security Center para uma pasta em um recurso de arquivo dedicado da organização. O objeto da política de grupo fornece um link para o arquivo MSI deste pacote armazenado em uma subpasta no recurso de arquivo dedicado da organização.

- O administrador baixa o pacote de distribuição do aplicativo (incluindo o do Agente de Rede) da Internet e carrega ele no recurso de arquivo dedicado da organização. O objeto da política de grupo fornece um link para o arquivo MSI deste pacote armazenado em uma subpasta no recurso de arquivo dedicado da organização. As configurações de instalação são definidas ao configurar as propriedades MSI ou ao configurar os arquivos de transformação MST.

Implementação forçada através da tarefa de instalação remota do Kaspersky Security Center

Para executar a implementação inicial do Agente de Rede ou outros aplicativos, é possível forçar a instalação de pacotes de instalação selecionados por meio do uso da tarefa de instalação remota do Kaspersky Security Center, desde que cada dispositivo tenha uma ou mais contas de usuário com direitos de administrador local.

A instalação forçada também pode ser aplicada se os dispositivos não puderem ser diretamente acessados pelo Servidor de Administração: por exemplo, os dispositivos estão em redes isoladas ou estão em uma rede local, enquanto o item Servidor de Administração está na DMZ.

No caso de implementação inicial, o Agente de Rede não é instalado. Portanto, nas configurações da tarefa de instalação remota, não é possível selecionar a distribuição dos arquivos necessários para a instalação do aplicativo com o uso do Agente de Rede. Você só pode optar por distribuir arquivos usando recursos do sistema operacional por meio do Servidor de Administração ou pontos de distribuição.

O serviço do Servidor de Administração deve ser executado em uma conta que tenha privilégios administrativos nos dispositivos de destino. Como alternativa, é possível especificar uma conta que tenha acesso ao compartilhamento admin$ nas configurações da tarefa de instalação remota.

Por padrão, a tarefa de instalação remota é aplicada aos dispositivos usando as credenciais da conta sob a qual o Servidor de Administração está sendo executado. É importante esclarecer que esta é a conta usada para acessar o compartilhamento admin$, e não a conta na qual a tarefa de instalação remota é executada. A instalação será realizada na conta LocalSystem.

É possível especificar dispositivos de destino explicitamente (com uma lista), por meio de seleção do grupo de administração do Kaspersky Security Center ao qual eles pertencem ou por meio de criação de uma seleção de dispositivos com base em um critério específico. A hora início da instalação é definida pelo agendamento da tarefa. Caso a configuração **Executar tarefas ignoradas** esteja ativada nas propriedades da tarefa, a tarefa poderá ser executada imediatamente após os dispositivos de destino serem ligados ou quando eles forem movidos para o grupo de administração de destino.

A instalação forçada consiste em entregar pacotes de instalação aos dispositivos de destino, cópia subsequente de arquivos para o recurso admin$ em cada um dos dispositivos de destino e registro remoto de serviços de suporte nesses dispositivos. A entrega de pacotes de instalação a dispositivos-alvo é executada por meio de um recurso do Kaspersky Security Center que garante a interação da rede. As seguintes condições devem ser atendidas neste caso:

- Os dispositivos de destino podem ser acessados no lado do Servidor de Administração ou no lado do ponto de distribuição.
- A resolução de nomes para dispositivos de destino funciona corretamente na rede.
- Os compartilhamentos administrativos (admin$) permanecem ativados nos dispositivos-alvo.
- Os seguintes serviços do sistema estão em execução nos dispositivos de destino:
  - Server (LanmanServer)

    Por padrão, este serviço está em execução.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- A porta TCP 445 está aberta nos dispositivos de destino para permitir acesso remoto por meio do Instrumentação de Gerenciamento do Windows (WMI).

  Os protocolos TCP 139, UDP 137 e UDP 138 são usados por protocolos mais antigos e não são mais necessários para aplicativos atuais.

  Portas de acesso de saída dinâmicas devem ser permitidas no firewall para conexões do Servidor de Administração e pontos de distribuição para dispositivos de destino.
- As configurações de segurança da política de domínio do Active Directory têm permissão para fornecer a operação do protocolo NTLM durante a implementação do Agente de Rede.
- Em dispositivos-alvo que executam o Microsoft Windows XP, o modo Compartilhamento Simples de Arquivo está desativado.
- Nos dispositivos de destino, o compartilhamento de acesso e o modelo de segurança são definidos como *Clássico: os usuários locais se autenticam como eles mesmos*. Ele não pode de forma alguma ser *apenas Visitante: os usuários locais são autenticados como Visitantes*.
- Os dispositivos-alvo são membros do domínio, ou as contas uniformes com direitos de administrador são criadas nos dispositivos-alvo com antecedência.

Para implementar com sucesso o Agente de Rede ou outros aplicativos em um dispositivo que não esteja associado a um domínio do Active Directory do Windows Server 2003 ou posterior, é necessário desativar o UAC remoto nesse dispositivo. O UAC remoto é um dos motivos que impedem que contas administrativas locais acessem admin$, o que é necessário para a implementação forçada do Agente de Rede ou de outros aplicativos. A desativação do UAC remoto não afeta o UAC local.

Durante a instalação em novos dispositivos que ainda não foram alocados à nenhum dos grupos de administração do Kaspersky Security Center, você pode abrir as propriedades da tarefa de instalação remota e especificar o grupo de administração para o qual os dispositivos serão movidos após a instalação do Agente de Rede.

Ao criar uma tarefa de grupo, tenha em mente que cada tarefa de grupo afeta todos os dispositivos em todos os grupos aninhados dentro de um grupo selecionado. Portanto, você deve evitar duplicar tarefas de instalação em subgrupos.

Uma maneira simplificada de criar tarefas para a instalação forçada de aplicativos é a instalação automática. Para fazer isso, você deve abrir as propriedades do grupo de administração, abrir a lista de pacotes de instalação e selecionar aqueles que devem ser instalados nos dispositivos deste grupo. Como resultado, os pacotes de instalação selecionados serão automaticamente instalados em todos os dispositivos neste grupo e em todos os seus subgrupos. O intervalo de tempo sobre o qual os pacotes serão instalados depende da produtividade da rede e o número total de dispositivos na rede.

Para reduzir a carga no Servidor de Administração durante a entrega de pacotes de instalação a dispositivos-alvo, é possível selecionar a instalação por meio dos pontos de distribuição na tarefa de instalação. Observe que este método de instalação coloca uma carga significativa nos dispositivos que atuam como pontos de distribuição. Portanto, é recomendável selecionar os dispositivos que atendam aos requisitos para pontos de distribuição. Se você usar pontos de distribuição, precisará garantir que eles estejam presentes em cada uma das sub-redes isoladas que hospedam os dispositivos de destino.

Usando pontos de distribuição como centros de instalação locais também pode ser útil ao executar a instalação em dispositivos em sub-redes comunicadas com o Servidor de Administração através de um canal de baixa potência enquanto um canal mais amplo esteja disponível entre os dispositivos na mesma sub-rede.

O espaço livre em disco na partição com a pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit deve exceder muitas vezes o tamanho total dos pacotes de distribuição dos aplicativos instalados.

Executar pacotes independentes criados pelo Kaspersky Security Center

Os métodos acima descritos da implementação inicial do Agente de Rede e de outros aplicativos nem sempre podem ser implementados porque não é possível atender todas as condições aplicáveis. Em tais casos, você pode criar um arquivo executável comum denominado como *pacote de instalação independente* através do Kaspersky Security Center, usando pacotes de instalação com as configurações de instalação relevantes que foram preparados pelo administrador. O pacote de instalação independente é armazenado na pasta compartilhada do Kaspersky Security Center.

Você pode usar o Kaspersky Security Center para enviar aos usuários selecionados uma mensagem de e-mail contendo um link à este arquivo na pasta compartilhada, solicitando-lhes que executem o arquivo (no modo interativo ou com a chave "-s" para a instalação silenciosa). Você pode anexar o pacote de instalação independente a uma mensagem de e-mail e então enviá-la aos usuários de dispositivos que não tenham acesso à pasta compartilhada do Kaspersky Security Center. O administrador também pode copiar o pacote independente em uma unidade removível, entregá-lo a um dispositivo relevante e, em seguida, executá-lo mais tarde.

Você pode criar um pacote independente a partir de um pacote de Agente de Rede, de um pacote de outro aplicativo (por exemplo, o aplicativo de segurança), ou ambos. Se o pacote independente foi criado a partir do Agente de Rede e de outro aplicativo, a instalação inicia com o Agente de Rede.

Ao criar um pacote independente com o Agente de Rede, você pode especificar o grupo de administração ao qual os novos dispositivos (aqueles que não foram alocados à nenhum dos grupos de administração) serão automaticamente movidos quando a instalação do Agente de Rede for concluída neles.

Os pacotes independentes podem ser executados no modo interativo (por padrão), exibindo o resultado da instalação de aplicativos que eles contêm, ou eles podem ser executados no modo silencioso (quando executados com a chave "-s"). O modo silencioso pode ser usado para a instalação de scripts, por exemplo, de scripts configurados para ser executados após a implementação da imagem do sistema operacional. O resultado da instalação no modo silencioso é determinado pelo código de retorno do processo.

O Agente de Rede independente para Linux tem uma dependência opcional da ferramenta nmap. Se o utilitário nmap estiver ausente ou for anterior à versão 6.0, a funcionalidade Broadcast DHCP Discover não será compatível.

Opções para a instalação manual de aplicativos

Os administradores ou os usuários experientes podem instalar os aplicativos manualmente no modo interativo. Eles podem usar pacotes de distribuição originais ou pacotes de instalação gerados a partir deles e armazenados na pasta compartilhada do Kaspersky Security Center. Por padrão, instaladores são executados no modo interativo e solicitam aos usuários todos os valores necessários. No entanto, ao executar o processo setup.exe a partir da raiz de um pacote de instalação com a chave "-s", o instalador será executado no modo silencioso e com as configurações que foram definidas ao configurar o pacote de instalação.

Ao executar o setup.exe a partir da raiz de um pacote de instalação armazenado na pasta compartilhada do Kaspersky Security Center, o pacote será primeiro copiado para uma pasta local temporária e, a seguir, o instalador do aplicativo será executado a partir da pasta local.

Como criar um arquivo MST

Para transformar o conteúdo de um pacote MSI e aplicar configurações personalizadas a um arquivo MSI existente, você deve criar um arquivo de transformação no formato MST. Para isso, use o editor Orca.exe, incluído no SDK do Windows.

Para criar um arquivo MST:

1. Execute o editor Orca.exe.
2. Acesse a guia **Arquivo** e, no menu, clique em **Abrir**.
3. Selecione o arquivo Kaspersky Network Agent.msi.
4. Acesse a guia **Transformação** e, no menu, selecione **Nova transformação**.
5. Na coluna **Tabelas**, selecione **Propriedade** e escreva os seguintes valores:
   - *EULA=1*
   - *SERVERADDRESS=<endereço do Servidor de Administração>*

   Clique no botão **Salvar**.
6. Acesse a guia **Transformar** e, no menu, selecione **Gerar transformação**.
7. Na janela exibida, especifique um nome do arquivo de transformação criado e clique no botão **Salvar**.

O arquivo MST é salvo.

Instalação remota de aplicativos em dispositivos com o Agente de Rede instalado

Se um Agente de Rede operável conectado ao Servidor de Administração principal (ou a algum dos seus Servidores secundários) for instalado em um dispositivo, você poderá fazer um upgrade do Agente de Rede neste dispositivo, assim como instalar, atualizar ou remover qualquer aplicativo compatível através do Agente de Rede.

Você pode ativar a opção **Usando o Agente de Rede** nas propriedades da tarefa de instalação remota.

Se esta opção estiver selecionada, os pacotes de instalação com configurações de instalação definidas pelo administrador serão transferidos para os dispositivos alvo através dos canais de comunicação entre o Agente de Rede e o Servidor de Administração.

Para otimizar a carga do Servidor de Administração e minimizar o tráfego entre o Servidor de Administração e os dispositivos, é útil atribuir pontos de distribuição em cada rede remota ou em cada domínio emissor (consulte as seções "Sobre os pontos de distribuição" e "Criar uma estrutura de grupos de administração e atribuir pontos de distribuição"). Neste caso, os pacotes de instalação e as configurações do instalador são distribuídos a partir do Servidor de Administração para os dispositivos alvo através de pontos de distribuição.

Além disso, você pode usar pontos de distribuição para transmitir (multicast) a entrega de pacotes de instalação, que permite reduzir significativamente o tráfego de rede ao implementar aplicativos.

Ao transferir pacotes de instalação para dispositivos alvo através dos canais de comunicação entre os Agentes de Rede e o Servidor de Administração, todos os pacotes de instalação que tenham sido preparados para transferência, também serão colocados em cache na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Ao usar múltiplos grandes pacotes de instalação de vários tipos e ao envolver um grande número de pontos de distribuição, o tamanho desta pasta pode aumentar drasticamente.

Os arquivos não podem ser excluídos da pasta FTServer manualmente. Quando os pacotes de instalação originais forem excluídos, os dados correspondentes serão automaticamente excluídos da pasta FTServer.

Os dados recebidos por pontos de distribuição são salvos na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Os arquivos não podem ser excluídos da pasta de $FTCITmp manualmente. Quando as tarefas usando dados desta pasta forem concluídas, o conteúdo desta pasta será automaticamente excluído.

Como os pacotes de instalação são distribuídos sobre os canais de comunicação entre o Servidor de Administração e os Agentes de Rede a partir de um repositório intermediário em um formato otimizado para transferências na rede, nenhuma modificação é permitida nos pacotes de instalação armazenados na pasta original de cada pacote de instalação. Estas modificações não serão automaticamente registradas pelo Servidor de Administração. Se você tiver de modificar os arquivos de pacotes de instalação manualmente (embora seja recomendado evitar este cenário), deverá editar qualquer configuração necessária de um pacote de instalação no Console de Administração. Editar as configurações de um pacote de instalação no Console de Administração faz com que o Servidor de Administração atualize a imagem do pacote na memória no cache que foi preparado para a transferência aos dispositivos alvo.

O gerenciamento do dispositivo reinicia na tarefa de instalação remota

Os dispositivos muitas vezes precisam de um reinício para concluir a instalação remota de aplicativos (em particular no Windows).

Caso a tarefa de instalação remota do Kaspersky Security Center seja usada, no assistente para novas tarefas ou na janela de propriedades da tarefa que foi criada (seção **Reinício do sistema operacional**), será possível selecionar a ação a ser executada quando o dispositivo Windows precisar ser reiniciado:

- **Não reiniciar o dispositivo**. Neste caso, nenhum reinício automático será executado. Para concluir a instalação, você deve reiniciar o dispositivo (por exemplo, manualmente ou através da tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário serão salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas de instalação em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**. Neste caso, o dispositivo sempre é reiniciado automaticamente se um reinício for necessário para a conclusão da instalação. Esta opção é útil para tarefas de instalação em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**. Neste caso, o lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). A opção **Perguntar ao usuário o que fazer** é a mais adequada para estações de trabalho onde os usuários precisam da possibilidade de selecionar a hora mais conveniente para um reinício.

Adequabilidade da atualização dos bancos de dados em um pacote de instalação de um aplicativo de segurança

Antes de iniciar a implementação da proteção, você deve ter em mente a possibilidade de atualizar os bancos de dados antivírus (incluindo os módulos de patches automáticas), fornecidos junto com o pacote de distribuição do aplicativo de segurança. É útil atualizar os bancos de dados no pacote de instalação do aplicativo antes de iniciar a implementação (por exemplo, usando o comando correspondente no menu de contexto de um pacote de instalação selecionado). Isto reduzirá o número de reinícios necessários para a conclusão da implementação da proteção em dispositivos alvo.

Usar as ferramentas da instalação remota de aplicativos no Kaspersky Security Center para executar arquivos executáveis relevantes em dispositivos gerenciados

Usando o Assistente de novo pacote, você pode selecionar qualquer arquivo executável e definir as configurações da linha de comando para ele. Para isto você pode adicionar ao pacote de instalação o próprio arquivo selecionado ou a pasta inteira na qual este arquivo está armazenado. Então você deve criar a tarefa de instalação remota e selecionar o pacote de instalação que foi criado.

Enquanto a tarefa estiver em execução, o arquivo executável especificado com as configurações definidas do prompt de comando serão executadas em dispositivos alvo.

Se você usar instaladores no formato do Microsoft Windows Installer (MSI), o Kaspersky Security Center analisa os resultados da instalação por meio de ferramentas padrão.

Se a licença do Gerenciamento de patches e vulnerabilidades estiver disponível, o Kaspersky Security Center (ao criar um pacote de instalação de qualquer aplicativo suportado no ambiente corporativo), também usa as regras para a instalação e análise dos resultados de instalação que estão no seu banco de dados atualizável.

De outra forma, a tarefa padrão para arquivos executáveis espera pela conclusão do processo de execução e de todos os seus processos secundários. Após a conclusão de todos os processos em execução, a tarefa será concluída dom êxito a despeito do código de retorno do processo inicial. Para modificar tal comportamento desta tarefa, antes de criar a tarefa, você deve modificar manualmente os arquivos .kpd gerados pelo Kaspersky Security Center na pasta do pacote de instalação recentemente criado e suas subpastas.

Os arquivos .kpd usam codificação ASCII. Os arquivos .kud usam codificação Unicode.

Para que a tarefa não espere pela conclusão do processo em execução, defina o valor da configuração Wait como 0 na seção [SetupProcessResult]:

```
[SetupProcessResult]
Wait=0
```

Para a tarefa somente esperar pela conclusão do processo em execução no Windows, não para a conclusão de todos os processos secundários, defina o valor da configuração WaitJob como 0 na seção [SetupProcessResult], por exemplo:

```
[SetupProcessResult]
WaitJob=0
```

Para que a tarefa seja concluída com sucesso ou retorne um erro dependendo do código de retorno do processo em execução, crie um arquivo executável .bat que salve o código de erro em um arquivo, por exemplo:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

E, depois, modifique os arquivos .kud que foram gerados pelo Kaspersky Security Center na pasta do pacote de instalação recém-criado:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Instalação concluída com êxito.
[SetupMainResult_ErrorCodes]
1=Erro de script de instalação
2=Erro personalizado
```

Neste caso, qualquer outro código que os dos listados resultará em um erro retornado.

Para exibir uma sequência de caracteres com um comentário sobre a conclusão bem sucedida da tarefa ou sobre um erro nos resultados da tarefa, insira breves descrições dos erros que correspondem aos códigos de retorno do processo na seção [SetupProcessResult_SuccessCodes] e [SetupProcessResult_ErrorCodes], por exemplo:

```
[SetupProcessResult_SuccessCodes]
0 = Instalação concluída com êxito
3010=Um reinício é necessário para concluir a instalação
[SetupProcessResult_ErrorCodes]
```

```
1602=Instalação cancelada pelo usuário
1603=Erro fatal durante a instalação
```

Para usar as ferramentas do Kaspersky Security Center para gerenciar o reinício do dispositivo (se um reinício for necessário para concluir uma operação), liste os códigos de retorno do processo que indicam que um reinício deve ser executado, na seção [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
3010=
```

Monitorar a implementação

Para monitorar a implementação do Kaspersky Security Center e assegurar-se de que um aplicativo de segurança e um Agente de Rede sejam instalados nos dispositivos gerenciados, você deve verificar o sinal luminoso na seção **Implementação**. Este sinal luminoso está localizado no espaço de trabalho do nó Servidor de Administração na janela principal do Console de Administração. O sinal luminoso reflete o status da implementação atual. O número de dispositivos com Agente de Rede e aplicativos de segurança instalados é exibido ao lado do sinal luminoso. Quando qualquer tarefa de instalação estiver em execução, você pode monitorar aqui seu andamento. Se algum erro de instalação ocorrer, o número de erros é aqui exibido. Você pode exibir os detalhes de qualquer erro clicando no link.

Você também pode usar o esquema de implementação no espaço de trabalho da pasta **Dispositivos gerenciados** na guia **Grupos**. O gráfico reflete o processo de implementação, mostrando o número de dispositivos sem o Agente de Rede, com o Agente de Rede, ou com o Agente de Rede e um aplicativo de segurança.

Para obter mais detalhes sobre o andamento da implementação (ou da operação de uma tarefa de instalação específica) abra a janela de resultados da tarefa de instalação remota relevante: clique com o botão direito do mouse na tarefa e selecione **Resultados** no menu de contexto. A janela exibe duas listas: a superior contém os status da tarefa em dispositivos, enquanto a mais baixa contém os eventos de tarefas no dispositivo que está atualmente selecionado na lista superior.

As informações sobre erros de implementação são adicionadas ao Log de Eventos Kaspersky no Servidor de Administração. As informações sobre os erros também estão disponíveis por meio da seleção do evento correspondente no nó Servidor de Administração na guia **Eventos**.

Configurar os instaladores

Esta seção fornece informações sobre os arquivos de instaladores do Kaspersky Security Center e as configurações de instalação, assim como recomendações sobre como instalar o Servidor de Administração e o Agente de Rede no modo silencioso.

Informações gerais

Os Instaladores dos componentes do Kaspersky Security Center 14.2 (Servidor de Administração, Agente de Rede e Console de Administração) são desenvolvidos com base na tecnologia do Windows Installer. Um pacote MSI é o núcleo de um instalador. Este formato de empacotar permite usar todas das vantagens fornecidas pelo Windows Installer: dimensionalidade, disponibilidade de um sistema de correção, sistema de transformação, instalação centralizada através de soluções de terceiros e o registro transparente com o sistema operacional.

Instalação em modo silencioso (com um arquivo de resposta)

Os instaladores do Servidor de Administração e do Agente de Rede têm o recurso de funcionar com o arquivo de resposta (ss_install.xml), onde os parâmetros para a instalação no modo silencioso sem a participação de usuário estão integradas. O arquivo ss_install.xml está localizado na mesma pasta que o pacote MSI; ele é usado automaticamente durante a instalação no modo silencioso. Você pode ativar o modo de instalação silenciosa com a tecla de linha de comando "/s".

Uma visão geral de uma execução de exemplo segue:

```
setup.exe /s
```

Antes de iniciar o instalador no modo silencioso, leia o Contrato de Licença do Usuário Final (EULA). Caso o kit de distribuição do Kaspersky Security Center não inclua um arquivo TXT com o texto do EULA, é possível baixá-lo no site da Kaspersky.

O arquivo ss_install.xml é uma instância do formato interno dos parâmetros do instalador do Kaspersky Security Center. Os pacotes de distribuição contêm o arquivo ss_install.xml com os parâmetros padrão.

Não modifique manualmente o arquivo ss_install.xml. Este arquivo pode ser modificado pelas ferramentas do Kaspersky Security Center ao editar os parâmetros de pacotes de instalação no Console de Administração.

Para modificar o arquivo de resposta para instalação do Servidor de Administração:

1. Abra o pacote de distribuição do Kaspersky Security Center. Caso use um pacote completo com arquivo EXE, é necessário descompactá-lo.
2. A partir da pasta Servidor, abra a linha de comando e, em seguida, execute o seguinte comando:

   ```
   setup.exe /r ss_install.xml
   ```

   O instalador do Kaspersky Security Center é iniciado.
3. Siga as etapas do assistente para configurar a instalação do Kaspersky Security Center.

   Ao concluir o assistente, o arquivo de resposta é modificado automaticamente de acordo com as novas configurações especificadas.

Instalação do Agente de Rede no modo silencioso (sem um arquivo de resposta)

Você pode instalar o Agente de Rede com um pacote .msi único, especificando os valores das propriedades MSI no modo padrão. Este cenário permite que o Agente de Rede seja instalado usando políticas de grupo.

Não renomeie o pacote de instalação Kaspersky Network Agent.msi. Renomear este pacote pode causar erros de instalação durante futuras atualizações do Agente de Rede.

Para evitar conflitos entre configurações definidas através dos parâmetros MSI e os parâmetros definidos no arquivo de resposta, você pode desativar o arquivo de resposta ao definir a propriedade `DONT_USE_ANSWER_FILE=1`. O arquivo MSI está localizado no pacote de distribuição do Kaspersky Security Center, na pasta Packages\NetAgent\exec. Um exemplo de uma execução do instalador do Agente de Rede com um pacote .msi é como segue.

A instalação do Agente de Rede no modo silencioso requer o aceite dos termos do Contrato de Licença de Usuário Final. Use o parâmetro `EULA=1` somente se você tiver lido, entende e aceita por completo os termos do Contrato de Licença do Usuário Final.

Exemplo:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Você também pode definir os parâmetros de instalação para um pacote .msi ao preparar o arquivo de resposta com antecedência (um com uma extensão .mst). Este comando aparece como segue:

Exemplo:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

Você pode especificar vários arquivos de resposta em um comando único.

Se você quiser atualizar o Agente de Rede usando o Windows Installer, execute o seguinte comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Configuração de instalação parcial através de setup.exe

Ao executar a instalação de aplicativos por meio do setup.exe, é possível adicionar os valores de qualquer propriedade de MSI ao pacote MSI.

Este comando aparece como segue:

Exemplo:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parâmetros de instalação do Servidor de Administração

A tabela abaixo descreve as propriedades MSI que você pode configurar ao instalar o Servidor de Administração. Todos os parâmetros são opcionais, exceto para o EULA e PRIVACYPOLICY.

Parâmetros da instalação do Servidor de Administração no modo silencioso

Propriedade de MSI	Descrição	Valores disponíveis
EULA	Aceitação dos termos do Contrato de Licença (necessária)	• 1 – Eu li, entendo e aceito por completo os termos do Contrato de Licença do Usuário Final. • Outro valor ou nenhum valor – Não aceito os termos do Contrato de Licença (a instalação não é executada).
PRIVACYPOLICY	Aceitação dos termos da Política de Privacidade (necessária)	• 1 – Estou ciente e concordo que meus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade. Confirmo que Eu li e entendo por completo a Política de Privacidade. • Outro valor ou nenhum valor – Não aceito os termos da Política de Privacidade (a instalação não é executada).

Propriedade de MSI	Descrição	Valores disponíveis
INSTALLATIONMODETYPE	Tipo de instalação do Servidor de Administração	• Padrão. • Personalizado.
INSTALLDIR	Pasta de instalação do aplicativo	Valor da sequência de caracteres.
ADDLOCAL	Lista de componentes para instalar (separado por vírgulas)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Lista mínima de componentes suficientes para a instalação correta do Servidor de Administração: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Tamanho da rede	• NRT_1_100 – De 1 a 100 dispositivos. • NRT_100_1000 – De 101 a 1000 dispositivos. • NRT_GREATER_1000 – Mais de 1000 dispositivos.
SRV_ACCOUNT_TYPE	Modo de especificar o usuário para a operação do serviço Servidor de Administração	• SrvAccountDefault – A conta de usuário será criada automaticamente. • SrvAccountUser – A conta de usuário é definida manualmente.
SERVERACCOUNTNAME	Nome do usuário para o serviço	Valor da sequência de caracteres.
SERVERACCOUNTPWD	Senha de usuário para o serviço	Valor da sequência de caracteres.
DBTYPE	Tipo de banco de dados	• MySQL – Um banco de dados MySQL ou MariaDB será usado. • MSSQL – Um banco de dados do Microsoft SQL Server (SQL Express) será usado.
MYSQLSERVERNAME	Nome completo do servidor MySQL ou MariaDB	Valor da sequência de caracteres.
MYSQLSERVERPORT	Número de uma porta para conexão ao MySQL Server ou MariaDB	Valor numérico.
MYSQLDBNAME	Nome do banco de dados do MySQL Server ou MariaDB	Valor da sequência de caracteres.
MYSQLACCOUNTNAME	Nome do usuário para a conexão ao banco de dados do MySQL Server ou MariaDB	Valor da sequência de caracteres.
MYSQLACCOUNTPWD	Senha do usuário para a conexão ao banco de dados do MySQL Server ou MariaDB	Valor da sequência de caracteres.
MSSQLCONNECTIONTYPE	Tipo de uso do banco de dados MSSQL	• InstallMSSEE – Instalar a partir de um pacote. • ChooseExisting – Usar o servidor instalado.
MSSQLSERVERNAME	Nome completo da instância do SQL Server	Valor da sequência de caracteres.
MSSQLDBNAME	Nome do banco de dados do SQL Server	Valor da sequência de caracteres.
MSSQLAUTHTYPE	Método de autenticação para a conexão ao SQL Server	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nome do usuário para a conexão ao SQL Server no modo SQLServer	Valor da sequência de caracteres.
MSSQLACCOUNTPWD	Senha do usuário para a conexão ao SQL Server no modo SQLServer	Valor da sequência de caracteres.

Propriedade de MSI	Descrição	Valores disponíveis

CREATE_SHARE_TYPE	Método para especificar a pasta compartilhada	• Create – Criar uma nova pasta compartilhada. Neste caso, as seguintes propriedades devem ser definidas:
		  • SHARELOCALPATH – Caminho a uma pasta local.
		  • SHAREFOLDERNAME – Nome da rede de uma pasta.
		• Null – A propriedade EXISTSHAREFOLDERNAME deve ser especificada.

EXISTSHAREFOLDERNAME	Caminho completo para uma pasta compartilhada existente	Valor da sequência de caracteres.
SERVERPORT	O número da porta usado para conectar ao Servidor de Administração	Valor numérico.
SERVERSSLPORT	Número de uma porta para estabelecer a conexão SSL ao Servidor de Administração	Valor numérico.
SERVERADDRESS	Administration Server address	Valor da sequência de caracteres.
SERVERCERT2048BITS	Tamanho da chave para o certificado do Servidor de Administração (bits)	• 1 – O tamanho da chave para o certificado do Servidor de Administração é de 2048 bits. • 0 – O tamanho da chave para o certificado do Servidor de Administração é de 1024 bits. • Se nenhum valor for especificado – O tamanho da chave para o certificado do Servidor de Administração é de 2048 bits.
MOBILESERVERADDRESS	Endereço do Servidor de Administração para a conexão de dispositivos móveis; ignorado se o componente MobileSupport não foi selecionado	Valor da sequência de caracteres.

Parâmetros de instalação do Agente de Rede

A tabela abaixo descreve as propriedades MSI que você pode configurar ao instalar o Agente de Rede. Todos os parâmetros são opcionais, exceto para o EULA e SERVERADDRESS.

Parâmetros da instalação do Agente de Rede no modo silencioso

Propriedade de MSI	Descrição	Valores disponíveis
EULA	Aceitação dos termos do Contrato de Licença	• 1 – Confirmo que li, entendi e aceito totalmente os termos e condições deste Contrato de Licença de Usuário Final. • 0 – Eu não aceito os termos do Contrato de Licença (a instalação não é executada). • Nenhum valor – Eu não aceito os termos do Contrato de Licença (a instalação não é executada).
DONT_USE_ANSWER_FILE	Ler as configurações de instalação a partir do arquivo de resposta	• 1 – Não usar. • Outro valor ou sem valor – Leitura.
INSTALLDIR	Caminho para a pasta de instalação do Agente de Rede	Valor da sequência de caracteres.
SERVERADDRESS	Endereço do Servidor de Administração (necessário)	Valor da sequência de caracteres.
SERVERPORT	Número de uma porta para conexão ao Servidor de Administração	Valor numérico.
SERVERSSLPORT	Número da porta para a conexão criptografada ao Servidor de Administração usando protocolo SSL	Valor numérico.

Propriedade de MSI	Descrição	Valores disponíveis
USESSL	Decida se deseja usar uma conexão SSL	• 1 – Usar. • Outro valor ou sem valor – Não usar.
OPENUDPPORT	Decida se deseja abrir uma porta UDP	• 1 – Abrir. • Outro valor ou sem valor – Não abrir.
UDPPORT	Número da porta UDP	Valor numérico.
USEPROXY	Se um servidor proxy deve ser usado. Para fins de compatibilidade, não é recomendável especificar as configurações de conexão proxy nas configurações do pacote de instalação do Agente de Rede.	• 1 – Usar. • Outro valor ou sem valor – Não usar.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Endereços de proxy e número de uma porta para conexão ao servidor de proxy	Valor da sequência de caracteres.
PROXYLOGIN	Conta para a conexão ao servidor proxy	Valor da sequência de caracteres.
PROXYPASSWORD	Senha da conta para conexão ao servidor proxy (Não especifique nenhum detalhe de contas privilegiadas nos parâmetros dos pacotes de instalação.)	Valor da sequência de caracteres.
GATEWAYMODE	Modo de uso do gateway de conexão	• 0 – Não usar gateway de conexão. • 1 – Usar este Agente de Rede como gateway de conexão. • 2 – Conectar-se ao Servidor de Administração usando o gateway de conexão.
GATEWAYADDRESS	Endereço gateway-conexão	Valor da sequência de caracteres.
CERTSELECTION	Método para receber um certificado	• GetOnFirstConnection – Receber um certificado a partir do Servidor de Administração. • GetExistent – Selecionar um certificado existente; se esta opção estiver selecionada, a propriedade CERTFILE deve ser especificada.
CERTFILE	Caminho para o arquivo do certificado	Valor da sequência de caracteres.
VMVDI	Ativar o modo dinâmico para a Virtual Desktop Infrastructure (VDI)	• 1 – Ativar. • 0 - Não ativar. • Sem valor – Não ativar.
VMOPTIMIZE	Define as configurações do Agente de Rede são ideais para o hypervisor	• 1 – Ativar. • 0 - Não ativar. • Sem valor – Não ativar.
LAUNCHPROGRAM	Decida se deseja iniciar o serviço Agente de Rede após a instalação. O parâmetro é ignorado se VMVDI=1	• 1 – Iniciar. • Outro valor ou sem valor – Não iniciar.
NAGENTTAGS	Tag para o Agente de Rede (tem prioridade sobre a tag fornecida no arquivo de resposta)	Valor da sequência de caracteres.

Infraestrutura virtual

O Kaspersky Security Center é compatível com o uso de máquinas virtuais. Você pode instalar o Agente de Rede e do aplicativo de segurança em cada máquina virtual, assim como a proteção de máquinas virtuais em nível de hipervisor. No primeiro caso, você pode usar o aplicativo de segurança padrão ou o Kaspersky Security for Virtualization Light Agent para proteger suas máquinas virtuais. No segundo caso, você pode usar o Kaspersky Security for Virtualization Agentless.

O Kaspersky Security Center comporta reversões de máquinas virtuais ao estado anterior.

Dicas sobre como reduzir a carga em máquinas virtuais

Ao instalar o Agente de Rede em uma máquina virtual, você é aconselhado a considerar a desativação de alguns recursos do Kaspersky Security Center que parecem ser de um pouco uso para máquinas virtuais.

Ao instalar o Agente de Rede em uma máquina virtual ou em um modelo destinado para a geração de máquinas virtuais, recomendamos executar as seguintes ações:

- Se estiver executando uma instalação remota, na janela Propriedades do pacote de instalação do Agente de Rede na seção **Avançado**, selecione a opção **Otimizar as configurações para VDI**.
- Se você estiver executando uma instalação interativa por meio de um assistente, na janela assistente, selecione a opção **Otimizar as configurações do Agente de Rede para a infraestrutura virtual**.

Selecionar essas opções alterará as configurações do Agente de Rede para que os seguintes recursos permaneçam desativados por padrão (antes da política ser aplicada):

- Recuperar informações sobre o software instalado
- Recuperar informações sobre o hardware
- Recuperar informações sobre as vulnerabilidades detectadas
- Recuperar informações sobre as atualizações necessárias

Normalmente, aqueles recursos não são necessários em máquinas virtuais porque elas usam o software uniforme e o hardware virtual.

A desativação dos recursos é irreversível. Se algum dos recursos desativados for necessário, você pode ativá-lo através da política do Agente de Rede ou através das configurações locais do Agente de Rede. As configurações locais do Agente de Rede estão disponíveis através do menu de contexto do dispositivo relevante no Console de Administração.

Suporte de máquinas virtuais dinâmicas

O Kaspersky Security Center Cloud Console é compatível com as máquinas virtuais dinâmicas. Se uma infraestrutura virtual tiver sido implementada na rede da organização, as máquinas virtuais dinâmicas (temporárias) podem ser usadas em determinados casos. As VMs dinâmicas são criadas sob nomes únicos com base em um modelo que foi preparado pelo administrador. O usuário trabalha em uma VM durante algum tempo, então, depois ser desligada, esta máquina virtual será removida da infraestrutura virtual. Se o Kaspersky Security Center tiver sido implementado na rede da organização, uma máquina virtual com o Agente de Rede instalado será adicionada ao banco de dados do Servidor de Administração. Depois que você desliga uma máquina virtual, a entrada correspondente também deve ser removida do banco de dados do Servidor de Administração.

Para tornar funcional o recurso de remoção automática de entradas em máquinas virtuais, ao instalar o Agente de Rede em um modelo para máquinas virtuais dinâmicas, selecione a opção **Ativar modo dinâmico para VDI**:

- Para a instalação remota - na janela de propriedades do pacote de instalação do Agente de Rede (seção **Avançado**)
- Para a instalação interativa - No Assistente de instalação do Agente de Rede

Evite selecionar a opção **Ativar modo dinâmico para VDI** ao instalar o Agente de Rede em dispositivos físicos.

Se desejar que os eventos das máquinas virtuais dinâmicas sejam armazenados no Servidor de Administração durante algum tempo após essas máquinas virtuais serem removidas, então, na janela Propriedades do Servidor de Administração, na seção **Repositório de eventos**, selecione a opção **Armazenar eventos após a exclusão dos dispositivos** e especifique o período máximo de armazenamento para eventos (em dias).

Não recomendamos ativar a criptografia de unidade em máquinas virtuais dinâmicas.

Suporte para copiar máquinas virtuais

Copiar uma máquina virtual com o Agente de Rede instalado ou criar um a partir de um modelo com o Agente de Rede instalado, é idêntico a implementação de Agentes de Rede ao capturar e copiar uma imagem do disco rígido. Deste modo, no caso geral, ao copiar máquinas virtuais, você tem de executar as mesmas ações feitas ao implementar o Agente de Rede copiando uma imagem do disco.

No entanto, as duas caixas descritas abaixo apresentam o Agente de Rede que detecta a cópia automaticamente. Devido aos motivos acima, você não tem que executar as operações sofisticadas descritas sob "Implementar ao capturar e copiar o disco rígido de um dispositivo":

- A opção **Ativar modo dinâmico para VDI** foi selecionada durante a instalação do Agente de Rede. Após cada reinicialização do sistema operacional, esta máquina virtual será reconhecida como um novo dispositivo, independentemente de ter sido copiada ou não.
- Um dos seguintes hypervisors está em uso: VMware™, HyperV®, ou Xen®: o Agente de Rede detecta a cópia da máquina virtual através das IDs alteradas do hardware virtual.

A análise das modificações no hardware virtual não é absolutamente confiável. Antes de aplicar este método amplamente, você deve testá-lo em um pequeno conjunto de máquinas virtuais da versão do hypervisor atualmente usado na sua organização.

O suporte do sistema de arquivos reverte para dispositivos com o Agente de Rede

O Kaspersky Security Center é um aplicativo distribuído. Reverter o sistema de arquivos a um estado anterior em um dispositivo com o Agente de Rede instalado conduzirá a dessincronização e ao funcionamento impróprio do Kaspersky Security Center.

O sistema de arquivos (ou uma parte dele) pode ser revertido nos seguintes casos:

- Ao copiar uma imagem do disco rígido.
- Ao restaurar um estado da máquina virtual por meio da infraestrutura virtual.
- Ao restaurar os dados de uma cópia backup ou de um ponto de recuperação.

Os cenários sob os quais o software de terceiros nos dispositivos com o Agente de Rede instalado que afetam a pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ somente são cenários críticos para o Kaspersky Security Center. Portanto, você sempre deve excluir esta pasta do procedimento de recuperação, se possível.

Como as regras do local de trabalho de algumas organizações compreendem a possibilidade para a reversão do sistema de arquivos em dispositivos, o suporte para a reversão do sistema de arquivos em dispositivos com o Agente de Rede instalado foi adicionado ao Kaspersky Security Center, a partir da versão 10 Maintenance Release 1 (Servidor de Administração e os Agentes de Rede devem ser da versão 10 Maintenance Release 1 ou posterior). Quando detectado, estes dispositivos são automaticamente reconectados ao Servidor de Administração com a total limpeza dos dados e a total sincronização.

Por padrão, o suporte da reversão de detecção do sistema de arquivos está ativado no Kaspersky Security Center 14.2.

Tanto quanto possível, evite reverter a pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ nos dispositivos com o Agente de Rede instalado, porque a ressincronização completa dos dados requer uma grande quantidade de recursos.

A reversão do estado de sistema não é absolutamente permitida em um dispositivo com o Servidor de Administração instalado. A reversão do banco de dados também não é usada pelo Servidor de Administração.

Você pode restaurar um estado do Servidor de Administração a partir de uma cópia backup somente com o utilitário klbackup padrão.

Instalação local de aplicativos

Esta seção fornece um procedimento de instalação para aplicativos que somente podem ser instalados em dispositivos locais.

Para executar a instalação local de aplicativos em um dispositivo cliente específico, você deve ter direitos de administrador naquele dispositivo.

Para instalar aplicativos localmente em um dispositivo cliente específico:

1. Instale o Agente de Rede no dispositivo cliente e configure a conexão entre o dispositivo cliente e o Servidor de Administração.

2. Instale os aplicativos necessários no dispositivo, tal como descrito nos guias desses aplicativos.

3. Instale um plugin de gerenciamento para cada um dos aplicativos instalados na estação de trabalho do administrador.

O Kaspersky Security Center também suporta a opção de instalação local de aplicativos usando um pacote de instalação independente. O Kaspersky Security Center não é compatível com a instalação de todos os aplicativos da Kaspersky.

Instalação local do Agente de Rede

Para instalar o Agente de Rede em um dispositivo localmente:

1. No dispositivo, execute o arquivo setup.exe do pacote de distribuição baixado da Internet. Consulte o seguinte tópico para obter detalhes: Obtendo o pacote de instalação do Agente de Rede do kit de distribuição do Kaspersky Security Center.

   Uma janela é exibida, solicitando que você selecione os aplicativos Kaspersky para instalar.

2. Na janela de seleção do aplicativo, clique no link **Instalar somente o Agente de Rede do Kaspersky Security Center 14.2** para iniciar o Assistente de instalação do Agente de Rede. Siga as instruções do Assistente.

   a. **Servidor de Administração**

   Porta

   Especifica a porta não-SSL usada pelo Servidor de Administração para receber conexões dos Agentes de Rede.

   Por padrão, essa opção é definida como 14000.

   Porta SSL

   Especifica a porta SSL usada pelo Servidor de Administração para receber conexões dos Agentes de Rede.

   Por padrão, essa opção é definida como 13000.

   Usar SSL para conectar-se ao Servidor de Administração

   Se esta opção estiver ativada, a conexão com o Servidor de Administração é estabelecida através de uma porta segura via SSL.

   Por padrão, esta opção está ativada.

   Permitir que o Agente de Rede abra a porta UDP

   Caso esta opção esteja ativada, o instalador abre automaticamente a porta usada pelo Servidor de Administração para gerenciar o dispositivo cliente e receber as informações sobre ele.

   Por padrão, esta opção está ativada.

   Porta UDP

   Permite configurar a porta usada pelo Servidor de Administração para gerenciar o dispositivo cliente e receber as informações sobre ele.

   Por padrão, a opção é definida como 15000.

   b. **Configuração do servidor proxy**

Usar o servidor proxy

Caso esta opção esteja marcada, é possível especificar as credenciais para a autenticação do servidor proxy.

Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

Por padrão, esta opção está desativada.

Endereço

Porta

Conta

Nome do usuário sob o qual a conexão ao servidor proxy é estabelecida.

Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

Senha

Nome do usuário sob a qual a conexão ao servidor proxy é estabelecida.

Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

c. Gateway de conexão

Não usar o gateway de conexão

Usar o Agente de Rede como um gateway de conexão na DMZ

Selecione esta opção para usar o Agente de Rede como um gateway de conexão na zona desmilitarizada (DMZ) para se conectar com o Servidor de Administração, estabelecer comunicação com ele e manter os dados no Agente de Rede seguros durante a transmissão de dados.

Conectar-se ao Servidor de Administração usando o gateway de conexão

Selecione esta opção e especifique o dispositivo que atuará como gateway de conexão.

d. **Certificado do Servidor de Administração**

e. **Tags do agente**

f. Configurações avançadas

Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido

Recomendamos manter essa opção ativada. É possível desmarcar essa opção para desativar a atualização e aplicação de patch automáticas dos componentes do Kaspersky Security Center. O administrador pode reativar a atualização e a aplicação automáticas de patches mais tarde usando uma política.

Por padrão, esta opção está desativada.

Ativar proteção do serviço Agente de Rede

Quando esta opção estiver ativado, após o Agente de Rede ter sido instalado em um dispositivo gerenciado, o componente não poderá ser removido ou reconfigurado sem os privilégios necessários. O serviço Agente de Rede não pode ser interrompido. Essa opção não tem efeito nos controladores de domínio.

Ative esta opção para proteger o Agente de Rede em estações de trabalho operadas com direitos de administrador local.

Por padrão, esta opção está desativada.

Ativar modo dinâmico para VDI

Se esta opção estiver ativada, o modo dinâmico para a Infraestrutura de Virtual Desktop Infrastructure (VDI) será habilitado para o Agente de Rede instalado em uma máquina virtual.

Por padrão, esta opção está desativada.

Otimize as configurações do Agente de Rede do Kaspersky Security Center para a infraestrutura virtual. Desabilite a verificação de vulnerabilidades e o inventário de aplicativos e hardware. É possível editar as configurações atuais por meio das políticas do Agente de Rede.

Se esta opção estiver ativada, os seguintes recursos estarão desativados nas configurações do Agente de Rede:

- Recuperar informações sobre o software instalado
- Recuperar informações sobre o hardware
- Recuperar informações sobre as vulnerabilidades detectadas
- Recuperar informações sobre as atualizações necessárias

Por padrão, esta opção está desativada.

g. **Iniciar aplicativo**

Quando o Assistente de instalação for concluído, o Agente de Rede será instalado no dispositivo.

Você pode visualizar as propriedades do serviço do Agente de Rede do Kaspersky Security Center. Você pode ainda iniciar, interromper e monitorar a atividade do Agente de Rede através de ferramentas padrão do Microsoft Windows: Gerenciamento do computador\Serviços.

Instalar o Agente de Rede em modo silencioso

O Agente de Rede pode ser instalado no modo silencioso, ou seja, sem a inserção interativa dos parâmetros de instalação. A instalação silenciosa usa um pacote do Windows Installer (MSI) para o Agente de Rede. O arquivo MSI está localizado no pacote de distribuição do Kaspersky Security Center, na pasta Packages\NetAgent\exec.

Não renomeie o pacote de instalação Kaspersky Network Agent.msi. Renomear este pacote pode causar erros de instalação durante futuras atualizações do Agente de Rede.

A instalação do Agente de Rede a partir do pacote MSI só é possível no modo silencioso, pois não é possível realizar a instalação interativa a partir do pacote MSI.

Para instalar o Agente de Rede em um dispositivo local no modo silencioso:

1. Leia o Contrato de Licença do Usuário Final. Use o comando abaixo somente entende e aceita os termos do Contrato de Licença do Usuário Final.

2. Execute o comando

   ```
   msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
   ```

   onde `setup_parameters` corresponde a uma lista de parâmetros e seus valores respectivos separados por um espaço (`PROP1=PROP1VAL PROP2=PROP2VAL`).

   Na lista de parâmetros, é preciso incluir `EULA=1`. Caso contrário, o Agente de Rede não será instalado.

Caso esteja usando as configurações de conexão padrão do Kaspersky Security Center e do Agente de Rede em dispositivos remotos, execute o comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1
```

`/l*vx` é a chave para gravar registros. O log é criado durante a instalação do Agente de Rede e salvo em C:\windows\temp\nag_inst.log.

Além do nag_inst.log, o aplicativo cria o arquivo $klssinstlib.log, que contém o log de instalação. Esse arquivo está armazenado na pasta %windir%\temp ou %temp%. Para fins de solução de problemas, você ou um especialista do Suporte Técnico da Kaspersky podem precisar dos dois arquivos de log – nag_inst.log e $klssinstlib.log.

Se você precisar especificar adicionalmente a porta para a conexão ao Servidor de Administração, execute o comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
SERVERADDRESS=kscserver.mycompany.com EULA=1 SERVERPORT=14000
```

O parâmetro `SERVERPORT` corresponde ao número da porta para conexão ao Servidor de Administração.

Os nomes e os valores possíveis de parâmetros que podem ser usados quando o Agente de Rede for instalado no modo silencioso são listados na seção Parâmetros de instalação do Agente de Rede.

Se você quiser atualizar o Agente de Rede usando o Windows Installer, execute o seguinte comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Instalar o Agente de Rede para Linux no modo silencioso (com um arquivo de resposta)

Você pode instalar o Agente de Rede em dispositivos Linux usando um arquivo de resposta – um arquivo de texto que contém um conjunto personalizado de parâmetros de instalação: variáveis e seus respectivos valores. O uso do arquivo de resposta permite executar a instalação no modo silencioso, ou seja, sem a participação do usuário.

Para executar a instalação do Agente de Rede para Linux no modo silencioso:

1. Prepare o dispositivo Linux relevante para a instalação remota. Baixe e crie o pacote de instalação remota usando um pacote .deb ou .rpm do Agente de Rede, por meio de qualquer sistema de gerenciamento de pacotes adequado.

2. Caso queira instalar o agente de rede em dispositivos com o sistema operacional SUSE Linux Enterprise Server 15, instale o pacote insserv-compat primeiro para configurar o agente de rede.

3. Leia o Contrato de Licença do Usuário Final. Siga as etapas abaixo somente se entender e aceitar os termos do Contrato de Licença do Usuário Final.

4. Crie o arquivo de resposta (no formato TXT). Adicione ao arquivo de resposta uma lista de variáveis no formato VARIABLE_NAME = variable_value, cada variável em uma linha separada.

   Para o uso correto do arquivo de resposta, você deve incluir nele um conjunto mínimo das três variáveis necessárias:

   - KLNAGENT_SERVER
   - KLNAGENT_AUTOINSTALL
   - EULA_ACCEPTED

   Você também pode adicionar quaisquer variáveis opcionais para usar parâmetros mais específicos da sua instalação remota. A tabela a seguir lista todas as variáveis que podem ser incluídas no arquivo de resposta:

   Variáveis do arquivo de resposta usadas como parâmetros de instalação do Agente de Rede para Linux no modo silencioso

Variáveis do arquivo de resposta usadas como parâmetros de instalação do Agente de Rede para Linux no modo silencioso

Nome da variável	Necessário	Descrição	Valores possíveis
KLNAGENT_SERVER	Sim	Contém o nome do Servidor de Administração apresentado como nome de domínio totalmente qualificado (FQDN) ou endereço IP.	Nome DNS ou endereço IP.
KLNAGENT_AUTOINSTALL	Sim	Define se o modo de instalação silenciosa está ativado.	1 – O modo silencioso está ativado; o usuário não é solicitado a executar nenhuma ação durante a instalação. Outro – O modo silencioso está desativado; o usuário pode ser solicitado a executar ações durante a instalação.
EULA_ACCEPTED	Sim	Define se o usuário aceita o Contrato de Licença do Usuário Final (EULA) do Agente de Rede; quando ausente, pode ser interpretado como não aceitação do EULA.	1 – Confirmo que li, entendi e aceito integralmente os termos e condições deste Contrato de Licença do Usuário Final. Outro ou não especificado – Não aceito os termos do Contrato de Licença (a instalação não é executada).
KLNAGENT_PROXY_USE	Não	Define se a conexão com o Servidor de Administração usará configurações de proxy. O valor padrão é 0.	1 – As configurações de proxy são usadas. Outro – As configurações de proxy não são usadas.
KLNAGENT_PROXY_ADDR	Não	Define o endereço do servidor proxy usado para conexão com o Servidor de Administração.	Nome DNS ou endereço IP.
KLNAGENT_PROXY_LOGIN	Não	Define o nome de usuário usado para fazer login no servidor proxy.	Qualquer nome de usuário existente.
KLNAGENT_PROXY_PASSWORD	Não	Define a senha de usuário usada para o login no servidor proxy.	Qualquer conjunto de caracteres alfanuméricos permitido pelo formato de senha no sistema operacional.
KLNAGENT_VM_VDI	Não	Define se o Agente de Rede está instalado em uma imagem para criação de máquinas virtuais dinâmicas.	1 – O Agente de Rede é instalado em uma imagem, usada posteriormente para a criação de máquinas virtuais dinâmicas. Outro – Nenhuma imagem é usada durante a instalação.
KLNAGENT_VM_OPTIMIZE	Não	Define se as configurações do Agente de Rede são ideais para o hypervisor.	1 – As configurações locais padrão do Agente de Rede são modificadas para permitir o uso otimizado no hypervisor.
KLNAGENT_TAGS	Não	Lista as tags atribuídas à instância do Agente de Rede.	Um ou vários nomes de tag separados por ponto e vírgula.
KLNAGENT_UDP_PORT	Não	Define a porta UDP usada pelo Agente de Rede. O valor padrão é 15000.	Qualquer número de porta existente.
KLNAGENT_PORT	Não	Define a porta não TLS usada pelo Agente de Rede. O valor padrão é 14000.	Qualquer número de porta existente.
KLNAGENT_SSLPORT	Não	Define a porta TLS usada pelo Agente de Rede. O valor padrão é 13000.	Qualquer número de porta existente.
KLNAGENT_USESSL	Não	Define se o TLS (Transport Layer Security) é usado para conexão.	1 (padrão) – O TLS é usado. Outro – O TLS não é usado.

KLNAGENT_GW_MODE	Não	Define se o gateway de conexão é usado.	1 (padrão) – As configurações atuais não são modificadas (na primeira chamada, nenhum gateway de conexão é especificado). 2 – Nenhum gateway de conexão é usado. 3 – O gateway de conexão é usado. 4 – A instância do Agente de Rede é usada como gateway de conexão na zona desmilitarizada (DMZ).
KLNAGENT_GW_ADDRESS	Não	Define o endereço do gateway de conexão. O valor é aplicável apenas se KLNAGENT_GW_MODE=3.	Nome DNS ou endereço IP.

5. Execute a instalação do Agente de Rede. A variável de ambiente KLAUTOANSWERS, que especifica o caminho para o arquivo de resposta, é fornecida ao comando de instalação. Execute um dos seguintes comandos:

   - Para instalar o Agente de Rede usando um pacote RPM em um sistema operacional de 32 bits, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> yum install ./klnagent-<número da compilação>.i386.rpm`

   - Para instalar o Agente de Rede usando um pacote RPM em um sistema operacional de 64 bits, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> yum install ./klnagent64-<número da compilação>.x86_64.rpm`

   - Para instalar o Agente de Rede usando um pacote RPM em um sistema operacional de 64 bits para arquitetura Arm, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> yum install ./klnagent64-<número da compilação>.aarch64.rpm`

   - Para instalar o Agente de Rede usando um pacote DEB em um sistema operacional de 32 bits, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> apt install ./klnagent_<número da compilação>_i386.deb`

   - Para instalar o Agente de Rede usando um pacote DEB em um sistema operacional de 64 bits, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> apt install ./klnagent64_<número da compilação>_amd64.deb`

   - Para instalar o Agente de Rede usando um pacote DEB em um sistema operacional de 64 bits para arquitetura Arm, execute o seguinte comando:
     `sudo KLAUTOANSWERS=<caminho para o arquivo de resposta> apt install ./klnagent64_<número da compilação>_arm64.deb`

   Dependendo da configuração do sistema operacional, você também pode usar os gerenciadores de pacotes rpm, dpkg ou dnf para instalar o Agente de Rede.

A instalação do Agente de Rede para Linux inicia no modo silencioso; o usuário não é solicitado a executar nenhuma ação durante o processo.

Instalação do Agente de Rede para Linux no modo interativo

Este artigo descreve passo a passo como instalar o Agente de Rede, ao especificar os parâmetros de instalação em dispositivos Linux no modo interativo. Como alternativa, é possível usar um arquivo de resposta, um arquivo de texto que contém um conjunto personalizado de parâmetros de instalação: variáveis e seus respectivos valores. O uso do arquivo de resposta permite executar a instalação no modo silencioso, ou seja, sem a participação do usuário.

Para instalar o Agente de Rede no modo interativo:

1. Execute a instalação do Agente de Rede. Dependendo da sua distribuição Linux, execute um dos seguintes comandos:

   - Para instalar o Agente de Rede com um pacote RPM para um sistema operacional de 32 bits:

     `# yum -i klnagent-<número da compilação>.i386.rpm`

   - Para instalar o Agente de Rede com um pacote RPM para um sistema operacional de 64 bits:

     `# yum -i klnagent64-<número da compilação>.x86_64.rpm`

   - Para instalar o Agente de Rede com um pacote RPM para um sistema operacional de 64 bits para a arquitetura Arm:

     `# yum -i klnagent64-<número da compilação>.aarch64.rpm`

   - Para instalar o Agente de Rede com um pacote DEB para um sistema operacional de 32 bits:

     `# apt install ./klnagent_<número da compilação>_i386.deb`

   - Para instalar o Agente de Rede com um pacote DEB para um sistema operacional de 64 bits:

     `# apt install ./klnagent64_<número da compilação>_amd64.deb`

   - Para instalar o Agente de Rede com um pacote DEB para um sistema operacional de 64 bits para a arquitetura Arm:

     `# apt install ./klnagent64_<número da compilação>_arm64.deb`

2. Execute a configuração do Agente de Rede:

   `# /opt/kaspersky/klnagent64/bin/setup/postinstall.pl`

3. Leia o Contrato de Licença do Usuário Final (EULA). O texto é exibido na janela de linha de comando. Pressione a barra de espaço para ver o próximo segmento de texto. Depois, quando for solicitado, digite um dos seguintes valores:

   - Digite `y` (sim), se você entende e aceita integralmente os termos do EULA.
   - Digite `n` (não) se você não aceita os termos do EULA. Para usar o Agente de Rede, é necessário aceitar os termos do EULA.
   - Insira `r` para mostrar o EULA novamente.

4. Digite o nome DNS do Servidor de Administração ou o endereço IP.

5. Digite o número da porta do Servidor de Administração. Por padrão, a porta 14000 é usada.

6. Digite o número da porta SSL do Servidor de Administração. Por padrão, a porta 13000 é usada.

7. Insira `s` caso queira usar a criptografia SSL para o tráfego entre o Agente de Rede e o Servidor de Administração. Caso contrário, insira `n`.

8. Selecione uma das seguintes opções para configurar o Agente de Rede:

   - `[1]` – Não configurar um gateway de conexão.

     Seu dispositivo não atuará como um gateway de conexão e não se conectará com o Servidor de Administração por meio de um gateway de conexão.

   - `[2]` – Não usar o gateway de conexão.

     Seu dispositivo não se conectará com o Servidor de Administração por meio de um gateway de conexão.

   - `[3]`- Conectar ao servidor usando um gateway de conexão.

     Seu dispositivo se conectará com o Servidor de Administração por meio de um gateway de conexão.

   - `[4]` – Usar como um gateway de conexão.

     Seu dispositivo atuará como um gateway de conexão.

O Agente de Rede está instalado em um dispositivo Linux.

Preparar um dispositivo executando o Astra Linux no modo de ambiente de software fechado para a instalação do Agente de Rede

Antes da instalação do Agente de Rede em um dispositivo executando o Astra Linux no modo de ambiente de software fechado, execute dois procedimentos de preparação: o mencionado nas instruções abaixo e as etapas gerais de preparação para qualquer dispositivo Linux.

> Execute os comandos fornecidos nesta instrução em uma conta com privilégios de acesso root.

Para preparar um dispositivo executando o Astra Linux no modo de ambiente de software fechado para a instalação do Agente de Rede:

1. Abra o arquivo `/etc/digsig/digsig_initramfs.conf` e especifique a seguinte configuração:

   ```
   DIGSIG_ELF_MODE=1
   ```

2. Na linha de comando, execute o seguinte comando para instalar o pacote de compatibilidade:

   ```
   apt install astra-digsig-oldkeys
   ```

3. Crie um diretório para a chave do aplicativo:

   ```
   mkdir -p /etc/digsig/keys/legacy/kaspersky/
   ```

4. Coloque a chave do aplicativo /opt/kaspersky/klnagent64/share/kaspersky_astra_pub_key.gpg no diretório criado na etapa anterior:

   ```
   cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
   ```

   Se o kit de distribuição do Kaspersky Security Center não incluir a chave do aplicativo kaspersky_astra_pub_key.gpg, você poderá baixá-lo clicando no link: https://media.kaspersky.com/utilities/CorporateUtilities/kaspersky_astra_pub_key.gpg.

5. Atualize os discos RAM:

   ```
   update-initramfs -u -k all
   ```

   Reinicialize o sistema.

O dispositivo Linux está pronto para a instalação do Agente de Rede. Você pode instalar o Agente de Rede remotamente, no modo interativo ou no modo silencioso.

Instalação local do plugin de gerenciamento de aplicativos

Para instalar o plugin de gerenciamento de aplicativos:

Em um dispositivo com o Console de Administração instalado, execute o arquivo klcfginst.exe, o qual está incluído no pacote de distribuição do aplicativo.

O arquivo klcfginst.exe é incluído em todos os aplicativos que podem ser gerenciado através do Kaspersky Security Center. A instalação é facilitada pelo Assistente e não requer configuração manual das configurações.

Instalando aplicativos no modo silencioso

Para instalar o aplicativo em modo silencioso:

1. Abra a janela principal do aplicativo do Kaspersky Security Center.
2. Na pasta **Instalação remota** da árvore do console, na subpasta **Pacotes de instalação**, selecione o pacote de instalação do aplicativo relevante ou crie um novo para esse aplicativo.

   O pacote de instalação será armazenado no Servidor de Administração na pasta Serviço de pacotes que está dentro da pasta compartilhada. Uma subpasta separada corresponde a cada pacote de instalação.

3. Abra a pasta que armazena o pacote de instalação requerido de uma das seguintes formas:

   - Copiando a pasta correspondente para o pacote de instalação relevante do Servidor de Administração ao dispositivo cliente. Então abra a pasta copiada no dispositivo cliente.

   - Abrindo a partir do dispositivo cliente a pasta compartilhada que corresponde ao pacote de instalação requerido no Servidor de Administração.

   Se a pasta compartilhada estiver localizada em um dispositivo com o sistema operacional Microsoft Windows Vista, selecione o valor **Desativado** para a configuração **Controle de conta do usuário: executar todos os administradores no modo de aprovação do administrador** (**Iniciar** → **Painel de Controle** → **Administração** → **Política de segurança local** → **Configurações de segurança**).

4. Dependendo do aplicativo selecionado, faça o seguinte:

   - Para Kaspersky Anti-Virus for Windows Workstations, Kaspersky Anti-Virus for Windows Servers e Kaspersky Security Center, navegue até à subpasta exec e execute o arquivo executável (o arquivo com a extensão .exe) com uma tecla /s.

   - Para outro aplicativo da Kaspersky, rode o arquivo executável (um arquivo com a extensão .exe) com a tecla /s a partir da pasta aberta.

   Executar o arquivo executável com o `EULA=1` e chaves `PRIVACYPOLICY=1` significa que você aceita os termos do Contrato de Licença e da Política de Privacidade, respectivamente. Você também está ciente de que seus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade. O texto do Contrato de Licença e da Política de Privacidade está incluído no kit de distribuição do Kaspersky Security Center. Aceitar os termos do Contrato de Licença e da Política de Privacidade é necessário para instalar o aplicativo ou atualizar uma versão anterior do aplicativo.

Instalação de aplicativos usando pacotes independentes

O Kaspersky Security Center permite criar pacotes de instalação independentes para aplicativos. Um pacote de instalação independente é um arquivo executável que pode estar localizado em um Servidor Web, ser enviado por e-mail ou transferido de outra maneira para um dispositivo cliente. O arquivo recebido pode ser executado localmente no dispositivo cliente para instalar um aplicativo sem envolver o Kaspersky Security Center.

O Agente de Rede independente para Linux tem uma dependência opcional da ferramenta nmap. Se o utilitário nmap estiver ausente ou for anterior à versão 6.0, a funcionalidade Broadcast DHCP Discover não será compatível.

Para instalar um aplicativo usando um pacote de instalação independente:

1. Conecte ao Servidor de Administração necessário.

2. Na pasta **Instalação remota** na árvore do console, selecione a subpasta **Pacotes de instalação**.

3. No espaço de trabalho, selecione o pacote de instalação do aplicativo necessário.

4. Inicie o processo de criação de um pacote de instalação independente em uma das seguintes formas:

   - Selecionando **Criar pacote de instalação independente** no menu de contexto do pacote de instalação.
   - Clicando no link **Criar pacote de instalação independente** no espaço de trabalho do pacote de instalação.

   O Assistente de Criação de Pacote de Instalação Independente é iniciado. Siga as instruções do Assistente.

   Na etapa final do assistente, selecione um método para transferir o pacote de instalação independente para o dispositivo cliente.

5. Transfira o pacote de instalação independente para o dispositivo cliente.

6. Execute o pacote de instalação independente no dispositivo cliente.

O aplicativo será instalado no dispositivo cliente com as configurações especificadas no pacote independente.

Ao criar um pacote de instalação independente, ela é automaticamente publicada no Servidor Web. Um link para o download do pacote independente é exibido na lista de pacotes de instalação independentes criados. Se necessário, você pode cancelar a publicação do pacote independente selecionado e publicá-lo novamente no Servidor Web. Por padrão, a porta 8060 é usada para o download de pacotes de instalação independentes.

Configurações do pacote de instalação do Agente de Rede

Para configurar um pacote de instalação do Agente de Rede:

1. Na pasta **Instalação remota** na árvore do console, selecione a subpasta **Pacotes de instalação**.

   Por padrão, a pasta **Instalação remota** é uma subpasta da pasta **Avançado**.

2. No menu de contexto do pacote de instalação do Agente de Rede, selecione **Propriedades**.

A janela de propriedades do pacote de instalação do Agente de Rede abre.

Geral

A seção **Geral** exibe informações gerais sobre o pacote de instalação:

- Nome do pacote de instalação
- Nome e versão do aplicativo para o qual o pacote de instalação foi criado
- Tamanho do pacote de instalação
- Data de criação do pacote de instalação
- Caminho para a pasta do pacote de instalação

Configurações

Esta seção apresenta as configurações necessárias para garantir o funcionamento adequado do Agente de Rede imediatamente após sua instalação. As configurações nesta seção estão disponíveis somente em dispositivos que executam o Windows.

No grupo de configurações da **Pasta de destino**, você pode selecionar a pasta do dispositivo cliente na qual o Agente de Rede será instalado.

- **Instalar na pasta padrão**

  Se esta opção estiver selecionada, o Agente de Rede será instalado na pasta <Unidade>:\Program Files\Kaspersky Lab\NetworkAgent. Se essa pasta não existir, ela será criada automaticamente.

  Por padrão, esta opção está selecionada.

- **Instalar na pasta especificada**

  Se esta opção estiver selecionada, o Agente de Rede será instalado na pasta especificada no campo de entrada.

No seguinte grupo de configurações, você pode definir uma senha para uma tarefa de desinstalação remota do Agente de Rede:

- **Usar senha de desinstalação**

  Se esta opção estiver ativada, ao clicar no botão **Modificar**, você pode inserir a senha para desinstalar (somente disponível para o Agente de Rede em dispositivos que executam sistemas operacionais Windows).

  Por padrão, esta opção está desativada.

- **Status**

  Status da senha: **Senha definida** ou **Senha não definida**.

  Por predefinição, esta senha não está instalada.

- **Proteger serviço do Agente de Rede contra remoção ou interrupção não autorizada e impedir alterações nas configurações**

  Quando esta opção estiver ativado, após o Agente de Rede ter sido instalado em um dispositivo gerenciado, o componente não poderá ser removido ou reconfigurado sem os privilégios necessários. O serviço Agente de Rede não pode ser interrompido. Essa opção não tem efeito nos controladores de domínio.

  Ative esta opção para proteger o Agente de Rede em estações de trabalho operadas com direitos de administrador local.

  Por padrão, esta opção está desativada.

- **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**

  Se essa opção estiver ativada, todas as atualizações e patches baixados para Servidor de Administração, Agente de Rede, Console de Administração, Servidor de dispositivos móveis do Microsoft Exchange e Servidor de MDM do iOS serão instalados automaticamente.

  Se esta opção estiver desativada, todas as atualizações e patches baixados somente serão instalados após você modificar seu status para *Aprovado*. As atualizações e patches com o status *Indefinido* não serão instaladas.

  Por padrão, esta opção está ativada.

Conexão

Nesta seção, é possível configurar a conexão do agente de rede para o Servidor de Administração. Para estabelecer uma conexão, é possível usar o protocolo SSL ou UDP. Para configurar a conexão, especifique as seguintes configurações:

- **Servidor de Administração**

  Endereço do dispositivo com o Servidor de Administração instalado.

- **Porta**

  O número da porta que é usada para conexão.

- **Porta SSL**

  Número da porta que é usada para conexão através do protocolo SSL.

- **Usar certificado do Servidor**

  Se esta opção estiver ativada, a autenticação do acesso do Agente de Rede ao Servidor de Administração usará o arquivo de certificado que você pode especificar clicando no botão **Procurar**.

  Se esta opção estiver desativada, o arquivo de certificado será recebido do Servidor de Administração na primeira conexão do Agente de Rede ao endereço especificado no campo **Endereço do servidor**.

  Não recomendamos desativar esta opção porque o recebimento automático de um certificado do Servidor de Administração pelo Agente de Rede na conexão ao Servidor de Administração é considerado inseguro.

  Por padrão, esta caixa de seleção está selecionada.

- **Usar SSL**

  Se esta opção estiver ativada, a conexão com o Servidor de Administração é estabelecida através de uma porta segura via SSL.

  Por padrão, esta opção está desativada. Recomendamos não desativar a opção para que a conexão permaneça segura.

- **Usar porta UDP**

  Se esta opção estiver ativada, o Agente de Rede é conectado ao Servidor de Administração através de uma porta UDP. Isso permite gerenciar os dispositivos clientes e receber as informações sobre eles.

  A porta UDP deve ser aberta nos dispositivos gerenciados onde o agente de rede está instalado. Portanto, recomendamos não desativar a opção.

  Por padrão, esta opção está ativada.

- **Número da porta UDP**

  Neste campo, é possível especificar a porta para conectar o Servidor de Administração com o Agente de Rede usando protocolo UDP.

  A porta UDP padrão é 15000.

- Abrir portas do Agente de Rede no Firewall do Microsoft Windows

  Caso essa opção esteja ativada, as portas usadas pelo Agente de Rede serão adicionadas na lista de exclusões do Firewall do Microsoft Windows.

  Por padrão, esta opção está ativada.

- Usar o servidor proxy

  Se essa opção estiver ativada, especifique os parâmetros do servidor proxy:

  - **Endereço do servidor proxy**
  - **Porta do servidor proxy**

  Se o servidor proxy exigir autenticação, ative a opção **Autenticação do servidor proxy** e especifique o **Nome do usuário** e a **Senha** da conta sob a qual a conexão com o servidor proxy será estabelecida. Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.

Para fins de compatibilidade, não é recomendável especificar as configurações de conexão proxy nas configurações do pacote de instalação do Agente de Rede.

Avançado

Na seção **Avançado**, é possível configurar como usar o gateway de conexão. Nesse caso, é possível fazer o seguinte:

- Use o agente de rede como um gateway de conexão na zona desmilitarizada (DMZ) para se conectar com o Servidor de Administração, estabelecer comunicação com ele e manter os dados no agente de rede seguros durante a transmissão de dados.
- Estabeleça conexão com o Servidor de Administração usando um gateway de conexão para reduzir o número de conexões com o Servidor de Administração. Nesse caso, insira o endereço do dispositivo que atuará como gateway de conexão no campo **Endereço do gateway de conexão**.
- Configure a conexão para Virtual Desktop Infrastructure (VDI) caso a rede tenha máquinas virtuais. Nesse caso, faça o seguinte:
  - **Ativar modo dinâmico para VDI**

    Se esta opção estiver ativada, o modo dinâmico para a Infraestrutura de Virtual Desktop Infrastructure (VDI) será habilitado para o Agente de Rede instalado em uma máquina virtual.

    Por padrão, esta opção está desativada.

  - **Otimizar as configurações para VDI**

    Se esta opção estiver ativada, os seguintes recursos estarão desativados nas configurações do Agente de Rede:
    - Recuperar informações sobre o software instalado
    - Recuperar informações sobre o hardware
    - Recuperar informações sobre as vulnerabilidades detectadas
    - Recuperar informações sobre as atualizações necessárias

    Por padrão, esta opção está desativada.

Componentes adicionais

Nesta seção, você pode selecionar componentes adicionais para instalação simultânea com Agente de Rede.

Tags

A seção **Tags** exibe uma lista de palavras-chave (tags) que podem ser adicionadas aos dispositivos cliente após a instalação do Agente de Rede. Você pode adicionar e remover tags da lista, bem como renomeá-las.

Se a caixa de seleção estiver marcada ao lado da tag, essa será automaticamente adicionada aos dispositivos gerenciados durante a instalação do Agente de Rede.

Se a caixa de seleção estiver desmarcada ao lado da tag, essa não será automaticamente adicionada aos dispositivos gerenciados durante a instalação do Agente de Rede. Você pode adicionar manualmente essa tag aos dispositivos.

Ao remover uma tag da lista, ele será automaticamente removido de todos os dispositivos aos quais foi adicionada.

Histórico de revisões

Nesta seção, você poderá exibir o histórico de revisões do pacote de instalação. Você pode comparar revisões, exibir revisões, salvar revisões em um arquivo, e adicionar e editar descrições da revisão.

As configurações do pacote de instalação do Agente de Rede disponíveis para um sistema operacional específico são fornecidas na tabela abaixo.

Configurações do pacote de instalação do Agente de Rede

Seção da propriedade	Windows	Mac	Linux
Geral	✓	✓	✓
Configurações	✓	—	—
Conexão	✓	✓ (exceto para as opções **Abrir portas do Agente de Rede no Firewall do Microsoft Windows** e **Use apenas detecção automática de servidor proxy**)	✓ (exceto para as opções **Abrir portas do Agente de Rede no Firewall do Microsoft Windows** e **Use apenas detecção automática de servidor proxy**)
Avançado	✓	✓	✓
Componentes adicionais	✓	✓	✓
Tags	✓	✓ (exceto para as regras de marcação automática)	✓ (exceto para as regras de marcação automática)
Histórico de revisões	✓	✓	✓

Ler a Política de Privacidade

A Política de Privacidade está disponível on-line no endereço https://www.kaspersky.com/products-and-services-privacy-policy. Ela também está disponível offline. Você pode ler a Política de Privacidade, por exemplo, antes de instalar o Agente de Rede.

Para ler a Política de Privacidade offline:

1. Inicie a instalação do Kaspersky Security Center.
2. Na janela do instalador, siga até o link **Extrair pacotes de instalação**.
3. Na lista aberta, selecione Agente de Rede do Kaspersky Security Center e, em seguida, clique em **Avançar**.

   O arquivo privacy_policy.txt aparece no dispositivo, na pasta especificada, na subpasta NetAgent.

Implementar sistemas de gerenciamento de dispositivos móveis

Essa seção descreve a implementação de sistemas de gerenciamento de dispositivos móveis usando os protocolos Exchange ActiveSync, MDM do iOS e Kaspersky Endpoint Security.

Implementar um sistema para gerenciamento através do protocolo Exchange ActiveSync

O Kaspersky Security Center permite que você gerencie dispositivos móveis conectados ao Servidor de Administração usando o protocolo Exchange ActiveSync. Os dispositivos móveis Exchange ActiveSync (EAS) são os dispositivos conectados a um Servidor de dispositivos móveis Exchange e gerenciados pelo Servidor de Administração.

Os sistemas operacionais que se seguem suportam o protocolo Exchange ActiveSync:

- Windows Phone® 8
- Windows Phone 8.1
- Windows 10 Mobile
- Android
- iOS

O conjunto de configurações de gerenciamento para um dispositivo Exchange ActiveSync depende do sistema operacional em que o dispositivo móvel está sendo executado. Para obter detalhes sobre as funcionalidades de suporte do protocolo Exchange ActiveSync para um sistema operacional específico, consulte a documentação incluída com o sistema operacional.

A implementação de um sistema de gerenciamento de dispositivos móveis usando o protocolo Exchange ActiveSync inclui as seguintes etapas:

1. O administrador instala o Servidor de dispositivos móveis Exchange no dispositivo cliente selecionado.
2. O administrador cria um perfil de gerenciamento no Console de Administração para gerenciar dispositivos EAS e adiciona esse perfil às caixas de correio dos usuários do Exchange ActiveSync.

   O *Perfil de gerenciamento de dispositivos móveis Exchange ActiveSync* é uma política de ActiveSync usada em um servidor Microsoft Exchange para gerenciamento de dispositivos móveis Exchange ActiveSync. Somente um perfil de gerenciamento de dispositivos EAS pode ser atribuído a uma caixa de correio do Microsoft Exchange.

   Os utilizadores de dispositivos móveis EAS conectam-se com suas caixas de correio Exchange. Qualquer perfil de gerenciamento impõe algumas restrições em dispositivos móveis.

Instalação de um Servidor de dispositivos móveis para Exchange ActiveSync

Um Servidor de dispositivos móveis Exchange deve ser instalado em um dispositivo cliente com um Microsoft Exchange Server instalado. É recomendável instalar o Servidor de dispositivos móveis Exchange em um Microsoft Exchange Server com a função de acesso de cliente atribuída. Se diversos servidores Microsoft Exchange com a função de acesso de cliente no mesmo domínio forem combinados em uma matriz de acesso cliente, é recomendável instalar o Servidor de dispositivos móveis Exchange em cada servidor Microsoft Exchange nessa matriz em um modo de cluster.

Para instalar um Servidor de dispositivos móveis Exchange em um dispositivo local:

1. Executar o arquivo executável setup.exe.

   Uma janela é exibida, solicitando que você selecione os aplicativos Kaspersky para instalar.

2. Na janela de seleção de aplicativos, clique no link **Instalar o Servidor de dispositivos móveis do Microsoft Exchange** para executar o Assistente de instalação do Servidor de dispositivos móveis do Microsoft Exchange.

3. Na janela **Configurações de instalação**, selecione o tipo de instalação do Servidor de dispositivos móveis Exchange:

   - Para instalar o Servidor de dispositivos móveis Exchange com as configurações padrão, selecione **Instalação padrão** e clique no botão **Avançar**.

   - Para definir as configurações de instalação do Servidor de dispositivos móveis Exchange manualmente, selecione **Instalação personalizada** e clique em **Avançar**. Em seguida, faça o seguinte:

     a. Selecione a pasta de destino na janela **Pasta de destino**. A pasta padrão é <Disco>:\Program Files\Kaspersky Lab\Mobile Device Management for Exchange. Se essa pasta não existir, ela é criada automaticamente durante a instalação. Você pode alterar a pasta de destino usando o botão **Procurar**.

     b. Escolha o modo de instalação do Servidor de dispositivos móveis Exchange na janela **Modo de instalação**: modo normal ou modo de cluster.

     c. Na janela **Selecionar conta**, selecione uma conta que será usada para gerenciar dispositivos móveis:

        - **Criar conta e grupo de funções automaticamente**. A conta será criada automaticamente.

        - **Especificar uma conta**. A conta será selecionada manualmente. Clique no botão **Procurar** para selecionar o usuário cuja conta será usada e especifique a senha. O usuário selecionado deve pertencer a um grupo com direitos para gerenciar dispositivos móveis usando o ActiveSync.

     d. Na janela **Configurações IIS**, permita ou proíba a configuração automática das propriedades do servidor Web do Internet Information Services (IIS).

        Caso você tenha proibido a configuração automática das propriedades do Internet Information Services (IIS), ative manualmente o mecanismo "Autenticação do Windows" nas configurações do IIS para Microsoft PowerShell Virtual Directory. Se o mecanismo "Autenticação do Windows" estiver desativado, o Servidor de dispositivos móveis Exchange não funcionará corretamente. Consulte a documentação de IIS para obter mais informações sobre a configuração de IIS.

     e. Clique em **Avançar**.

4. Na janela que se abre, verifique as propriedades da instalação do Servidor de dispositivos móveis Exchange, e então clique em **Instalar**.

Após o Assistente concluir sua operação, o Servidor de dispositivos móveis Exchange será instalado no dispositivo local. O Servidor de dispositivos móveis Exchange será exibido na pasta **Gerenciamento de dispositivos móveis** na árvore do console.

Conectar dispositivos móveis a um Servidor de dispositivos móveis Exchange

Antes de conectar quaisquer dispositivos móveis, você deve configurar o Microsoft Exchange Server para permitir que outros dispositivos se conectem usando o protocolo ActiveSync.

Para conectar um dispositivo a um Servidor de dispositivos móveis Exchange, o usuário conecta-se a sua caixa de correio do Microsoft Exchange a partir do dispositivo móvel através do ActiveSync. Ao conectar, o usuário deve especificar as configurações de conexão no cliente ActiveSync, como o endereço de e-mail e a senha de e-mail.

O dispositivo móvel do usuário conectado ao servidor Microsoft Exchange é exibido na subpasta **Dispositivos móveis** contida na pasta **Gerenciamento de Dispositivos Móveis** na árvore do console.

Após o dispositivo móvel Exchange ActiveSync ter sido conectado ao Servidor de dispositivos móveis Exchange, o administrador pode gerenciar o dispositivo móvel Exchange ActiveSync conectado.

Configurar o servidor da Web dos Serviços de informações da Internet

Ao usar o Microsoft Exchange Server (versões 2010 e 2013), você deve ativar o mecanismo de autenticação do Windows de um diretório virtual do Windows PowerShell™ nas configurações do servidor Web Internet Information Services (IIS). Este mecanismo de autenticação será ativado automaticamente se a opção **Configurar automaticamente o Microsoft Internet Information Services (IIS)** for selecionada no Assistente de implementação do servidor de dispositivos móveis do Microsoft Exchange (opção padrão).

De outra forma, você terá de ativar o mecanismo de autenticação por si só.

Para ativar o mecanismo de autenticação do Windows para diretório virtual PowerShell manualmente:

1. No console Internet Information Services (IIS) Manager, abra as propriedades do diretório virtual PowerShell.
2. Siga para a seção **Autenticação**.
3. Selecione **Autenticação do Microsoft Windows** e, a seguir, clique no botão **Ativar**.
4. Abrir **Configurações avançadas**.
5. Selecione a opção **Ativar a autenticação no modo Kernel**.
6. Na lista suspensa **Proteção expandida**, selecione **Necessária**.

Quando usa o Microsoft Exchange Server 2007, o servidor da Web IIS não necessita de nenhuma configuração.

Instalação local de um Servidor de dispositivos móveis Exchange

Para uma instalação local de um Servidor de dispositivos móveis Exchange, o administrador deve executar as seguintes operações:

1. Copie o conteúdo da pasta \Server\Packages\MDM4Exchange\ do pacote de distribuição do Kaspersky Security Center para um dispositivo cliente.
2. Executar o arquivo executável setup.exe.

A instalação local inclui dois tipos da instalação:

- A instalação padrão é uma instalação simplificada que não necessita que o administrador defina qualquer configuração; é recomendada na maioria dos casos.
- A instalação estendida é uma instalação que necessita que o administrador defina as seguintes configurações:
  - Caminho para a instalação do Servidor de dispositivos móveis Exchange.
  - Modo de operação do Servidor de dispositivos móveis Exchange: modo padrão ou modo de cluster.
  - A possibilidade de especificar a conta sob a qual o serviço Servidor de dispositivos móveis do Microsoft Exchange será executado.
  - Ativar/desativar a configuração automática do servidor da Web IIS.

O Assistente de implementação do servidor de dispositivos móveis do Microsoft Exchange deve ser executado sob uma conta que tenha todos os direitos necessários.

Instalação remota de um Servidor de dispositivos móveis do Microsoft Exchange

Para configurar a instalação remota de um Servidor de dispositivos móveis do Microsoft Exchange, o administrador deve executar as seguintes ações:

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Instalação remota** e a, seguir, a subpasta **Pacotes de instalação**.
2. Na subpasta **Pacotes de instalação**, abra as propriedades do pacote **Plug-in do Servidor de dispositivos móveis Exchange**.
3. Siga para a seção **Configurações**.

   Esta seção contém as mesmas configurações que as usados para a instalação local do aplicativo.

Após a configuração da instalação remota, é possível iniciar a instalação de um Servidor de dispositivos móveis do Microsoft Exchange.

Para instalar um Servidor de dispositivos móveis do Microsoft Exchange:

1. Na árvore do Console de Administração do Kaspersky Security Center, selecione a pasta **Instalação remota** e a, seguir, a subpasta **Pacotes de instalação**.
2. Na subpasta **Pacotes de instalação**, selecione o pacote **Plug-in do Servidor de dispositivos móveis Exchange**.
3. Abra o menu de contexto do pacote e selecione **Instalar o aplicativo**.
4. No Assistente de Instalação Remota que for aberto, selecione um dispositivo (ou múltiplos dispositivos para a instalação no modo de cluster).
5. No campo **Executar o assistente de instalação do aplicativo com a conta especificada**, especifique a conta sob a qual o processo de instalação será executado no dispositivo remoto.

   A conta deve ter os direitos necessários.

Implementar um sistema para gerenciamento através do protocolo MDM do iOS

O Kaspersky Security Center possibilita gerenciar dispositivos móveis executando o iOS. Os dispositivos MDM do iOS são dispositivos móveis do iOS conectados a um Servidor de MDM do iOS e gerenciados por um Servidor de Administração.

Os dispositivos móveis são conectados a um Servidor de MDM do iOS por meio das seguintes etapas:

1. O administrador instala o Servidor de MDM do iOS.
2. O administrador recebe um certificado do Apple Push Notification Service (APNs) (Recebendo um certificado APNs, https://support.kaspersky.com/help/KSMM/4.1/en-US/64900.htm).

   O certificado de APNs possibilita que o Servidor de Administração se conecte ao servidor de APNs para enviar notificações push para dispositivos iOS MDM.
3. O administrador instala o Certificado de APNs no Servidor de MDM do iOS.
4. O administrador cria um perfil de MDM do iOS para o usuário do dispositivo móvel iOS.

   O perfil de iOS MDM contém uma coleção de configurações para a conexão de dispositivos móveis iOS ao Servidor de Administração.

Após perfil de iOS MDM ser instalado e o dispositivo MDM do iOS ser sincronizado com o Servidor de Administração, o dispositivo será exibido na pasta **Dispositivos móveis**, que é uma subpasta da pasta **Gerenciamento de Dispositivos Móveis** na árvore do console.

Instalando o Servidor de MDM do iOS

Para instalar o Servidor de MDM do iOS em um dispositivo local:

1. Executar o arquivo executável setup.exe.

   Uma janela é exibida, solicitando que você selecione os aplicativos Kaspersky para instalar.

   Na janela de seleção de aplicativos, clique no link **Instalar o Servidor de MDM do iOS** para executar o Assistente de Configuração do Servidor de MDM do iOS.
2. Selecione uma pasta de destino.

   A pasta padrão é <Disco>:\Program Files\Kaspersky Lab\Mobile Device Management for iOS. Se essa pasta não existir, ela é criada automaticamente durante a instalação. Você pode alterar a pasta de destino usando o botão **Procurar**.

3. Na janela **Especifique as configurações para conectar-se ao Servidor de MDM do iOS** do Assistente, no campo **Porta externa para a conexão ao serviço MDM do iOS**, especifique uma porta externa para a conexão de dispositivos móveis ao serviço MDM do iOS.

   A porta externa 5223 é usada por dispositivos móveis para comunicação com o servidor APNs. Certifique-se de que a porta 5223 é aberta no firewall para conexão com o intervalo de endereços 17.0.0.0/8.

   A Porta 443 é usada para a conexão ao Servidor de MDM do iOS por padrão. Se a porta 443 já estiver sendo usada por outro serviço ou aplicativo, ela pode ser substituída por, por exemplo, a porta 9443.

   O Servidor de MDM do iOS usa a porta externa 2197 para enviar notificações para o servidor APNs.

   Os servidores APNs são executados no modo de balanceamento de carga. Os dispositivos móveis nem sempre se conectam com os mesmos endereços IP para receber notificações. A faixa de endereços 17.0.0.0/8 está reservada para a Apple, e por esse motivo é recomendável especificar toda esta faixa como uma faixa permitida nas configurações do Firewall.

4. Se desejar configurar portas de interação para componentes do aplicativo manualmente, selecione a opção **Configurar manualmente as portas locais** e especifique valores para as configurações seguintes:

   - **Porta para a conexão ao Agente de Rede**. Neste campo, especifique uma porta para a conexão do serviço MDM do iOS ao Agente de Rede. O número da porta padrão é 9799.
   - **Porta local para conectar ao serviço MDM do iOS**. Neste campo, especifique uma porta local para a conexão do Agente de Rede ao serviço MDM do iOS. O número da porta padrão é 9899.

   Recomenda-se o uso dos valores padrão.

5. Na janela **Endereço externo do Servidor de dispositivos móveis** do assistente, no campo **Endereço da Web para conexão remota ao Servidor de dispositivos móveis**, especifique o endereço do dispositivo cliente no qual o Servidor de MDM do iOS deve ser instalado.

   Esse endereço será usado para a conexão de dispositivos móveis gerenciados ao serviço MDM do iOS. Esse dispositivo cliente deve estar disponível para conexão de dispositivos MDM do iOS.

   Você pode especificar o endereço de um dispositivo cliente em qualquer um dos seguintes formatos:

   - Dispositivo FQDN (tal como mdm.example.com)
   - Nome do dispositivo NetBIOS

   Evite adicionar o esquema de URL e o número da porta na cadeia de endereço: esses valores serão adicionados automaticamente.

Quando o Assistente for concluído, o Servidor de MDM do iOS será instalado no dispositivo local. O Servidor de MDM do iOS é exibido na pasta **Gerenciamento de dispositivos móveis** na árvore do console.

Instalando o Servidor de MDM do iOS no modo silencioso

O Kaspersky Security Center permite instalar o Servidor de MDM do iOS em um dispositivo local no modo silencioso, ou seja, sem uma entrada interativa das configurações de instalação.

Para instalar o Servidor de MDM do iOS em um dispositivo local no modo silencioso:

1. Leia o Contrato de Licença do Usuário Final. Use o comando abaixo somente entende e aceita os termos do Contrato de Licença do Usuário Final.

2. Execute o seguinte comando:

   ```
   .\exec\setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 <parâmetros_de_configuração>"
   ```

   onde `setup_parameters` correspondem a uma lista de configurações e seus valores respectivos separados por vírgulas (`PROP1=PROP1VAL PROP2=PROP2VAL`). O arquivo setup.exe está localizado na pasta Servidor, que faz parte do kit de distribuição do Kaspersky Security Center.

Os nomes e valores possíveis para parâmetros que podem ser usados quando Servidor de MDM do iOS é instalado no modo silencioso são listados na tabela abaixo. Os parâmetros podem ser especificados em qualquer ordem conveniente.

Parâmetros de instalação do Servidor de MDM do iOS no modo silencioso

Nome do parâmetro	Descrição do parâmetro	Valores disponíveis
EULA	Aceitação dos termos do Contrato de Licença do Usuário Final. Este parâmetro é obrigatório.	• 1 – Eu li, entendo e aceito por completo os termos do Contrato de Licença do Usuário Final. • Outro valor ou nenhum valor – Não aceito os termos do Contrato de Licença (a instalação não é executada).
DONT_USE_ANSWER_FILE	Se usar um arquivo XML com configurações de instalação do Servidor MDM do iOS. O arquivo XML está incluído no pacote de instalação ou armazenado no Servidor de Administração. Você não precisa especificar um caminho adicional para o arquivo. Este parâmetro é obrigatório.	• 1 – Não usar o arquivo de XML com parâmetros. • Outro valor ou nenhum valor definido – Usar o arquivo de XML com parâmetros.
INSTALLDIR	A pasta de instalação do Servidor MDM do iOS. Este parâmetro é opcional.	Valor da sequência de caracteres, por exemplo, `INSTALLDIR=\"C:\install\"`
CONNECTORPORT	Porta local para conexão do serviço MDM do iOS com o Agente de Rede. O número da porta padrão é 9799. Este parâmetro é opcional.	Valor numérico.
LOCALSERVERPORT	Porta local para conexão do Agente de Rede com o serviço MDM do iOS. O número da porta padrão é 9899. Este parâmetro é opcional.	Valor numérico.
EXTERNALSERVERPORT	Porta para conectar um dispositivo ao Servidor MDM do iOS. O número da porta padrão é 443. Este parâmetro é opcional.	Valor numérico.
EXTERNAL_SERVER_URL	O endereço externo do dispositivo cliente no qual o Servidor MDM do iOS deve ser instalado. Esse endereço será usado para a conexão de dispositivos móveis gerenciados ao serviço MDM do iOS. O dispositivo cliente deve estar disponível para a conexão através do MDM do iOS. O endereço não deve incluir o esquema URL e o número da porta, já que estes valores serão adicionados automaticamente. Este parâmetro é opcional.	• Dispositivo FQDN (tal como mdm.example.com) • Nome do dispositivo NetBIOS • Endereço IP do dispositivo

Nome do parâmetro	Descrição do parâmetro	Valores disponíveis
WORKFOLDER	Pasta de trabalho do Servidor MDM do iOS. Se nenhuma pasta de trabalho for especificada, os dados serão gravados na pasta padrão. Este parâmetro é opcional.	Valor da sequência de caracteres, por exemplo, `WORKFOLDER=\"C:\work\"`
MTNCY	Uso do Servidor MDM do iOS por múltiplos Servidores virtuais. Este parâmetro é opcional.	• 1 – O Servidor MDM do iOS será usado por múltiplos Servidores de Administração virtuais. • Outro valor ou nenhum valor definido – O Servidor MDM do iOS não será usado por múltiplos Servidores de Administração virtuais.

Exemplo:

```
\exec\setup.exe /s /v"EULA=1 DONT_USE_ANSWER_FILE=1 EXTERNALSERVERPORT=9443 EXTERNAL_SERVER_URL=\"www.test-mdm.com\""
```

Os parâmetros do Servidor MDM do iOS são fornecidos em detalha na seção "Instalar o Servidor MDM do iOS".

Cenários de implementação do Servidor de MDM do iOS

O número de cópias do Servidor de MDM do iOS a ser instalado pode ser selecionado com base no hardware disponível ou no número total de dispositivos móveis cobertos.

Tenha em mente que o número máximo recomendado de dispositivos móveis para uma instalação única do Kaspersky Device Management for iOS é de 50.000 no máximo. Para reduzir a carga, todo o conjunto de dispositivos pode ser distribuído entre vários servidores que tenham o Servidor de MDM do iOS instalado.

A autenticação de dispositivos MDM do iOS é executada por certificados de usuário (qualquer perfil instalado em um dispositivo contém o certificado do proprietário do dispositivo). Assim, dois esquemas de implementação são possíveis para um Servidor de MDM do iOS:

- Esquema simplificado
- Esquema de implementação envolvendo a delegação de restrição Kerberos (KCD)

Esquema de implementação simplificada

Ao implementar um Servidor de MDM do iOS de acordo com o esquema simplificado, os dispositivos móveis conectam-se ao serviço da Web do MDM do iOS diretamente. Neste caso, os certificados de usuário emitidos pelo Servidor de Administração somente podem ser aplicados para a autenticação de dispositivos. A integração com a Infraestrutura de Chaves Públicas (PKI) é impossível para certificados de usuário.

Esquema de implementação envolvendo a delegação de restrição Kerberos (KCD)

Para usar o esquema de implementação com a delegação de restrição Kerberos (KCD), os seguintes requisitos devem ser atendidos:

- O Servidor de Administração e o Servidor de MDM do iOS estão localizados na rede interna da organização.
- Um proxy reverso com suporte a KCD está em uso.

Este esquema de implementação fornece para o seguinte:

- Integração com o proxy reverso compatível com KCD
- Uso do KCD para a autenticação de dispositivos móveis
- Integração com o PKI para aplicar certificados de usuário

Ao usar este esquema de implementação, você deve fazer o seguinte:

- No Console de Administração, nas configurações do serviço da Web MDM do iOS, selecione a caixa de seleção **Assegurar compatibilidade com a delegação restrita de Kerberos**.
- Como certificado do serviço da Web MDM do iOS, especifique o certificado personalizado definido quando o serviço da Web MDM do iOS foi publicado no proxy reverso.
- Os certificados de usuário para dispositivos iOS devem ser emitidos por Certificate Authority (CA) do domínio. Caso o domínio contenha CAs com múltiplas raízes, os certificados de usuário devem ser emitidos pela CA especificada quando o serviço da Web MDM do iOS foi publicado no proxy reverso.

  Você pode assegurar-se de que o certificado do usuário está em conformidade como o requisito de emissão CA usando um dos seguintes métodos:

  - Especifique o certificado do usuário no Assistente de novo perfil de iOS MDM e no Assistente de instalação de certificados.
  - Integre o Servidor de Administração com o PKI do domínio e defina a configuração correspondente nas regras de emissão de certificados:

    1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis** e selecione a subpasta **Certificados**.
    2. No espaço de trabalho da pasta **Certificados**, clique no botão **Configurar as regras de emissão de certificados** para abrir a janela **Regras de emissão do certificado**.
    3. Na seção **Integração com PKI**, configure a integração com a infraestrutura de chaves públicas.
    4. Na seção **Emissão de certificados móveis**, especifique a origem dos certificados.

Abaixo encontra-se um exemplo da Kerberos Constrained Delegation (KCD) com as seguintes suposições:

- O serviço da Web MDM do iOS está em execução na porta 443.
- O nome do dispositivo com o proxy reverso é firewall.mydom.local.
- O nome do dispositivo com o serviço da Web MDM do iOS é iosmdm.mydom.local.
- O nome da publicação externa do serviço da Web MDM do iOS é iosmdm.mydom.global.

Nome do serviço principal para http/iosmdm.mydom.local

No domínio, você deve registrar o nome do serviço principal (SPN) para o dispositivo com o serviço da Web MDM do iOS (iosmdm.mydom.local):

```
setspn -a http/iosmdm.mydom.local iosmdm
```

Configuração das propriedades de domínio do dispositivo com o proxy reverso (firewall.mydom.local)

Para delegar o tráfego, confie o dispositivo com o proxy reverso (firewall.mydom.local) ao serviço definido pelo SPN (http/iosmdm.mydom.local).

Para confiar o dispositivo com o proxy reverso ao serviço definido pelo SPN (http/iosmdm.mydom.local), o administrador deve executar as seguintes ações:

1. No snap-in do Microsoft Management Console nomeado "Usuários e computadores do Active Directory", selecione o dispositivo com o proxy reverso instalado (firewall.mydom.local).

2. Nas propriedades do dispositivo, na guia **Delegação**, defina **Confiar neste computador somente para a delegação ao serviço especificado** alterne para **Usar qualquer protocolo de autenticação**.

3. Adicione o SPN (http/iosmdm.mydom.local) à lista **Serviços aos quais esta conta possa apresentar credenciais delegadas**.

Certificado especial (personalizado) do serviço da Web publicado (iosmdm.mydom.global)

Você tem de emitir um certificado especial (personalizado) para serviço da Web MDM do iOS no FQDN iosmdm.mydom.global e especificar que ele substitui o certificado padrão nas configurações do serviço da Web MDM do iOS no Console de Administração.

Observe que o contêiner de certificado (arquivo com a extensão p12 ou pfx) também deve conter uma cadeia de certificados raiz (chaves públicas).

Publicação do serviço da Web de MDM do iOS no proxy reverso

No proxy reverso, para o tráfego que vai de um dispositivo móvel para a porta 443 do iosmdm.mydom.global, é necessário configurar a KCD no SPN (http/iosmdm.mydom.local) usando o certificado emitido para o FQDN (iosmdm.mydom.global). Observe que publicar e o serviço da Web publicado devem compartilhar o mesmo certificado do servidor.

Recebimento de um certificado de APNs

Caso já tenha um certificado de APNs, considere renová-lo em vez de criar um novo. Quando o certificado de APNs existente é substituído por um recém-criado, o Servidor de Administração perde a capacidade de gerenciar os dispositivos móveis iOS conectados atualmente.

Quando a Solicitação de Assinatura do Certificado (CSR) é criada na primeira etapa do Assistente de Certificado de APNs, sua chave privada é armazenada na RAM do dispositivo. Portanto, todas as etapas do assistente devem ser concluídas em uma única sessão do aplicativo.

Para receber um Certificado de APNs:

1. Na pasta **Gerenciamento de Dispositivos Móveis** na árvore do console, selecione a subpasta **Servidores de dispositivos móveis**.

2. No espaço de trabalho da pasta **Servidores de dispositivos móveis**, selecione um Servidor de MDM do iOS.

3. No menu de contexto do Servidor de MDM do iOS, selecione **Propriedades**.

   Isso abre a janela de propriedades Servidor MDM do iOS.

4. Na janela de propriedades do Servidor de MDM do iOS, selecione a seção **Certificados**.

5. Na seção **Certificados**, no grupo de configurações **Certificado de notificação Apple Push**, clique no botão **Solicitar novo**.

   O Assistente Receber Certificado de APNs é iniciado e a janela **Solicitar novo** se abre.

6. Crie uma solicitação de assinatura de certificado (daqui por diante citada como solicitação CSR). Para fazer isso, execute como seguintes ações:

   a. Clique no botão **Criar CSR**.

   b. Na janela **Criar CSR** que é aberta, especifique um nome para sua solicitação, os nomes da sua empresa e departamento, sua cidade, região e país.

   c. Clique no botão **Salvar** e especifique um nome para o arquivo em que sua solicitação CSR será salva.

   A chave privada do certificado será salva na memória do dispositivo.

7. Use sua CompanyAccount para enviar o arquivo com a solicitação CSR criada para a Kaspersky, para ser assinada.

   > Assinar sua solicitação CSR somente estará disponível após transferir para o portal CompanyAccount uma chave que permite usar o Gerenciamento de Dispositivos Móveis.

   Após o processamento de sua solicitação online, você receberá um arquivo de solicitação CSR assinado pela Kaspersky.

8. Envie o arquivo CSR assinado para o site da Apple Inc. usando uma Apple ID aleatória.

   Recomenda-se que evite usar uma Apple ID pessoal. Crie uma Apple ID dedicada para usar como sua ID corporativa. Após você ter criado uma Apple ID, deve vinculá-la à caixa de correio da organização, e não a uma caixa de correio de um funcionário.

   Após o processamento de sua solicitação CSR pela Apple Inc., você receberá a chave pública do Certificado de APNs. Salve o arquivo em disco.

9. Exporte o Certificado de APNs junto com a chave privada criada ao gerar a solicitação CSR em formato de arquivo PFX. Para fazer isso:

   a. Na janela **Solicitar novo certificado de APNs**, clique no botão **Concluir CSR**.

   b. Na janela **Abrir**, selecione um arquivo com a chave pública do certificado recebida da Apple Inc. como resultado do processamento CSR e clique no botão **Abrir**.

      O processo de exportação do certificado será iniciado.

   c. Na janela que se segue, insira a senha da chave privada e clique em **OK**.

      Esta senha será usada para a instalação de Certificado de APNs no Servidor de MDM do iOS.

   d. Na janela **Salvar certificado de APNs** especifique um nome de arquivo para o certificado de APNs, selecione uma pasta e clique em **Salvar**.

A chave privada e a chave pública do certificado são combinadas e o certificado de APNs é salvo em formato PFX. Após esta ação, você pode instalar o certificado de APNs no Servidor de MDM do iOS.

Renovação de um certificado de APNs

Para renovar um Certificado de APNs:

1. Na pasta **Gerenciamento de Dispositivos Móveis** na árvore do console, selecione a subpasta **Servidores de dispositivos móveis**.

2. No espaço de trabalho da pasta **Servidores de dispositivos móveis**, selecione um Servidor de MDM do iOS.

3. No menu de contexto do Servidor de MDM do iOS, selecione **Propriedades**.

   Isso abre a janela de propriedades Servidor MDM do iOS.

4. Na janela de propriedades do Servidor de MDM do iOS, selecione a seção **Certificados**.

5. Na seção **Certificados**, no grupo de configurações **Certificado de notificação Apple Push**, clique no botão **Renovar**.

   O Assistente de Renovação de Certificado de APNs inicia, a janela **Renovar o certificado de APNs** é aberta.

6. Crie uma solicitação de assinatura de certificado (daqui por diante citada como solicitação CSR). Para fazer isso, execute como seguintes ações:

   a. Clique no botão **Criar CSR**.

   b. Na janela **Criar CSR** que é aberta, especifique um nome para sua solicitação, os nomes da sua empresa e departamento, sua cidade, região e país.

   c. Clique no botão **Salvar** e especifique um nome para o arquivo em que sua solicitação CSR será salva.

   A chave privada do certificado será salva na memória do dispositivo.

7. Use sua CompanyAccount para enviar o arquivo com a solicitação CSR criada para a Kaspersky, para ser assinada.

   > Assinar sua solicitação CSR somente estará disponível após transferir para o portal CompanyAccount uma chave que permite usar o Gerenciamento de Dispositivos Móveis.

   Após o processamento de sua solicitação online, você receberá um arquivo de solicitação CSR assinado pela Kaspersky.

8. Envie o arquivo CSR assinado para o site da Apple Inc. usando uma Apple ID aleatória.

   > Recomenda-se que evite usar uma Apple ID pessoal. Crie uma Apple ID dedicada para usar como sua ID corporativa. Após você ter criado uma Apple ID, deve vinculá-la à caixa de correio da organização, e não a uma caixa de correio de um funcionário.

   Após o processamento de sua solicitação CSR pela Apple Inc., você receberá a chave pública do Certificado de APNs. Salve o arquivo em disco.

9. Solicite a chave pública do certificado. Para fazer isso, execute como seguintes ações:

    a. Siga para o portal Apple Push Certificates. Para efetuar o login no portal, use a Apple ID recebida na solicitação inicial do certificado.

    b. Na lista de certificados, selecione o certificado cujo nome APSP (no formato "APSP: <número>") coincide com o nome APSP do certificado usado pelo Servidor de MDM do iOS e clique no botão **Renovar**.

    O Certificado de APNs é renovado.

    c. Salve o certificado criado no portal.

10. Exporte o Certificado de APNs junto com a chave privada criada ao gerar a solicitação CSR em formato de arquivo PFX. Para fazer isso, execute como seguintes ações:

    a. Na janela **Renovar o certificado de APNs**, clique no botão **Concluir CSR**.

    b. Na janela **Abrir**, selecione um arquivo com a chave pública do certificado recebida da Apple Inc. como resultado do processamento da solicitação CSR e clique no botão **Abrir**.

    O processo de exportação do certificado será iniciado.

    c. Na janela que se segue, insira a senha da chave privada e clique em **OK**.

    Esta senha será usada para a instalação de Certificado de APNs no Servidor de MDM do iOS.

    d. Na janela **Renovar o certificado de APNs** que se abre, especifique um nome de arquivo para o certificado de APNs, selecione uma pasta e clique em **Salvar**.

A chave privada e a chave pública do certificado são combinadas e o certificado de APNs é salvo em formato PFX.

Configurando um certificado de reserva de servidor MDM iOS

A funcionalidade do Servidor MDM do iOS permite emitir um certificado de reserva. Este certificado destina-se ao uso em perfis do MDM do iOS, para garantir a alternância perfeita de dispositivos iOS gerenciados após a expiração do certificado do Servidor de MDM do iOS.

Se o Servidor de MDM usa um certificado padrão emitido pela Kaspersky, você pode emitir um certificado de reserva (ou especificar seu próprio certificado personalizado como reserva) antes que o certificado do Servidor de MDM do iOS expire. Por padrão, o certificado de reserva é emitido automaticamente 60 dias antes do término do certificado do Servidor de MDM do iOS. O certificado de reserva do Servidor de MDM do iOS se torna o certificado principal imediatamente após o término do certificado do Servidor de MDM do iOS. A chave pública é distribuída a todos os dispositivos gerenciados por meio de perfis de configuração, para que você não precise transmiti-la manualmente.

Para emitir um certificado de reserva do Servidor de MDM do iOS ou especificar um certificado de reserva personalizado:

1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis**, e selecione a subpasta **Servidores de dispositivos móveis**.

2. Na lista de servidores de dispositivos móveis, selecione o Servidor de MDM do iOS relevante e, no painel direito, clique no botão **Configurar o Servidor de MDM do iOS**.

3. Na janela de configurações do Servidor de MDM do iOS que é exibida, selecione a seção **Certificados**.

4. No bloco de configurações **Certificado de reserva** execute uma das seguintes ações:

   - Se planeja continuar usando um certificado autoassinado (ou seja, o emitido pela Kaspersky):

     a. Clique no botão **Problema**.

     b. Na janela aberta **Data de ativação**, selecione uma das duas opções para a data em que o certificado de reserva deve ser aplicado:

        - Se deseja aplicar o certificado de reserva no momento do término do certificado atual, selecione a opção **Quando o certificado atual expira**.

        - Se deseja aplicar o certificado de reserva antes que o certificado atual expire, selecione a opção **Após período especificado (dias)**. No campo de entrada próximo a esta opção, especifique a duração do período após o qual o certificado de reserva deve substituir o certificado atual.

        > O período de validade do certificado de reserva especificado não pode exceder o prazo de validade do certificado atual do Servidor de MDM do iOS.

     c. Clique no botão **OK**.

     O certificado do Servidor de MDM do iOS é emitido.

   - Se você planeja usar um certificado personalizado emitido pela sua autoridade de certificação:

     a. Clique no botão **Adicionar**.

     b. Na janela aberta do File Explorer, especifique um arquivo de certificado no formato PEM, PFX ou P12, que é armazenado em seu dispositivo, e clique no botão **Abrir**.

     Seu certificado personalizado é especificado como o certificado de reserva do Servidor de MDM do iOS.

Você tem um certificado de reserva do Servidor de MDM do iOS especificado. Os detalhes do certificado de reserva são exibidos no bloco de configurações **Certificado de reserva** (nome do certificado, nome do emissor, data de término e a data em que o certificado de reserva deve ser aplicado, se houver).

Instalação de um certificado de APNs em um Servidor de MDM do iOS

Após receber o Certificado de APNs, você deve instalá-lo no Servidor de MDM do iOS.

Para instalar o Certificado de APNs no Servidor de MDM do iOS:

1. Na pasta **Gerenciamento de Dispositivos Móveis** na árvore do console, selecione a subpasta **Servidores de dispositivos móveis**.

2. No espaço de trabalho da pasta **Servidores de dispositivos móveis**, selecione um Servidor de MDM do iOS.

3. No menu de contexto do Servidor de MDM do iOS, selecione **Propriedades**.

   Isso abre a janela de propriedades Servidor MDM do iOS.

4. Na janela de propriedades do Servidor de MDM do iOS, selecione a seção **Certificados**.

5. Na seção **Certificados**, no grupo de configurações **Certificado de notificação Apple Push**, clique no botão **Instalar**.

6. Selecione o arquivo PFX que contem o Certificado de APNs.

7. Insira a senha da chave privada especificada durante a exportação do certificado de APNs.

O Certificado de APNs será instalado no Servidor de MDM do iOS. Os detalhes do certificado serão exibidos na janela de propriedades do Servidor de MDM do iOS, na seção **Certificados**.

Configurar o acesso ao serviço Apple Push Notification

Para assegurar o funcionamento apropriado do serviço da Web MDM do iOS e as respostas em tempo dos dispositivos móveis aos comandos do administrador, você tem de especificar um certificado de Apple Push Notification Service (aqui referido como certificado de APNs) nas configurações do Servidor de MDM do iOS.

Interação com o Apple Push Notification (aqui referido como APNs), o serviço da Web MDM do iOS se conecta ao endereço externo api.push.apple.com por meio da porta 2197 (saída). Portanto, o serviço da Web MDM do iOS necessita do acesso à porta TCP 2197 para a faixa de endereços 17.0.0.0/8. Do dispositivo iOS está o acesso à porta TCP 5223 para a faixa de endereços 17.0.0.0/8.

Se você pretender acessar APNs a partir do serviço da Web MDM do iOS através de um servidor proxy, deverá executar as seguintes ações no dispositivo com o serviço da Web MDM do iOS instalado:

1. Adicione as seguintes sequências de caracteres ao registro:

   - Para sistemas operacionais de 32 bits:

```
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Nome do host proxy>"
"ApnProxyPort"="<Porta proxy>"
"ApnProxyLogin"="<Login proxy>"
"ApnProxyPwd"="<Senha proxy>"
```

   - Para sistemas operacionais de 64 bits:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Conset
"ApnProxyHost"="<Nome do host proxy>"
"ApnProxyPort"="<Porta proxy>"
"ApnProxyLogin"="<Login proxy>"
"ApnProxyPwd"="<Senha proxy>"
```

2. Reinicie o serviço da Web MDM do iOS.

Emissão e instalação de um certificado compartilhado em um dispositivo móvel

Para emitir um certificado compartilhado para um usuário:

1. Na árvore do console, na pasta **Contas de usuário**, selecione uma conta do usuário.

2. No menu de contexto da conta do usuário, selecione **Instalar certificado**.

O Assistente de Instalação de Certificado é iniciado. Siga as instruções do Assistente.

Quando o assistente tiver sido concluído, um certificado será criado e adicionado à lista de certificados do usuário.

O certificado emitido será baixado pelo usuário, juntamente com o pacote de instalação que contém o perfil de MDM do iOS.

Após o dispositivo móvel ter sido conectado ao Servidor de MDM do iOS, as configurações do perfil de MDM do iOS serão aplicadas ao dispositivo do usuário. O administrador poderá gerenciar o dispositivo após a conexão.

O dispositivo móvel do usuário conectado ao servidor MDM do iOS é exibido na subpasta **Dispositivos móveis** contida na pasta **Gerenciamento de Dispositivos Móveis** na árvore do console.

Adicionar um dispositivo KES na lista de dispositivos gerenciados

Para adicionar o dispositivo KES de um usuário na lista de dispositivos gerenciados usando um link ao Google Play™:

1. Na árvore do console, selecione a pasta **Contas de usuário**.

   Por padrão, a pasta **Contas de usuário** é uma subpasta da pasta **Avançado**.

2. Selecione a conta de usuário cujo dispositivo móvel que você deseja adiciona à lista de dispositivos gerenciados.

3. No menu de contexto da conta do usuário, selecione **Adicionar dispositivo móvel**.

   O Assistente de conexão de novos dispositivos móveis é iniciado. Na janela **Origem do certificado** do assistente, você deve especificar o método para a criação do certificado compartilhado que o Servidor de Administração usará para identificar o dispositivo móvel. Você poderá especificar um certificado compartilhado usando uma das seguintes formas:

   - Crie um certificado compartilhado automaticamente, por meio das ferramentas do Servidor de Administração, e então entregue o certificado ao dispositivo.
   - Especifique um arquivo de certificado compartilhado.

4. Na janela **Tipo de dispositivo** do assistente, selecione **Link para o Google Play**.

5. Na janela **Método de notificação ao usuário**, do assistente, defina as configurações para a notificação ao usuário do dispositivo móvel sobre a criação do certificado (com uma mensagem SMS ou por e-mail ou ao exibir a informação quando o Assistente for concluído).

6. Na janela Informações do certificado do Assistente, clique no botão **Concluir** para fechar o Assistente.

Após o Assistente concluir as atividades, um link e um código QR serão enviados para o dispositivo móvel do usuário, permitindo que ele baixe o Kaspersky Endpoint Security no Google Play. O usuário segue para o Google Play ao usar o link ou ao digitalizar o código QR. Depois disto, o sistema operacional do dispositivo solicita que o usuário aceite a instalação do Kaspersky Endpoint Security for Android. Depois que Kaspersky Endpoint Security para Android for baixado e instalado, o dispositivo móvel conecta-se ao Servidor de Administração e baixa um certificado compartilhado. Após o certificado ter sido instalado no dispositivo móvel, este é exibido na pasta **Dispositivos móveis**, que é uma subpasta da pasta **Gerenciamento de Dispositivos Móveis** na árvore do console.

Se o Kaspersky Endpoint Security for Android já tiver sido instalado no dispositivo, o usuário precisa receber as configurações de conexão ao Servidor de Administração do administrador e, a seguir, inseri-las por si próprio. Após as configurações de conexão tiverem sido definidas, o dispositivo móvel conecta-se ao Servidor de Administração. O administrador emite um certificado compartilhado para o dispositivo e envia ao usuário uma mensagem por e-mail ou uma mensagem SMS com um login e senha para baixar o certificado. O usuário baixa e instala o certificado compartilhado. Após o certificado ter sido instalado no dispositivo móvel, este é exibido na pasta **Dispositivos móveis**, que é uma subpasta da pasta **Gerenciamento de Dispositivos Móveis** na árvore do console. Neste caso, o Kaspersky Endpoint Security for Android não será baixado e instalado novamente.

Conectar dispositivos KES ao Servidor de Administração

Dependendo do método usado para a conexão de dispositivos ao Servidor de Administração, dois esquemas de implementação são possíveis para o Kaspersky Device Management for iOS para dispositivo KES:

- Esquema de implementação com conexão direta dos dispositivos ao Servidor de Administração
- Esquema de implementação envolvendo um proxy reverso que dá suporte à delegação restrita de Kerberos

Conexão direta de dispositivos ao Servidor de Administração

Os dispositivos KES podem conectar-se diretamente à porta 13292 do Servidor de Administração.

Dependendo do método usado para a autenticação, duas opções são possíveis para a conexão de dispositivos KES ao Servidor de Administração:

- Conectar dispositivos com um certificado do usuário
- Conectar dispositivos sem um certificado do usuário

Conectar um dispositivo com um certificado do usuário

Ao conectar um dispositivo com um certificado do usuário, aquele dispositivo é associado com a conta de usuário à qual o certificado correspondente foi atribuído através das ferramentas do Servidor de Administração.

Neste caso, a autenticação SSL de duas vias (autenticação mútua) será usada. Tanto o Servidor de Administração quanto o dispositivo serão autenticados com certificados.

Conectar um dispositivo sem um certificado do usuário

Ao conectar um dispositivo sem um certificado do usuário, aquele dispositivo não se associa com nenhuma das contas de usuário no Servidor de Administração. No entanto, quando o dispositivo recebe qualquer certificado, ele é associado ao usuário ao qual o certificado correspondente foi atribuído através das ferramentas do Servidor de Administração.

Ao conectar aquele dispositivo ao Servidor de Administração, a autenticação SSL bilateral será aplicada, o que significa que somente o Servidor de Administração será autenticado com o certificado. Após o dispositivo recuperar o certificado do usuário, o tipo de autenticação mudará para a autenticação SSL bilateral (autenticação bilateral SSL, autenticação mútua).

Esquema para conectar dispositivos KES ao servidor envolvendo a delegação de restrição Kerberos (KCD)

O esquema para conectar dispositivos KES ao Servidor de Administração envolvendo a delegação restringida Kerberos (KCD) fornece o seguinte:

- Integração com um proxy reverso compatível com KCD.
- Uso do Kerberos Constrained Delegation (aqui referido como KCD) para a autenticação de dispositivos móveis.
- Integração com a Infraestrutura de chaves públicas (aqui referida como PKI) para aplicar certificados de usuário.

Ao usar este esquema de conexão, observe o seguinte:

- O tipo de conexão dos dispositivos KES com o proxy reverso deve ser "autenticação SSL bilateral", ou seja, um dispositivo deve se conectar ao proxy reverso por meio de seu certificado do usuário proprietário. Para fazer isto, você deve integrar o certificado do usuário no pacote de instalação de Kaspersky Endpoint Security for Android que foi instalado no dispositivo. Este pacote KES deve ser criado pelo Servidor de Administração especificamente para este dispositivo (usuário).
- Você deve especificar o certificado especial (personalizado) em vez do certificado de servidor padrão para o protocolo móvel:

  1. Na janela de propriedades do Servidor de Administração, na seção **Configurações**, marque a caixa de seleção **Abrir a porta para dispositivos móveis** e selecione **Adicionar certificado** na lista suspensa.
  2. Na janela exibida, especifique o mesmo certificado definido no proxy reverso quando o ponto de acesso ao protocolo móvel foi publicado no Servidor de Administração.

- Os certificados de usuário de dispositivos KES devem ser emitidos por Certificate Authority (CA) do domínio. Não se esqueça de que, se o domínio incluir CAs de múltiplas raízes, os certificados de usuário devem ser emitidos pela CA, definida na publicação no proxy reverso.

  Você pode assegurar-se de que o certificado do usuário esteja em conformidade com requisito acima descrito, usando um dos seguintes métodos:

  - Especifique o certificado do usuário especial no Assistente de novo pacote e no Assistente de instalação de certificados.
  - Integre o Servidor de Administração com o PKI do domínio e defina a configuração correspondente nas regras de emissão de certificados:

    1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis** e selecione a subpasta **Certificados**.
    2. No espaço de trabalho da pasta **Certificados**, clique no botão **Configurar as regras de emissão de certificados** para abrir a janela **Regras de emissão do certificado**.
    3. Na seção **Integração com PKI**, configure a integração com a infraestrutura de chaves públicas.
    4. Na seção **Emissão de certificados móveis**, especifique a origem dos certificados.

Abaixo encontra-se um exemplo da Kerberos Constrained Delegation (KCD) com as seguintes suposições:

- O ponto do acesso ao protocolo móvel no Servidor de Administração é definido na porta 13292.
- O nome do dispositivo com o proxy reverso é firewall.mydom.local.
- O nome do dispositivo com o Servidor de Administração é ksc.mydom.local.
- O nome da publicação externa do ponto de acesso ao protocolo móvel é kes4mob.mydom.global.

Conta de domínio para o Servidor de Administração

Você deve criar uma conta de domínio (por exemplo, KSCMobileSrvcUsr) sob a qual o serviço Servidor de Administração será executado. Você pode especificar uma conta do serviço Servidor de Administração ao instalar o Servidor de Administração ou através do utilitário klsrvswch. O utilitário klsrvswch está localizado na pasta de instalação do Servidor de Administração. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Uma conta de domínio deve ser especificada pelos seguintes motivos:

- O recurso para o gerenciamento de dispositivos KES é uma parte integral do Servidor de Administração.
- Para assegurar um funcionamento apropriado do Kerberos Constrained Delegation (KCD), o lado recebedor (ou seja, o Servidor de Administração) deve ser executado sob uma conta de domínio.

Nome do serviço principal para http/kes4mob.mydom.local

No domínio, sob a conta KSCMobileSrvcUsr, adicione um SPN para publicar o serviço de protocolo móvel na porta 13292 do dispositivo com o Servidor de Administração. Para o dispositivo kes4mob.mydom.local com o Servidor de Administração, isto aparecerá como segue:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Configuração das propriedades de domínio do dispositivo com o proxy reverso (firewall.mydom.local)

Para delegar o tráfego, é necessário confiar o dispositivo com o proxy reverso (firewall.mydom.local) ao serviço definido pelo SPN (http/kes4mob.mydom.local:13292).

Para confiar o dispositivo com proxy reverso ao serviço definido pelo SPN (http/kes4mob.mydom.local:13292), o administrador deve executar as seguintes ações:

1. No snap-in Microsoft Management Console nomeado "usuários e computadores do Active Directory", selecione o dispositivo com o proxy reverso instalado (firewall.mydom.local).
2. Nas propriedades do dispositivo, na guia **Delegação**, defina **Confiar neste computador somente para a delegação ao serviço especificado** alterne para **Usar qualquer protocolo de autenticação**.
3. Na lista **Serviços aos quais esta conta pode apresentar credenciais delegadas**, adicione o SPN http/kes4mob.mydom.local:13292.

Certificado especial (personalizado) para a publicação (kes4mob.mydom.global)

Para publicar o protocolo móvel do Servidor de Administração, você deve emitir um certificado especial (personalizado) para o FQDN kes4mob.mydom.global e especificá-lo em vez do certificado de servidor padrão nas configurações do protocolo móvel do Servidor de Administração no Console de Administração. Para fazer isso, na janela de propriedades do Servidor de Administração, na seção **Configurações**, selecione a caixa de seleção **Abrir a porta para dispositivos móveis** e, a seguir, selecione **Adicionar certificado** na lista suspensa.

Observe que o contêiner de certificado do servidor (arquivo com a extensão p12 ou pfx) também deve conter uma cadeia de certificados raiz (chaves públicas).

Configuração da publicação no proxy reverso

No proxy reverso, para o tráfego que vai de um dispositivo móvel até a porta 13292 do kes4mob.mydom.global, é necessário configurar a KCD no SPN (http/kes4mob.mydom.global:13292) usando o certificado emitido para o FQND (kes4mob.mydom.global). Observe que publicar e ponto de acesso publicado (porta 13292 do Servidor de Administração) deve compartilhar o mesmo certificado de servidor.

Usar o Firebase Cloud Messaging

Para assegurar a entrega em tempo dos comandos para dispositivos KES gerenciados pela sistema operacional Android, o Kaspersky Security Center usa o mecanismo de notificações push. As notificações push são trocadas entre os dispositivos KES e o Servidor de Administração por meio do Firebase Cloud Messaging (aqui referido como FCM). No Console de Administração do Kaspersky Security Center, é possível especificar as configurações do Firebase Cloud Messaging para conectar dispositivos KES ao serviço.

Para recuperar as configurações do Firebase Cloud Messaging, é necessário ter uma conta do Google.

Para ativar o uso do FCM:

1. No console de administração, selecione o nó **Gerenciamento de Dispositivos Móveis** e a pasta **Dispositivos móveis**.
2. No menu de contexto da pasta **Dispositivos móveis**, selecione **Propriedades**.
3. Nas propriedades da pasta, selecione a seção **Configurações do Google Firebase Cloud Messaging**.
4. No campo **ID do Remetente**, especifique o ID do remetente do FCM.
5. No campo **Arquivo de chave privada (em formato JSON)**, selecione o arquivo de chave privada.

   Na próxima sincronização com o Servidor de Administração, os dispositivos KES gerenciados por sistemas operacionais Android serão conectados ao Firebase Cloud Messaging.

É possível editar as configurações do Firebase Cloud Messaging clicando no botão **Redefinir as configurações**.

Ao alternar para um projeto diferente do Firebase, é necessário aguardar 10 minutos para que o FCM seja retomado.

O serviço FCM é executado nas seguintes faixas de endereços:

- Do dispositivo KES, o acesso é necessário às portas 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) e 5230 (HTTPS) dos seguintes endereços:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Todos dos endereços IP listados no ASN da Google de 15169
- No Servidor de Administração, o acesso é necessário à porta 443 (HTTPS) dos seguintes endereços:
  - fcm.googleapis.com
  - Todos dos endereços IP listados no ASN da Google de 15169

Se as configurações do servidor proxy (**Avançado** / **Configurações de conexão à Internet**) tiverem sido especificadas nas propriedades do Servidor de Administração no Console de Administração, elas serão usadas para a interação com o FCM.

Como configurar o FCM: obter o ID do remetente e o arquivo de chave privada

Para configurar o FCM:

1. Registre-se no portal do Google.
2. Acesse o Console do Firebase.
3. Execute uma das seguintes ações:
   - Para criar um novo projeto, clique em **Criar um projeto** e siga as instruções na tela.
   - Abra um projeto existente.
4. Clique no ícone de engrenagem e escolha **Configurações do projeto**.
   A janela **Configurações do projeto** é aberta.
5. Selecione a guia **Mensagens na nuvem**.
6. Obtenha o ID do remetente relevante no campo **ID do remetente** na seção **Firebase Cloud Messaging API (V1)**.
7. Selecione a guia **Contas de serviço** e clique em **Gerar nova chave privada**.
8. Na janela exibida, clique em **Gerar chave** para gerar e baixar um arquivo de chave privada.

O Firebase Cloud Messaging agora está configurado.

Integração com a infraestrutura de chaves públicas

A integração com a infraestrutura de chaves públicas (aqui referido como PKI) é principalmente destinada para simplificar a emissão de certificados de usuário de domínio pelo Servidor de Administração.

O administrador pode atribuir um certificado de domínio para um usuário no Console de Administração. Isto pode ser feito usando um dos seguintes métodos:

- Atribuir ao usuário um certificado especial (personalizado) de um arquivo no Assistente de instalação de certificados.
- Execute a integração com PKI e atribua o PKI a atuar como a fonte de certificados de um tipo específico de certificados ou para todos os tipos de certificados.

As configurações de integração com a PKI estão disponíveis na área de trabalho da pasta **Gerenciamento de Dispositivos Móveis** / **Certificados** ao clicar no link **Integrar com infraestrutura de chave pública**.

Princípio geral de integração com PKI para a emissão de certificados de usuário de domínio

No Console de Administração, clique no link **Integrar com infraestrutura de chave pública** no espaço de trabalho da pasta **Gerenciamento de Dispositivos Móveis** / **Certificados** que será usada pelo Servidor de Administração para emitir os certificados do usuário do domínio através do CA do domínio CA (aqui referido como a conta sob a qual a integração com PKI é executada).

Observe o seguinte:

- As configurações da integração com PKI fornecem-lhe a possibilidade de especificar o modelo padrão para todos os tipos de certificados. Observe que as regras de emissão de certificados (disponível no espaço de trabalho da pasta **Gerenciamento de Dispositivos Móveis**/**Certificados** clicando no botão **Configurar as regras de emissão de certificados**) permitem especificar um modelo individual para cada tipo de certificado.
- Um certificado de Enrollment Agent (EA) especial deve ser instalado no dispositivo com o Servidor de Administração, no repositório de certificados da conta sob a qual a integração com PKI é executada. O certificado Enrollment Agent (EA) é emitido pelo administrador da CA do domínio (Autoridade de Certificado).

A conta sob a qual a integração com PKI é executada deve atender os seguintes critérios:

- É um usuário do domínio.
- É um administrador local do dispositivo com o Servidor de Administração a partir do qual a integração com PKI é iniciada.
- Tem o direito de fazer *Login como serviço*.
- O dispositivo com o Servidor de Administração instalado deve ser executado ao menos uma vez sob desta conta para criar um perfil de usuário permanente.

Servidor Web do Kaspersky Security Center

O Servidor Web do Kaspersky Security Center (aqui referido como Servidor Web) é um componente do Kaspersky Security Center. O Servidor da Web foi projetado para publicar pacotes de instalação independentes, pacotes de instalação independentes para dispositivos móveis, perfis MDM do iOS e arquivos da pasta compartilhada.

Os perfis MDM do iOS e os pacotes de instalação que foram criados são publicados no Servidor da Web automaticamente e então removidos depois do primeiro download. O administrador pode enviar o novo link ao usuário de qualquer forma prática: por exemplo, por e-mail.

Ao clicar no link, o usuário poderá baixar as informações necessárias para um dispositivo móvel.

Configurações do servidor da Web

Se um ajuste fino do Servidor da Web for necessário, a propriedades do Console de Administração do Servidor da Web fornecem a possibilidade de alterar as portas para HTTP (8060) e HTTPS (8061). Além de alterar as portas, você pode substituir o certificado do servidor por HTTPS e alterar o FQDN o servidor da Web para HTTP.

Instalação do Kaspersky Security Center

Esta seção descreve os componentes de instalação do Kaspersky Security Center. Se você deseja instalar o aplicativo localmente em apenas um dispositivo, duas opções de instalação estão disponíveis:

- **Padrão**. Esta opção é recomendada se você quiser testar o Kaspersky Security Center ao, por exemplo, testar a sua operação em uma pequena área dentro sua rede. Durante a instalação padrão, você somente configura o banco de dados. Você também pode instalar somente o conjunto padrão de plugins de gerenciamento de aplicativos Kaspersky. Você também poderá usar a instalação padrão se já tiver alguma experiência em trabalhar com o Kaspersky Security Center e conseguir especificar todas as configurações relevantes após a instalação padrão.

- **Personalizada**. Esta opção será recomendada se você planejar modificar as configurações do Kaspersky Security Center, como o caminho para a pasta compartilhada, contas, e portas para a conexão ao Servidor de Administração e as configurações do banco de dados. A instalação personalizada permite especificar quais plugins de gerenciamento da Kaspersky devem ser instalados. Caso necessário, é possível iniciar a instalação personalizada no modo silencioso.

Se pelo menos um Servidor de Administração estiver instalado na rede, os Servidores podem ser instalados em outros dispositivos remotamente através da tarefa de instalação remota usando a instalação conseguida. Ao criar a tarefa de instalação remota, você deve usar o pacote de instalação do Servidor de Administração: ksc_<número_da_versão> .<número da compilação> _full_<idioma da localização>.exe.

Use este pacote se quiser instalar todos os componentes necessários para a funcionalidade completa do Kaspersky Security Center ou para atualizar as versões atuais destes componentes.

Caso queira implementar o cluster de failover do Kaspersky Security Center, será preciso instalar o Kaspersky Security Center em todos os nós do cluster.

Preparar para instalar

Execute as seguintes ações antes de iniciar a instalação.

- **Verifique os requisitos de hardware e software**

  Confirme se o hardware e o software do dispositivo atendem aos requisitos do Servidor de Administração e do Console de Administração.

- **Selecione e instale o sistema de gerenciamento de banco de dados (DBMS)**

  O Kaspersky Security Center armazena suas informações em um banco de dados gerenciado por um DBMS. Instale o DBMS na rede antes do Kaspersky Security Center (saiba mais sobre como selecionar um DBMS). Caso decida instalar o PostgreSQL ou Postgres Pro DBMS, especifique uma senha para o superusuário. Se a senha não for especificada, o Servidor de Administração pode não conseguir se conectar ao banco de dados.

  Recomenda-se instalar o Servidor de Administração em um servidor dedicado em vez de um controlador de domínio. Porém, ao instalar o Kaspersky Security Center em um servidor que atua como controlador de domínio somente leitura (RODC), o Microsoft SQL Server (SQL Express) não deve estar instalado localmente (no mesmo dispositivo). Nesse caso, recomendamos que você instale o Microsoft SQL Server (SQL Express) remotamente (em um outro dispositivo) ou use MySQL, MariaDB ou PostgreSQL se precisar instalar o DBMS localmente.

- **Preparar pastas para o Servidor de Administração, Agente de Rede e Console de Administração**

  O Servidor de Administração, o Agente de Rede e o Console de Administração devem ser instalados em pastas onde a distinção entre maiúsculas e minúsculas não esteja habilitada. Além disso, a diferenciação entre maiúsculas e minúsculas deve ser desativada para a pasta compartilhada do Servidor de Administração e a pasta oculta do Kaspersky Security Center (%ALLUSERSPROFILE%\KasperskyLab\adminkit).

- **Remova o Agente de Rede antigo**

  A versão do servidor do Agente de Rede será instalada no dispositivo junto com o Servidor de Administração. O Servidor de Administração não pode ser instalado junto com a versão regular do Agente de Rede. Se a versão do servidor do Agente de Rede já estiver instalada em seu dispositivo, remova-a e reinicie a instalação do Servidor de Administração. Para obter os detalhes sobre a versão do servidor do Agente de Rede, consulte Alterações no sistema após a instalação do Kaspersky Security Center.

- **Verificação de contas**

  A instalação do Kaspersky Security Center necessita de direitos de administrador no dispositivo no qual a instalação é executada.

  O Kaspersky Security Center dá suporte a contas de serviço gerenciadas e contas de serviço gerenciadas em grupo. Se esses tipos de contas forem usadas no seu domínio e você desejar especificar uma delas como a conta do serviço do Servidor de Administração, instale primeiro a conta no mesmo dispositivo em que deseja instalar o Servidor de Administração. Para detalhes sobre a instalação de contas de serviço gerenciadas em um dispositivo local, consulte a documentação oficial da Microsoft.

Contas para trabalhar com o DBMS

Para instalar o Servidor de Administração e trabalhar com ele, você precisa de uma conta do Windows para executar o instalador do Servidor de Administração (adiante também denominado instalador) e para iniciar o serviço do Servidor de Administração, além de uma conta de DBMS interno para acessar o DBMS. Você pode criar novas contas ou usar as existentes. Todas essas contas requerem direitos específicos. Um conjunto de contas necessárias e seus direitos depende dos seguintes critérios:

- Tipo de DBMS:
  - Microsoft SQL Server (com autenticação do Windows e com autenticação do SQL Server)
  - MySQL ou MariaDB
  - PostgreSQL or Postgres Pro
- Localização do DBMS:
  - **DBMS local**. O *DBMS local* é um DBMS instalado no mesmo dispositivo que o do Servidor de Administração.
  - **DBMS remoto**. O *DBMS remoto* é um DBMS instalado em um dispositivo diferente.
- Método de criação do banco de dados do Servidor de Administração:
  - **Automático**. Durante a instalação do Servidor de Administração, é possível criar automaticamente um banco de dados do Servidor de Administração (doravante também denominado banco de dados do Servidor) usando o instalador.
  - **Manual**. Você pode usar um aplicativo de terceiros (por exemplo, SQL Server Management Studio) ou um script para criar um banco de dados vazio. Depois disso, você pode especificar este banco de dados como o banco de dados do Servidor durante a instalação do Servidor de Administração.

Siga o princípio do menor privilégio ao conceder direitos e permissões às contas. Isso significa que os direitos concedidos devem ser suficientes apenas para executar as ações necessárias.

As tabelas abaixo contêm informações sobre os direitos do sistema e os direitos do DBMS que você deve conceder às contas antes de instalar e iniciar o Servidor de Administração.

Microsoft SQL Server com autenticação do Windows

Se você escolher o SQL Server como DBMS, poderá usar a autenticação do Windows para acessar o SQL Server. Configure os direitos do sistema para uma conta do Windows usada para executar o instalador e uma conta do Windows usada para iniciar o serviço do Servidor de Administração. No SQL Server, crie logins para ambas as contas do Windows. Dependendo do método de criação do banco de dados do servidor, conceda os direitos necessários do SQL Server a essas contas, conforme descrito na tabela abaixo. Para obter mais informações sobre como configurar os direitos das contas, consulte Configurando contas para uso com SQL Server (autenticação do Windows).

DBMS: Microsoft SQL Server (incluindo a Express Edition) com a autenticação do Windows

	Criação automática de banco de dados (pelo instalador)	Criação manual de banco de dados (pelo Administrador)
Conta sob a qual o Instalador está sendo executado	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto no qual o DBMS está instalado. • DBMS local: uma conta de administrador local ou uma conta de domínio.	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto no qual o DBMS está instalado. • DBMS local: uma conta de administrador local ou uma conta de domínio.

Direitos à conta sob a qual o Instalador está sendo executado	• Direitos do sistema: direitos de administrador local.
	• Direitos do SQL Server:
	  • Função no nível do servidor: sysadmin.
		• Direitos do sistema: direitos de administrador local.
		• Direitos do SQL Server:
		  • Função no nível do servidor: público.
		  • Participação na função de banco de dados para o banco de dados do Servidor: db_owner, public.
		  • Esquema padrão para o banco de dados do Servidor: dbo.

Conta de serviço do Servidor de Administração	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto no qual o DBMS está instalado.
	• DBMS local:
	  • Uma conta do Windows escolhida pelo administrador.
	  • Uma conta no formato KL-AK-* que o instalador cria automaticamente.
		• DBMS remoto: apenas uma conta de domínio do dispositivo remoto no qual o DBMS está instalado.
		• DBMS local:
		  • Uma conta do Windows escolhida pelo administrador.
		  • Uma conta no formato KL-AK-* que o instalador cria automaticamente (neste caso, não recomendamos gerar uma conta KL-AK-*).

Direitos à conta do serviço do Servidor de Administração	• Sistema de direitos: os direitos necessários atribuídos pelo instalador.
	• Direitos do SQL Server: os direitos necessários atribuídos pelo instalador.
		• Sistema de direitos: os direitos necessários atribuídos pelo instalador.
		• Direitos do SQL Server:
		  • Função no nível do servidor: público.
		  • Participação na função de banco de dados para o banco de dados do Servidor: db_owner, public.
		  • Esquema padrão para o banco de dados do Servidor: dbo.

Microsoft SQL Server com autenticação do SQL Server

Se você escolher o SQL Server como DBMS, poderá usar a autenticação do SQL Server para acessar o SQL Server. Configure os direitos do sistema para uma conta do Windows usada para executar o instalador e para uma conta do Windows usada para iniciar o serviço do Servidor de Administração. No SQL Server, crie um login com senha para usá-lo para autenticação. Em seguida, conceda a esta conta do SQL Server os direitos necessários listados na tabela abaixo. Para obter mais informações sobre como configurar os direitos das contas, consulte Configurando contas para uso com SQL Server (autenticação do SQL Server).

DBMS: Microsoft SQL Server (incluindo a Express Edition) com autenticação do SQL Server

	Criação automática de banco de dados (pelo instalador)	Criação manual de banco de dados (pelo Administrador)
Conta sob a qual o Instalador está sendo executado	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto no qual o DBMS está instalado. • DBMS local: uma conta de administrador local ou uma conta de domínio.	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto no qual o DBMS está instalado. • DBMS local: uma conta de administrador local ou uma conta de domínio.
Direitos à conta sob a qual o Instalador está sendo executado	Direitos do sistema: direitos de administrador local.	Direitos do sistema: direitos de administrador local.

	Criação automática de banco de dados (pelo instalador)	Criação manual de banco de dados (pelo Administrador)

Conta de serviço do Servidor de Administração	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto no qual o DBMS está instalado.
	• DBMS local:
	  • Uma conta do Windows escolhida pelo administrador.
	  • Uma conta no formato KL-AK-* que o instalador cria automaticamente.
		• DBMS remoto: apenas uma conta de domínio do dispositivo remoto no qual o DBMS está instalado.
		• DBMS local:
		  • Uma conta de usuário do Windows escolhida pelo administrador.
		  • Uma conta no formato KL-AK-* que o instalador cria automaticamente.

Direitos à conta do serviço do Servidor de Administração	Sistema de direitos: os direitos necessários atribuídos pelo instalador.	Sistema de direitos: os direitos necessários atribuídos pelo instalador.

Direitos do login usado para autenticação do SQL Server	Direitos do SQL Server necessários para criar um banco de dados e instalar o Servidor de Administração:
	• Função no nível do servidor: público.
	• Associação da função de banco de dados para o banco de dados *mestre*: db_owner.
	• Esquema padrão para o banco de dados *mestre*: dbo.
	• Permissões:
	  • CONNECT ANY DATABASE
	  • CONNECT SQL
	  • CREATE ANY DATABASE
	  • VIEW ANY DATABASE
	  • VIEW SERVER STATE (caso a opção **Sempre Ativado** esteja ativada)
	Direitos do SQL Server necessários para uso com o Servidor de Administração:
	• Função no nível do servidor: público.
	• Associação da função de banco de dados para o banco de dados do Servidor: db_owner.
	• Esquema padrão para o banco de dados do Servidor: dbo.
	• Permissões:
	  • CONNECT SQL
	  • VIEW ANY DATABASE
	  • VISUALIZAR ESTADO DO SERVIDOR (caso a opção **Sempre Ativado** esteja ativada)
	  • EXIBIR QUALQUER DEFINIÇÃO
		Direitos do SQL Server:
		• Função no nível do servidor: público.
		• Associação da função de banco de dados para o banco de dados do Servidor: db_owner.
		• Esquema padrão para o banco de dados do Servidor: dbo.
		• Permissões:
		  • CONNECT SQL
		  • VIEW ANY DATABASE
		  • EXIBIR QUALQUER DEFINIÇÃO

Configurar direitos do SQL Server para recuperação de dados do Servidor de Administração

Para restaurar dados do Servidor de Administração do backup, execute o utilitário klbackup na conta do Windows usada para instalar o Servidor de Administração. Antes de iniciar o utilitário klbackup, no SQL Server, conceda os direitos para o login do SQL Server associado a essa conta do Windows. Os direitos do SQL Server são diferentes dependendo da versão do Servidor de Administração. Para o Servidor de Administração da versão 14.2 ou posterior, é possível conceder a função no nível do servidor sysadmin ou a função no nível do servidor dbcreator.

Direitos do SQL Server para a recuperação do banco de dados de administração

Servidor de Administração versão 14.2 ou posterior	Outras versões do Servidor de Administração

• Direitos do SQL Server:
  • Função no nível do servidor: dbcreator.
• Permissões:
  • EXIBIR QUALQUER DEFINIÇÃO
Antes de iniciar o utilitário klbackup, especifique o sinalizador do servidor KLSRV_SKIP_ADJUSTING_DBMS_ACCESS. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Em seguida, execute o seguinte comando na linha de comando:
`klscflag.exe -fset -pv klserver -n KLSRV_SKIP_ADJUSTING_DBMS_ACCESS -t d -v 1`	

MySQL e MariaDB

Se você escolher MySQL ou MariaDB como DBMS, crie uma conta interna do DBMS e conceda a essa conta os direitos necessários relacionados na tabela abaixo. O instalador e o serviço do Servidor de Administração usam essa conta de DBMS interna para acessar o DBMS. Observe que o método de criação do banco de dados não afeta o conjunto de direitos necessários. Para obter mais informações sobre como configurar os direitos da conta, consulte Configuração de contas para uso com MySQL e MariaDB.

DBMS: MySQL e MariaDB

	Criação de banco de dados automática ou manual
Conta sob a qual o Instalador está sendo executado	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto com o DBMS instalado. • DBMS local: uma conta de administrador local ou uma conta de domínio.
Direitos à conta sob a qual o Instalador está sendo executado	Direitos do sistema: direitos de administrador local.

Conta de serviço do Servidor de Administração	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto com o DBMS instalado.
	• DBMS local:
	  • Uma conta do Windows escolhida pelo administrador.
	  • Uma conta no formato KL-AK-* que o instalador cria automaticamente.

Direitos à conta do serviço do Servidor de Administração	Sistema de direitos: os direitos necessários atribuídos pelo instalador.
Direitos da conta interna do DBMS	Privilégios do esquema: • Banco de dados do Servidor de Administração: ALL (excluindo GRANT OPTION). • Esquemas do sistema (mysql e sys): SELECT, SHOW VIEW. • O procedimento armazenado sys.table_exists: EXECUTE (caso use o MariaDB 10.5 ou anterior como um DBMS, não será necessário conceder o privilégio EXECUTE). Privilégios globais para todos os esquemas: PROCESS, SUPER.

Para obter informações sobre como mover dados de um espaço de tabela compartilhado para um espaço de tabela individual, consulte Mover dados de um espaço de tabela compartilhado para um espaço de tabela individual nos DBMSs MySQL e MariaDB.

Configurar privilégios para recuperação de dados do Servidor de Administração

Os direitos que você concedeu à conta interna do DBMS são suficientes para restaurar dados do Servidor de Administração do backup. Para iniciar a restauração, execute o utilitário klbackup na conta do Windows usada para instalar o Servidor de Administração.

PostgreSQL or Postgres Pro

Caso escolha o PostgreSQL ou Postgres Pro como DBMS, é possível utilizar o usuário *Postgres* (a função padrão do Postgres) ou criar uma nova função Postgres (adiante também denominada função) para acessar o DBMS. Dependendo do método de criação do banco de dados do servidor, conceda os direitos necessários à função, conforme descrito na tabela abaixo. Para obter mais informações sobre como configurar os direitos da função, consulte Configurando contas para uso com PostgreSQL ou Postgres Pro.

DBMS: PostgreSQL ou Postgres Pro

	Criação automática de banco de dados		Criação manual de banco de dados
Conta sob a qual o Instalador está sendo executado	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto com o DBMS instalado. • DBMS local: uma conta de administrador local ou uma conta de domínio.		• DBMS remoto: apenas uma conta de domínio do dispositivo remoto com o DBMS instalado. • DBMS local: uma conta de administrador local ou uma conta de domínio.
Direitos à conta sob a qual o Instalador está sendo executado	Direitos do sistema: direitos de administrador local.		Direitos do sistema: direitos de administrador local.

Conta de serviço do Servidor de Administração	• DBMS remoto: apenas uma conta de domínio do dispositivo remoto com o DBMS instalado.
	• DBMS local:
	  • Uma conta do Windows escolhida pelo administrador.
	  • Uma conta no formato KL-AK-* que o instalador cria automaticamente.
			• DBMS remoto: apenas uma conta de domínio do dispositivo remoto com o DBMS instalado.
			• DBMS local:
			  • Uma conta do Windows escolhida pelo administrador.
			  • Uma conta no formato KL-AK-* que o instalador cria automaticamente.

Direitos à conta do serviço do Servidor de Administração	Sistema de direitos: os direitos necessários atribuídos pelo instalador.		Sistema de direitos: os direitos necessários atribuídos pelo instalador.
Direitos da função do Postgres	O usuário do *Postgres* não requer direitos adicionais.	Privilégios para uma nova função: `CREATEDB`.	Para uma nova função: • Privilégios no banco de dados do Servidor de Administração: `ALL`. • Privilégios em todas as tabelas no esquema público: `ALL`. • Privilégios em todas as sequências no esquema público: `ALL`.

Configurar privilégios para recuperação de dados do Servidor de Administração

Para restaurar dados do Servidor de Administração do backup, execute o utilitário klbackup na conta do Windows usada para instalar o Servidor de Administração. Observe que a função do Postgres usada para acessar o DBMS deve ter direitos de proprietário no banco de dados do Servidor de Administração.

Configurando contas para trabalhar com SQL Server (autenticação do Windows)

Pré-requisitos

Antes de atribuir direitos às contas, execute as seguintes ações:

1. Certifique-se de fazer login no sistema com a conta de administrador local.
2. Instale um ambiente para uso com SQL Server.
3. Certifique-se de ter uma conta do Windows na qual instalará o Servidor de Administração.
4. Certifique-se de ter uma conta do Windows na qual iniciará o serviço do Servidor de Administração.
5. No SQL Server, crie um login para a conta do Windows usada para executar o instalador do Servidor de Administração (adiante também denominado instalador). Crie também um login para a conta do Windows usada para iniciar o serviço do Servidor de Administração.

Caso o SQL Server Management Studio seja usado, na página **Geral** da janela de propriedades de login, selecione a opção **Autenticação do Windows**.

Caso queira instalar o Servidor de Administração e o SQL Server em dispositivos localizados em domínios do Windows separados, observe que esses domínios devem ter relações confiáveis bidirecionais para garantir a operação correta do Servidor de Administração, inclusive a execução de tarefas e a aplicação de políticas. Para obter informações sobre as contas necessárias para uso com vários DBMSs e os direitos das contas, consulte contas para funcionar com o DBMS.

Configuração de contas para instalar o Servidor de Administração (criação automática do banco de dados do Servidor de Administração)

Para configurar as contas para a instalação do Servidor de Administração:

1. No SQL Server, atribua a função de nível de servidor sysadmin ao login da conta do Windows usada para executar o instalador.
2. Faça login no sistema com a conta do Windows usada para executar o instalador.
3. Execute o instalador do Servidor de Administração.

   O Assistente de instalação do Servidor de Administração é iniciado. Siga as instruções do Assistente.
4. Selecione a opção instalação personalizada do Servidor de Administração.
5. Selecione o Microsoft SQL Server como DBMS que armazena o banco de dados do Servidor de Administração.

6. Selecione o modo de autenticação do Microsoft Windows para estabelecer uma conexão entre o Servidor de Administração e o SQL Server por meio de uma conta do Windows.

7. Especifique a conta de Windows usada para iniciar o serviço do Servidor de Administração.

   É possível selecionar a conta de usuário do Windows para a qual um login do SQL Server foi criado anteriormente. Como alternativa, você pode criar automaticamente uma nova conta do Windows no formato KL-AK-* usando o instalador. Nesse caso, o instalador cria automaticamente um login do SQL Server para essa conta. Independentemente da escolha da conta, o instalador atribui os direitos de sistema e os direitos do SQL Server necessários à conta de serviço do Servidor de Administração.

Após a conclusão da instalação, o banco de dados do Servidor é criado e todos os direitos de sistema e direitos do SQL Server necessários são atribuídos à conta de serviço do Servidor de Administração. O Servidor de Administração está pronto para uso.

Configuração de contas para instalar o Servidor de Administração (criação manual do banco de dados do Servidor de Administração)

Para configurar as contas para a instalação do Servidor de Administração:

1. No SQL Server, crie um banco de dados vazio. Este banco de dados será usado como banco de dados do Servidor de Administração (adiante também denominado banco de dados do Servidor).

2. Para ambos os logins do SQL Server criados para as contas do Windows, especifique a função de nível de servidor público e, em seguida, configure o mapeamento para o banco de dados criado:

   - Função no nível do servidor: público
   - Associação de função de banco de dados: db_owner, público
   - Esquema padrão: dbo

3. Faça login no sistema com a conta do Windows usada para executar o instalador.

4. Execute o instalador do Servidor de Administração.

   O Assistente de instalação do Servidor de Administração é iniciado. Siga as instruções do Assistente.

5. Selecione a opção instalação personalizada do Servidor de Administração.

6. Selecione o Microsoft SQL Server como DBMS que armazena o banco de dados do Servidor de Administração.

7. Especifique o nome do banco de dados criado como o nome do banco de dados do Servidor de Administração.

8. Selecione o modo de autenticação do Microsoft Windows para estabelecer uma conexão entre o Servidor de Administração e o SQL Server por meio de uma conta do Windows.

9. Especifique a conta de Windows usada para iniciar o serviço do Servidor de Administração.

   É possível selecionar a conta de usuário do Windows para a qual um login do SQL Server foi criado e cujos direitos foram configurados anteriormente.

Não recomendamos que você crie automaticamente uma nova conta do Windows no formato KL-AK-*. Nesse caso, o instalador criará uma nova conta do Windows para a qual você não criou nem configurou uma conta do SQL Server. O Servidor de Administração não pode usar esta conta para iniciar o serviço do Servidor de Administração. Se for necessário criar uma conta Windows KL-AK-*, não inicie o Console de Administração após a instalação. Em vez disso, faça o seguinte:

1. Pare o serviço kladminserver.
2. No SQL Server, crie um login do SQL Server para a conta KL-AK-* do Windows criada.
3. Conceda os direitos a este login do SQL Server e configure o mapeamento para o banco de dados criado:
   - Função no nível do servidor: público
   - Associação de função de banco de dados: db_owner, público
   - Esquema padrão: dbo
4. Reinicie o serviço kladminserver e, em seguida, execute o Console de Administração.

Após a conclusão da instalação, o Servidor de Administração usará o banco de dados criado para armazenar os dados do Servidor. O Servidor de Administração está pronto para uso.

Configurar contas para trabalhar com SQL Server (autenticação do SQL Server)

Pré-requisitos

Antes de atribuir direitos às contas, execute as seguintes ações:

1. Certifique-se de fazer login no sistema com a conta de administrador local.
2. Instale um ambiente para uso com SQL Server.
3. Certifique-se de ter uma conta do Windows na qual instalará o Servidor de Administração.
4. Certifique-se de ter uma conta do Windows na qual iniciará o serviço do Servidor de Administração.
5. No SQL Server, ative o modo de autenticação do SQL Server.

   Caso o SQL Server Management Studio seja usado, na janela de propriedades do SQL Server, na página **Segurança**, selecione a opção **modo de autenticação do SQL Server e do Windows**.
6. No SQL Server, crie um login com uma senha. O instalador do Servidor de Administração (adiante também denominado instalador) e o serviço do Servidor de Administração usarão essa conta de SQL Server para acessá-lo.

   Se você usar o SQL Server Management Studio, na página **Geral** da janela de propriedades de login, selecione a opção **Autenticação do SQL Server**.

Caso queira instalar o Servidor de Administração e o SQL Server em dispositivos localizados em domínios do Windows separados, observe que esses domínios devem ter relações confiáveis bidirecionais para garantir a operação correta do Servidor de Administração, inclusive a execução de tarefas e a aplicação de políticas. Para obter informações sobre as contas necessárias para uso com vários DBMSs e os direitos das contas, consulte contas para funcionar com o DBMS.

Configuração de contas para instalar o Servidor de Administração (criação automática do banco de dados do Servidor de Administração)

Para configurar as contas para a instalação do Servidor de Administração:

1. No SQL Server, mapeie a conta do SQL Server para o padrão banco de dados *mestre*. O banco de dados *mestre* é um modelo para o banco de dados do Servidor de Administração (adiante também denominado banco de dados do Servidor). O banco de dados *mestre* será usado para mapeamento até que o instalador crie um banco de dados do Servidor. Conceda os seguintes direitos e permissões à conta do SQL Server:
   - Função no nível do servidor: público
   - Associação da função de banco de dados para o banco de dados *mestre*: db_owner
   - Esquema padrão para o banco de dados *mestre*: dbo
   - Permissões:
     - CONNECT ANY DATABASE
     - CONNECT SQL
     - CREATE ANY DATABASE
     - VIEW ANY DATABASE
2. Faça login no sistema com a conta do Windows usada para executar o instalador.
3. Execute o instalador.

   O Assistente de instalação do Servidor de Administração é iniciado. Siga as instruções do Assistente.
4. Selecione a opção instalação personalizada do Servidor de Administração.
5. Selecione o Microsoft SQL Server como DBMS que armazena o banco de dados do Servidor de Administração.
6. Especifique o Nome do banco de dados do Servidor de Administração.
7. Selecione o modo de autenticação do SQL Server para estabelecer uma conexão entre o Servidor de Administração e o SQL Server por meio da conta do SQL Server. Em seguida, especifique as credenciais da conta do SQL Server.
8. Especifique a conta de Windows usada para iniciar o serviço do Servidor de Administração.

   É possível selecionar uma conta de usuário do Windows existente ou criar uma nova conta do Windows no formato KL-AK-* usando o instalador. Independentemente da escolha da conta, o instalador atribui os direitos de sistema necessários à conta de serviço do Servidor de Administração.

Após a conclusão da instalação, o banco de dados do Servidor é criado e todos os direitos de sistema são atribuídos à conta de serviço do Servidor de Administração. O Servidor de Administração está pronto para uso.

É possível cancelar o mapeamento para o banco de dados *principal*, porque o instalador criou um banco de dados do Servidor e configurou o mapeamento para esse banco de dados durante a instalação do Servidor de Administração.

Como a criação automática do banco de dados requer mais permissões do que o trabalho normal com o Servidor de Administração, você pode revogar algumas permissões. No SQL Server, selecione a conta do SQL Server e, em seguida, conceda os seguintes direitos para uso com o Servidor de Administração:

- Função no nível do servidor: público
- Associação da função de banco de dados para o banco de dados do Servidor: db_owner
- Esquema padrão para o banco de dados do Servidor: dbo
- Permissões:
  - CONNECT SQL
  - VIEW ANY DATABASE

Configuração de contas para instalar o Servidor de Administração (criação manual do banco de dados do Servidor de Administração)

Para configurar as contas para a instalação do Servidor de Administração:

1. No SQL Server, crie um banco de dados vazio. Este banco de dados será usado como um banco de dados do Servidor de Administração.
2. No SQL Server, conceda os seguintes direitos e permissões à conta do SQL Server:
   - Função no nível do servidor: público.
   - Associação da função de banco de dados para o banco de dados criado: db_owner.
   - Esquema padrão para o banco de dados criado: dbo.
   - Permissões:
     - CONNECT SQL
     - VIEW ANY DATABASE
3. Faça login no sistema com a conta do Windows usada para executar o instalador.
4. Execute o instalador.

   O Assistente de instalação do Servidor de Administração é iniciado. Siga as instruções do Assistente.
5. Selecione a opção instalação personalizada do Servidor de Administração.
6. Selecione o Microsoft SQL Server como DBMS que armazena o banco de dados do Servidor de Administração.
7. Especifique o nome do banco de dados criado como o nome do banco de dados do Servidor de Administração.

8. Selecione o modo de autenticação do SQL Server para estabelecer uma conexão entre o Servidor de Administração e o SQL Server por meio da conta do SQL Server. Em seguida, especifique as credenciais da conta do SQL Server.

9. Especifique a conta de Windows usada para iniciar o serviço do Servidor de Administração.

   É possível selecionar uma conta de usuário do Windows existente ou criar uma nova conta do Windows no formato KL-AK-* usando o instalador. Independentemente da escolha da conta, o instalador atribui os direitos de sistema necessários à conta de serviço do Servidor de Administração.

Após a conclusão da instalação, o Servidor de Administração usará o banco de dados criado para armazenar os dados do Servidor de Administração. Todos os direitos do sistema necessários são atribuídos à conta de serviço do Servidor de Administração. O Servidor de Administração está pronto para uso.

Configuração de contas para trabalhar com MySQL e MariaDB

Pré-requisitos

Antes de atribuir direitos às contas, execute as seguintes ações:

1. Certifique-se de fazer login no sistema com a conta de administrador local.

2. Instale um ambiente para trabalhar com MySQL ou MariaDB.

3. Certifique-se de ter uma conta do Windows na qual instalará o Servidor de Administração.

4. Certifique-se de ter uma conta do Windows na qual iniciará o serviço do Servidor de Administração.

Configuração de contas para instalar o Servidor de Administração

Para configurar as contas para a instalação do Servidor de Administração:

1. Execute um ambiente para uso com MySQL ou MariaDB na conta raiz criada ao instalar o DBMS.

2. Crie uma conta DBMS interna com uma senha. O instalador do Servidor de Administração (adiante também denominado instalador) e o serviço do Servidor de Administração usarão esta conta DBMS interna para acessar o DBMS. Conceda os seguintes privilégios a essa conta:

   - Privilégios do esquema:
     - Banco de dados do Servidor de Administração: ALL (excluindo `GRANT OPTION`)
     - Esquemas do sistema (mysql e sys): `SELECT`, `SHOW VIEW`
     - O procedimento armazenado sys.table_exists: `EXECUTE`
   - Privilégios globais para todos os esquemas: `PROCESS`, `SUPER`

   Para criar uma conta DBMS interna e conceder os privilégios necessários a esta conta, execute o script abaixo (neste script, o login do DBMS será *KSCAdmin* e o nome do banco de dados do Servidor de Administração será *kav*):

   ```
   /* Crie um usuário chamado KSCAdmin */
   CREATE USER 'KSCAdmin'
   /* Especifique uma senha para o KSCAdmin */
   IDENTIFIED BY '<senha>';
   ```

   Caso use o MySQL 8.0 ou anterior como um DBMS, observe que, para essas versões, a autenticação "Caching SHA2 password" não é compatível. Altere a autenticação padrão de "Cache de senha SHA2" para "Senha nativa do MySQL":

   - Para criar uma conta DBMS que use a autenticação "Senha nativa do MySQL", execute o seguinte comando:

     ```
     CREATE USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<senha>';
     ```

   - Para alterar a autenticação de uma conta DBMS existente, execute o seguinte comando:

     ```
     ALTER USER 'KSCAdmin'@'%' IDENTIFIED WITH mysql_native_password BY '<senha>';
     ```

   ```
   /* Conceda privilégios ao 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';
   ```

   Caso use o MariaDB 10.5 ou anterior como um DBMS, não será preciso conceder o privilégio EXECUTE. Nesse caso, exclua o seguinte comando do script: `GRANT EXECUTE ON PROCEDURE sys.table_exists TO 'KSCAdmin'`.

3. Para visualizar a lista de privilégios concedidos à conta do DBMS, execute o seguinte script:

   ```
   SHOW grants for 'KSCAdmin';
   ```

4. Para criar um banco de dados do Servidor de Administração, execute o seguinte script (neste script, o nome do banco de dados do Servidor de Administração será *kav*):

   ```
   CREATE DATABASE kav
   DEFAULT CHARACTER SET ascii
   DEFAULT COLLATE ascii_general_ci;
   ```

   Use o mesmo nome do banco de dados especificado no script que cria a conta DBMS.

5. Faça login no sistema com a conta do Windows usada para executar o instalador.

6. Execute o instalador.

   O Assistente de instalação do Servidor de Administração é iniciado. Siga as instruções do Assistente.

7. Selecione a opção instalação personalizada do Servidor de Administração.

8. Selecione o MySQL ou MariaDB como DBMS que armazena o banco de dados do Servidor de Administração.

9. Especifique o Nome do banco de dados do Servidor de Administração. Use o mesmo nome do banco de dados especificado no script.

10. Especifique as credenciais da conta DBMS que você criou pelo script.

11. Especifique a conta de Windows usada para iniciar o serviço do Servidor de Administração.

    Você pode selecionar uma conta de usuário do Windows existente ou criar automaticamente uma nova conta do Windows no formato KL-AK-* usando o instalador. Independentemente da escolha da conta, o instalador atribui os direitos de sistema necessários à conta de serviço do Servidor de Administração.

Após a conclusão da instalação, o banco de dados do Servidor de Administração é criado e o Servidor de Administração está pronto para uso.

Mover dados de um espaço de tabela compartilhado para um espaço de tabela individual nos DBMSs MySQL e MariaDB

Em um DBMS MySQL e MariaDB, é possível armazenar dados das seguintes formas:

- Como um espaço de tabela compartilhado, quando os dados de todos os bancos de dados do usuário forem armazenados em um único arquivo (geralmente no arquivo `ibdata1`).

- Como um espaço de tabela individual, quando um espaço para dados separado é criado como um arquivo separado.

Usar um espaço de tabela compartilhado aumenta o risco de fragmentação. Como não é possível executar uma operação `SHRINK`, um arquivo em um espaço de tabela compartilhado pode ocupar cerca de 90% do espaço em disco. Isso prejudica o desempenho do subsistema de disco. Portanto, é útil optar por um espaço de tabela individual.

Este artigo descreve como mover dados de um espaço de tabela compartilhado para um espaço de tabela individual. Se os DBMSs MySQL ou MariaDB também forem utilizados por outros aplicativos, será necessário mover os bancos de dados desses aplicativos para o espaço de tabela individual.

Recomendamos que o procedimento seja executado somente se você estiver utilizando DBMSs MySQL ou MariaDB para o Servidor de Administração.
Mover dados de um espaço de tabela compartilhado para um espaço de tabela individual pode aumentar a carga no subsistema de disco.

Pré-requisitos

Antes de começar, certifique-se de que:

- Uma cópia de backup dos dados do Servidor de Administração foi criada por meio da execução de uma tarefa de backup de dados ou do utilitário klbackup.
- Uma cópia de backup de outros aplicativos foi criada, cujos bancos de dados são gerenciados por um DBMS MySQL ou MariaDB (se houver).
- No dispositivo com o DBMS instalado, há um espaço livre em disco na partição com o banco de dados.

O espaço em disco necessário corresponde a 150% do tamanho total atual dos bancos de dados (tamanho atual do arquivo `ibdata1`).

Processar

Para mover dados de um espaço de tabela compartilhado para um espaço de tabela individual:

1. Pare o serviço do Servidor de Administração do Kaspersky Security Center e outros aplicativos por meio da instância do DBMS para a qual você deseja executar este procedimento.

2. Dependendo da versão do DBMS, faça login no seu DBMS como superusuário e então, em qualquer aplicativo conveniente, execute o script `fix_tablespace.sql`.

   É possível visualizar os scripts `fix_tablespace.sql` clicando nestes links:

   [Visualizar o script para 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;
```

Visualizar o script para 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;
```

A execução do script não deve ser interrompida.
Se nenhum erro de DBMS ocorreu, mas você interrompeu a execução do script, execute o script novamente ou pare de executar as etapas deste procedimento, reinicie o serviço DBMS e restaure os dados do Servidor de Administração a partir do backup.

3. Na seção `[mysqld]` do arquivo my.cnf, defina o parâmetro `innodb_file_per_table` como `1`.

4. Reinicie o serviço MySQL ou MariaDB.

5. Reinicie o serviço do Servidor de Administração do Kaspersky Security Center.

Os dados serão movidos de um espaço de tabela compartilhado para um espaço de tabela individual.

Configurar contas para trabalhar com PostgreSQL e Postgres Pro

Pré-requisitos

Antes de atribuir direitos às contas, execute as seguintes ações:

1. Certifique-se de fazer login no sistema com a conta de administrador local.
2. Instale um ambiente para uso com PostgreSQL e Postgres Pro.
3. Configurar o servidor PostgreSQL ou Postgres Pro para uso com o Kaspersky Security Center 14.2.
4. Certifique-se de ter uma conta do Windows na qual instalará o Servidor de Administração.
5. Certifique-se de ter uma conta do Windows na qual iniciará o serviço do Servidor de Administração.

Configuração de contas para instalar o Servidor de Administração (criação automática do banco de dados do Servidor de Administração)

Para configurar as contas para a instalação do Servidor de Administração:

1. Execute um ambiente para trabalhar com PostgreSQL e Postgres Pro.
2. Escolha uma função do Postgres para acessar o DBMS. É possível usar uma das seguintes funções:
   - O usuário do *Postgres* (a função padrão do Postgres).

     Caso use o usuário do *Postgres*, não é necessário conceder direitos adicionais para ele.
   - Uma nova função do Postgres.

     Se quiser usar uma nova função do Postgres, crie essa função e conceda a ela o privilégio CREATEDB. Para fazer isso, execute o seguinte script (neste script, a função é *KSCAdmin*):

     ```
     CREATE USER "KSCAdmin" WITH PASSWORD '<senha>' CREATEDB;
     ```

     A função criada será usada como proprietária do banco de dados do Servidor de Administração (adiante também denominado banco de dados do Servidor).
3. Faça login no sistema com a conta do Windows usada para executar o instalador do Servidor de Administração (adiante também denominado instalador).
4. Execute o instalador.

   O Assistente de instalação do Servidor de Administração é iniciado. Siga as instruções do Assistente.
5. Selecione a opção instalação personalizada do Servidor de Administração.
6. Selecione os PostgreSQL ou Postgres Pro como DBMS que armazena o banco de dados do Servidor de Administração.
7. Especifique o Nome do banco de dados do Servidor. O instalador criará automaticamente o banco de dados do Servidor.

8. Especifique as credenciais da função de Postgres.

9. Especifique a conta de Windows usada para iniciar o serviço do Servidor de Administração.

   Você pode selecionar uma conta de usuário do Windows existente ou criar automaticamente uma nova conta do Windows no formato KL-AK-* usando o instalador. Independentemente da escolha da conta, o instalador atribui os direitos de sistema necessários à conta de serviço do Servidor de Administração.

Após a conclusão da instalação, o banco de dados do Servidor é criado automaticamente e o Servidor de Administração está pronto para uso.

Configuração de contas para instalar o Servidor de Administração (criação manual do banco de dados do Servidor de Administração)

Para configurar as contas para a instalação do Servidor de Administração:

1. Execute um ambiente para uso com Postgres.

2. Faça login com o usuário do *Postgres* no banco de dados *Postgres*.

3. Crie uma nova função Postgres (neste exemplo, a função é *KSCAdmin*):

   ```
   CREATE USER "KSCAdmin" WITH PASSWORD '< senha >';
   ```

4. Crie um banco de dados do Servidor de Administração (neste exemplo, o nome do banco de dados do Servidor de Administração é *KAV*):

   ```
   CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";
   ```

   > Caso ocorra o erro "A nova codificação (UTF8) é incompatível com a codificação do banco de dados de modelo", crie um banco de dados usando o comando:
   > `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin" TEMPLATE template0;`
   > em vez de:
   > `CREATE DATABASE "KAV" ENCODING 'UTF8' OWNER "KSCAdmin";`

5. Conceda todos os privilégios à função no banco de dados do Servidor de Administração:

   ```
   GRANT ALL PRIVILEGES ON DATABASE "KAV" TO "KSCAdmin";
   ```

   > Certifique-se de que a função tenha os privilégios padrão CONNECT e TEMPORARY no banco de dados do Servidor de Administração.

6. Conceda os seguintes privilégios à função Postgres criada:

   - Privilégios em todas as tabelas no esquema público: ALL
   - Privilégios em todas as sequências no esquema público: ALL

   Para isso, faça login com o usuário do *Postgres* no banco de dados do Servidor e execute o seguinte script (neste script, a função será *KSCAdmin*):

   ```
   GRANT ALL PRIVILEGES ON ALL TABLES IN SCHEMA "public" TO "KSCAdmin";
   GRANT ALL PRIVILEGES ON ALL SEQUENCES IN SCHEMA "public" TO "KSCAdmin";
   ```

7. Faça login no sistema com a conta do Windows usada para executar o instalador.

8. Execute o instalador do Servidor de Administração.

   O Assistente de instalação do Servidor de Administração é iniciado. Siga as instruções do Assistente.

9. Selecione a opção instalação personalizada do Servidor de Administração.

10. Selecione os PostgreSQL ou Postgres Pro como DBMS que armazena o banco de dados do Servidor de Administração.

11. Especifique o Nome do banco de dados do Servidor. Use o mesmo nome do banco de dados especificado no script. Observe que o nome do banco de dados diferencia maiúsculas de minúsculas.

12. Especifique as credenciais da função de Postgres.

13. Especifique a conta de Windows usada para iniciar o serviço do Servidor de Administração.

    Você pode selecionar uma conta de usuário do Windows existente ou criar automaticamente uma nova conta do Windows no formato KL-AK-* usando o instalador. Independentemente da escolha da conta, o instalador atribui os direitos de sistema necessários à conta de serviço do Servidor de Administração.

Após a conclusão da instalação, o Servidor de Administração usará o banco de dados criado para armazenar os dados do Servidor de Administração. O Servidor de Administração está pronto para uso.

Cenário: Autenticação do Microsoft SQL Server

As informações nesta seção são aplicáveis apenas às configurações nas quais o Kaspersky Security Center usa o Microsoft SQL Server como um sistema de gerenciamento de banco de dados.

Para proteger os dados do Kaspersky Security Center transferidos para ou do banco de dados e os dados armazenados no banco de dados contra o acesso não autorizado, é necessário proteger a comunicação entre o Kaspersky Security Center e o SQL Server. A maneira mais confiável de fornecer comunicação segura é instalando o Kaspersky Security Center e o SQL Server no mesmo dispositivo e usando o mecanismo de memória compartilhada para os dois aplicativos. Em todos os outros casos, recomendamos usar um certificado SSL ou TLS para autenticar a instância do SQL Server. É possível usar um certificado de uma autoridade de certificação (AC) confiável ou um certificado autoassinado. Recomendamos usar um certificado de uma AC confiável, porque um certificado autoassinado fornece apenas proteção limitada.

A autenticação do SQL Server continua em estágios:

1. **Geração de um certificado SSL ou TLS autoassinado para SQL Server de acordo com os requisitos de certificado**

   Se você já possui um certificado para o SQL Server, pule esta etapa.

   Um certificado SSL é aplicável apenas às versões do SQL Server anteriores a 2016 (13.x). No SQL Server 2016 (13.x) e versões posteriores, use um certificado TLS.

   Por exemplo, para gerar um certificado TLS, insira o seguinte comando no PowerShell:

   ```
   New-SelfSignedCertificate -DnsName SQL_HOST_NAME -CertStoreLocation cert:\LocalMachine
   -KeySpec KeyExchange
   ```

No comando, em vez que SQL_HOST_NAME, é necessário inserir o nome do host do SQL Server se o host estiver incluso no domínio, ou inserir o *nome de domínio totalmente qualificado* (FQDN) do host se o host não estiver incluído no domínio. O mesmo nome – nome do host ou FQDN – deve ser especificado como um nome de instância do SQL Server no Assistente de Instalação do Servidor de Administração.

2. **Adicionar o certificado na instância do SQL Server**

   As instruções para este estágio dependem da plataforma em que o SQL Server está sendo executado. Consulte a documentação oficial para obter detalhes:

   - Windows
   - Linux
   - Serviço de banco de dados relacional da Amazon
   - Windows Azure

   Para usar o certificado em um cluster de failover, é necessário instalar o certificado em cada nó do cluster de failover. Para detalhes, consulte a documentação da Microsoft.

3. **Atribuição das permissões de conta de serviço**

   Verifique se a conta de serviço na qual o serviço do SQL Server é executado tem a permissão de Controle total para acessar chaves privadas. Para detalhes, consulte a documentação da Microsoft.

4. **Adição do certificado à lista de certificados confiáveis do Kaspersky Security Center**

   No dispositivo do Servidor de Administração, adicione o certificado à lista de certificados confiáveis. Para detalhes, consulte a documentação da Microsoft.

5. **Ativação de conexões criptografadas entre a instância do SQL Server e o Kaspersky Security Center**

   No dispositivo Servidor de Administração, configure o valor `1` para a variável de ambiente `KLDBADO_UseEncryption`. Por exemplo, no Windows Server 2012 R2, é possível alterar as variáveis de ambiente clicando em **Variáveis de ambiente** na guia **Avançado** da janela de **Propriedades do Sistema**. Adicione uma nova variável, nomeie-a `KLDBADO_UseEncryption` e defina o valor `1`.

6. **Configuração adicional para usar o protocolo TLS 1.2**

   Se você usa o protocolo TLS 1.2, faça também o seguinte:

   - Verifique se a versão instalada do SQL Server é um aplicativo de 64 bits.
   - Instale o driver Microsoft OLE DB no dispositivo do Servidor de Administração. Para detalhes, consulte a documentação da Microsoft.
   - No dispositivo do Servidor de Administração, configure o valor `1` para a variável de ambiente `KLDBADO_UseMSOLEDBSQL`. Por exemplo, no Windows Server 2012 R2, é possível alterar as variáveis de ambiente clicando em **Variáveis de ambiente** na guia **Avançado** da janela de **Propriedades do Sistema**. Adicione uma nova variável, nomeie-a de `KLDBADO_UseMSOLEDBSQL` e defina o valor para `1`.

     Caso a versão do driver OLE DB seja 19 ou mais recente, defina também o valor `MSOLEDBSQL19` para a variável de ambiente `KLDBADO_ProviderName`.

7. **Ativação do uso do protocolo TCP/IP em uma instância nomeada do SQL Server**

Ao usar uma instância nomeada do SQL Server, ative adicionalmente o uso do protocolo TCP/IP e atribua um número de porta TCP/IP ao Mecanismo de Banco de Dados do SQL Server. Ao configurar a conexão do SQL Server no Assistente de instalação do Servidor de Administração, especifique o nome do host do SQL Server e o número da porta no campo **Nome da instância do SQL Server**.

Recomendações sobre a instalação do Servidor de Administração

Esta seção contém recomendações sobre como instalar o Servidor de Administração. Esta seção também fornece cenários para usar uma pasta compartilhada no dispositivo do Servidor de Administração para implementar o Agente de Rede em dispositivos cliente.

Criar contas para os serviços do Servidor de Administração em um cluster para falhas

Por padrão, o instalador automaticamente cria contas não-privilegiadas para os serviços do Servidor de Administração. Este comportamento é o mais conveniente para a instalação do Servidor de Administração em um dispositivo comum.

No entanto, a instalação do Servidor de Administração em um cluster de correção de falha necessita de um cenário diferente:

1. Crie contas de domínio não privilegiado para os serviços do Servidor de Administração e torne-as membros de um grupo de segurança de domínio global denominado KLAdmins.

2. No instalador do Servidor de Administração, especifique as contas de domínio que foram criadas para os serviços.

Definir uma pasta compartilhada

Ao instalar o Servidor de Administração, você pode especificar a localização da pasta compartilhada. Também é possível especificar a localização da pasta compartilhada após a instalação, nas propriedades do Servidor de Administração. Por padrão, a pasta compartilhada será criada no dispositivo com o Servidor de Administração (com os direitos de leitura para o subgrupo **Todos**). No entanto, em alguns casos (como alta carga ou a necessidade para o acesso a partir de uma rede isolada), é útil localizar a pasta compartilhada em um recurso de arquivo dedicado.

A pasta compartilhada é usada ocasionalmente na implementação de Agente de Rede.

A diferenciação entre maiúsculas e minúsculas para a pasta compartilhada deve estar desativada.

Instalação remota com as ferramentas do Servidor de Administração através das políticas de grupo do Active Directory

Se os dispositivos alvo estiverem localizados em um domínio do Windows (nenhum grupo de trabalho), a implementação inicial (a instalação do Agente de Rede e do aplicativo de segurança em dispositivos que ainda não são gerenciados) tem de ser realizada através das políticas de grupo do Active Directory. A implementação é executada usando a tarefa padrão para a instalação remota do Kaspersky Security Center. Se a rede for de larga escala, é útil localizar a pasta compartilhada em um recurso de arquivo dedicado para reduzir a carga no subsistema de disco do dispositivo do Servidor de Administração.

Instalação remota através da entrega do caminho UNC a um pacote independente

Se os usuários de dispositivos em rede na organização tiverem direitos de administrador local, outro método de implementação inicial é o de criar um pacote de Agente de Rede independente (ou até um pacote de Agente de Rede "vinculado" junto com o aplicativo de segurança). Após você criar um pacote independente, envie a um link aos usuários àquele pacote, que é armazenado na pasta compartilhada. A instalação inicia quando os usuários clicam no link.

Atualizar da partir da pasta compartilhada do Servidor de Administração

Na tarefa de atualização de antivírus, você pode configurar a atualização a partir da pasta compartilhada do Servidor de Administração. Se a tarefa tiver sido atribuída à a um grande número de dispositivos, é útil localizar a pasta compartilhada em um recurso de arquivo dedicado.

Imagens de instalação de sistemas operacionais

As imagens do sistema operacional sempre são instaladas pela pasta compartilhada: os dispositivos leem as imagens do sistema operacional na pasta compartilhada. Se a implementação das imagens for planejada em um grande número de dispositivos corporativos, é útil localizar a pasta compartilhada em um recurso de arquivo dedicado.

Especificar o endereço do Servidor de Administração

Ao instalar o Servidor de Administração, você pode especificar o endereço do Servidor de Administração. Este endereço será usado como o endereço padrão ao criar pacotes de instalação do Agente de Rede.

Como o endereço do Servidor de Administração, é possível especificar o seguinte:

- Nome NetBIOS do Servidor de Administração, especificado por padrão
- Nome de domínio totalmente qualificado (FQDN) do Servidor de Administração caso o Domain Name System (DNS) na rede da organização tenha sido configurado e esteja funcionando corretamente
- Endereço externo caso o Servidor de Administração esteja instalado na zona desmilitarizada (DMZ)

Após isso, você será capaz de modificar o endereço do Servidor de Administração usando as ferramentas do Console de Administração; o endereço não se modificará automaticamente em pacotes de instalação do Agente de Rede que já tiverem sido criados.

Instalação padrão

A instalação padrão é uma instalação do Servidor de Administração que usa os caminhos padrão para arquivos de aplicativo, instala o conjunto padrão de plugins e não ativa o Gerenciamento de Dispositivos Móveis.

Para instalar o Servidor de Administração do Kaspersky Security Center em um dispositivo local:

Execute o arquivo ksc_<número da versão>.<número de build>_full_<idioma de localização>.exe.

Uma janela é exibida, solicitando que você selecione os aplicativos Kaspersky para instalar. Na janela de seleção do aplicativo, clique no link **Instalar o Servidor de Administração do Kaspersky Security Center** para executar o assistente de instalação do Servidor de Administração. Siga as instruções do Assistente.

Etapa 1. Leitura do Contrato de Licença e da Política de Privacidade

Nessa etapa do Assistente de instalação, você deve ler o Contrato de Licença, o qual é celebrado entre você e a Kaspersky, assim como a Política de Privacidade.

Também é possível que seja solicitado que leia os Contrato de Licença e as Políticas de Privacidade dos plugins de gerenciamento disponíveis no kit de distribuição do Kaspersky Security Center.

Leia cuidadosamente o Contrato de Licença e a Política de privacidade. Caso concorde com todos os termos do Contrato de licença e da Política de Privacidade, confirme tudo isso marcando as caixas de seleção apropriadas.

A Instalação do aplicativo no seu dispositivo continuará após você selecionar ambas as caixas de seleção.

Se você não concordar com o Contrato de Licença ou a Política de Privacidade, cancele a instalação clicando no botão **Cancelar**.

Etapa 2. Seleção do método de instalação

Na janela de seleção de tipo de instalação, selecione **Padrão**.

Instalação padrão é recomendada se você quiser testar o Kaspersky Security Center ao, por exemplo, testar a sua operação em uma pequena área dentro da rede da sua empresa. Durante a instalação padrão, você somente configura o banco de dados. Você não especifica nenhuma configuração do Servidor de Administração: os seus respectivos valores padrões são usados. A instalação padrão não lhe permite selecionar plugins de gerenciamento para instalar; somente o conjunto padrão de plugins é instalado. Durante a instalação padrão, nenhum pacote de instalação para dispositivos móveis é criado. No entanto, você pode criá-las depois no Console de Administração.

Etapa 3. Instalar o Kaspersky Security Center Web Console

Esta etapa será exibida apenas se você estiver usando um sistema operacional de 64 bits. Caso contrário, essa etapa não é exibida, porque o Kaspersky Security Center Web Console não trabalha com sistemas operacionais de 32 bits.

Por padrão, o Kaspersky Security Center Web Console e o Console de Administração baseado no MMC serão instalados.

Se deseja instalar apenas o Kaspersky Security Center Web Console:

1. Selecione **Instalar apenas este**.
2. Escolha **console baseado na web** na lista suspensa.

A instalação do Kaspersky Security Center Web Console começa automaticamente após a conclusão da instalação do Servidor de Administração.

Se você desejar instalar apenas o Console de Administração baseado em MMC:

1. Selecione **Instalar apenas este**.
2. Escolha o **console baseado em MMC** na lista suspensa.

Etapa 4. Selecionando o tamanho da rede

Especifique o tamanho da rede na qual o Kaspersky Security Center deve ser instalado. Dependendo do número de dispositivos na rede, o assistente configura a instalação e a aparência da interface do aplicativo de maneira que eles coincidam.

A tabela seguinte lista as configurações de instalação do aplicativo e configurações de aspeto da interface que são ajustadas com base em vários tamanhos de rede.

Configurações de instalação dependendo do tamanho da rede

Configurações	1 a 100 dispositivos gerenciados	101 a 1.000 dispositivos gerenciados	1.001 a 5.000 dispositivos gerenciados	Mais de 5.000 dispositivos gerenciados
Exibição com o nó para Servidores de Administração secundários e virtuais e todas as configurações relacionadas com os Servidores de Administração secundários e virtuais na árvore do console (disponível apenas em um Console de Administração baseado em MMC)	Indisponível	Indisponível	Disponível	Disponível
Exibição com a sessão **Segurança** na janela de propriedades do Servidor de Administração e grupos de administração (disponível apenas em Consoles de Administração baseados em MMC)	Indisponível	Indisponível	Disponível	Disponível
Distribuição aleatória do tempo de inicialização para a tarefa de atualização em dispositivos cliente	Indisponível	Em um intervalo de 5 minutos	Em um intervalo de 10 minutos	Em um intervalo de 10 minutos

Se você conectar o Servidor de Administração com um servidor de banco de dados MySQL (versão 5.7) ou SQL Express, recomendamos evitar usar o aplicativo para gerenciar mais do que 10.000 dispositivos. Para o sistema de gerenciamento de banco de dados MariaDB, o número máximo recomendado de dispositivos gerenciados é 20.000.

Etapa 5. Seleção do banco de dados

Nesta etapa do assistente, selecione um dos sistemas de gerenciamento de banco de dados (DBMS) a seguir que serão usados para armazenar o banco de dados do Servidor de Administração:

- **Microsoft SQL Server ou SQL Server Express**
- **MySQL ou MariaDB**
- **PostgreSQL ou Postgres Pro**

Recomenda-se instalar o Servidor de Administração em um servidor dedicado em vez de um controlador de domínio. Porém, ao instalar o Kaspersky Security Center em um servidor que atua como controlador de domínio somente leitura (RODC), o Microsoft SQL Server (SQL Express) não deve estar instalado localmente (no mesmo dispositivo). Nesse caso, recomendamos que você instale o Microsoft SQL Server (SQL Express) remotamente (em um outro dispositivo) ou use MySQL, MariaDB ou PostgreSQL se precisar instalar o DBMS localmente.

A estrutura do banco de dados do Servidor de Administração é fornecida no arquivo klakdb.chm, localizado na pasta de instalação do Kaspersky Security Center. Esse arquivo também está disponível em um arquivo no portal Kaspersky: klakdb.zip.

Etapa 6. Configuração do servidor SQL

Nesta etapa do assistente, especifique as seguintes configurações de conexão, dependendo do sistema de gerenciamento de banco de dados (DBMS) selecionado:

- Se você selecionou **Microsoft SQL Server ou SQL Server Express** na etapa anterior:

  - No campo **Nome da instância do SQL Server**, especifique o nome do SQL Server na rede. Para visualizar uma lista de todos os servidores SQL que estão na rede, clique no botão **Procurar**. Este valor está vazio por padrão.

    Se você se conectar ao SQL Server por uma porta personalizada, juntamente com o nome do host do SQL Server, especifique o número da porta separado por vírgula, por exemplo:

    ```
    SQL_Server_host_name,1433
    ```

    Ao proteger a comunicação entre o Servidor de Administração e o SQL Server por meio de um certificado, especifique no campo **Nome da instância do SQL Server** o mesmo nome do host usado na geração do certificado. Ao usar uma instância nomeada do SQL Server, juntamente com o nome do host do SQL Server, especifique o número da porta separado por vírgula, por exemplo:

    ```
    SQL_Server_name,1433
    ```

    Ao usar várias instâncias do SQL Server no mesmo host, especifique adicionalmente o nome da instância separado por uma barra invertida, por exemplo:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Caso um SQL Server na rede corporativa tenha o recurso Always On ativado, especifique o nome do ouvinte do grupo de disponibilidade no campo **Nome da instância do SQL Server**. Observe que o Servidor de Administração é compatível apenas com o modo de disponibilidade de confirmação síncrona quando o recurso Always On estiver ativado.

  - No campo **Nome do banco de dados**, especifique o nome do DBMS que foi criado para armazenar dados do Servidor de Administração. O valor padrão é *KAV*.

  Se você desejar instalar o SQL Server em um dispositivo do qual você estiver instalando o Kaspersky Security Center, deverá parar a instalação e reiniciá-la após a instalação do SQL Server. As versões do SQL Server suportadas estão listadas nos requisitos do sistema.

  Se você deseja instalar o SQL Server em um dispositivo remoto, não há necessidade de interromper o Assistente de Instalação do Kaspersky Security Center. Instale o servidor SQL e retome a instalação do Kaspersky Security Center.

- Se você selecionou **MySQL ou MariaDB** na etapa anterior:

  - No campo **Nome da instância do SQL Server**, especifique o nome da instância do DBMS. Por padrão, o nome é o endereço IP do dispositivo no qual o Kaspersky Security Center deve ser instalado.

  - No campo **Porta**, especifique a porta de conexão do Servidor de Administração ao DBMS. O número da porta padrão é 3306.

  - No campo **Nome do banco de dados**, especifique o nome do DBMS que foi criado para armazenar dados do Servidor de Administração. O valor padrão é *KAV*.

- Se você selecionou **PostgreSQL ou Postgres Pro** na etapa anterior:

  - No campo **Servidor PostgreSQL ou Postgres Pro**, especifique o nome da instância do DBMS. Por padrão, o nome é o endereço IP do dispositivo no qual o Kaspersky Security Center deve ser instalado.

- No campo **Porta**, especifique a porta de conexão do Servidor de Administração ao DBMS. O número da porta padrão é 5432.

- No campo **Nome do banco de dados**, especifique o nome do DBMS que foi criado para armazenar dados do Servidor de Administração. O valor padrão é *KAV*.

Etapa 7. Seleção do modo de autenticação

Determine o modo de autenticação que será usado durante a conexão do Servidor de Administração ao sistema de gerenciamento do banco de dados (DBMS).

Dependendo do DBMS selecionado, será possível selecionar um dos seguintes modos de autenticação:

- Para SQL Express ou Microsoft SQL Server, selecione uma das seguintes opções:

  - **Modo de Autenticação do Microsoft Windows**. A verificação de direitos usa a conta usada para iniciar o Servidor de Administração.

  - **Modo de Autenticação do SQL Server**. Se selecionar essa opção, a conta especificada na janela será usada para verificar os direitos de acesso. Preencha os campos **Conta** e **Senha**.

    Para ver a senha inserida, mantenha pressionado o botão **Exibir**.

  Para ambos os modos de autenticação, o aplicativo verifica se o banco de dados está disponível. Você precisa fornecer as credenciais corretas, pois receberá uma mensagem de erro caso o banco de dados não esteja disponível.

  Se o banco de dados de Servidor de Administração estiver armazenado em outro dispositivo e a conta do Servidor de Administração não tiver acesso ao servidor do banco de dados, você deve usar o modo de autenticação do SQL Server instalando ou atualizando o Servidor de Administração. Isso pode ocorrer quando o dispositivo que armazena os bancos de dados estiver fora do domínio ou quando o Servidor de Administração estiver instalado sob uma conta do LocalSystem.

- Para MySQL, MariaDB, PostgreSQL ou Postgres Pro, especifique a conta e a senha.

Etapa 8. Descompactação e instalação dos arquivos no disco rígido

Após a instalação dos componentes do Kaspersky Security Center, você pode iniciar a instalação dos arquivos no disco rígido.

Se a instalação requerer programas adicionais, o Assistente de instalação vai notificá-lo, na página **Pré-requisitos de instalação**, antes de iniciar a instalação do Kaspersky Security Center. Os programas requeridos serão instalados automaticamente após você clicar no botão **Avançar**.

Na última página, você pode selecionar qual console iniciar para uso com o Kaspersky Security Center:

- **Iniciar Console de Administração baseado em MMC**

- **Iniciar o Kaspersky Security Center Web Console**

  Esta opção estará disponível somente se você tiver optado por instalar o Kaspersky Security Center Web Console em uma das etapas anteriores.

Você também pode clicar em **Concluir** para fechar o assistente sem iniciar o trabalho com o Kaspersky Security Center. Você pode iniciar o trabalho depois, a qualquer momento.

No momento da primeira inicialização do Console de Administração ou Kaspersky Security Center Web Console, você poderá executar a configuração inicial do aplicativo.

Quando o Assistente de instalação concluir sua operação, os seguintes componentes do aplicativo são instalados no disco rígido no qual o sistema operacional foi instalado:

- Servidor de Administração (junto com a versão do Agente de Rede)
- Console de Administração baseado em Console de Gerenciamento Microsoft
- Kaspersky Security Center Web Console (se você optou por instalá-lo)
- Plugins de gerenciamento de aplicativo disponíveis no kit de distribuição

Adicionalmente, o Microsoft Windows Installer 4.5 será instalado se ele já não tiver sido instalado anteriormente.

Instalação personalizada

A instalação personalizada é uma instalação do Servidor de Administração durante a qual você é solicitado a selecionar os componentes para instalar e especificar a pasta na qual o aplicativo deve ser instalado.

Usando este tipo da instalação, você pode configurar o banco de dados e o Servidor de Administração, assim como instalar componentes que não estão incluídos na instalação padrão ou plugins de gerenciamento para diversos aplicativos de segurança da Kaspersky. Você também pode ativar o Gerenciamento de Dispositivos Móveis.

Para instalar o Servidor de Administração do Kaspersky Security Center em um dispositivo local:

Execute o arquivo ksc_<número da versão>.<número de build>_full_<idioma de localização>.exe.

Uma janela é exibida, solicitando que você selecione os aplicativos Kaspersky para instalar. Na janela de seleção do aplicativo, clique no link **Instalar o Servidor de Administração do Kaspersky Security Center** para executar o assistente de instalação do Servidor de Administração. Siga as instruções do Assistente.

Etapa 1. Leitura do Contrato de Licença e da Política de Privacidade

Nessa etapa do Assistente de instalação, você deve ler o Contrato de Licença, o qual é celebrado entre você e a Kaspersky, assim como a Política de Privacidade.

Também é possível que seja solicitado que leia os Contrato de Licença e as Políticas de Privacidade dos plugins de gerenciamento disponíveis no kit de distribuição do Kaspersky Security Center.

Leia cuidadosamente o Contrato de Licença e a Política de privacidade. Caso concorde com todos os termos do Contrato de licença e da Política de Privacidade, confirme tudo isso marcando as caixas de seleção apropriadas.

A Instalação do aplicativo no seu dispositivo continuará após você selecionar ambas as caixas de seleção.

Se você não concordar com o Contrato de Licença ou a Política de Privacidade, cancele a instalação clicando no botão **Cancelar**.

Etapa 2. Seleção do método de instalação

Na janela de seleção de tipo de instalação, especifique **Personalizada**.

Instalação personalizada permite modificar as configurações do Kaspersky Security Center, como o caminho à pasta compartilhada, contas, e portas para a conexão ao Servidor de Administração e as configurações do banco de dados. A instalação personalizada permite especificar quais plugins de gerenciamento da Kaspersky devem ser instalados. Durante a instalação personalizada, você pode criar pacotes de instalação para dispositivos móveis ativando a opção correspondente.

Etapa 3. Seleção dos componentes a serem instalados

Selecione os componentes do Servidor de Administração do Kaspersky Security Center que você deseja instalar:

- **Gerenciamento de Dispositivos Móveis**. Selecione esta caixa de seleção, se você deve criar pacotes de instalação para dispositivos móveis quando o Assistente de instalação do Kaspersky Security Center estiver em execução. Você também pode criar pacotes de instalação para dispositivos móveis manualmente, após a instalação do Servidor de Administração, usando as ferramentas do Console de Administração.

- **Agente SNMP**. O componente recebe as informações estatísticas para o Servidor de Administração através do protocolo SNMP. O componente está disponível se o aplicativo estiver instalado em um dispositivo com o SNMP instalado.

  Após a instalação do Kaspersky Security Center, os arquivos .mib necessários para recuperar as estatísticas estarão localizados na subpasta SNMP da pasta de instalação do aplicativo.

O Agente de Rede e o Console de Administração não são exibidos na lista de componentes. Esses componentes são instalados automaticamente e você não pode cancelar sua instalação.

Nessa etapa, você deve especificar uma pasta para instalação dos componentes do Servidor de Administração. Por padrão, os componentes são instalados em <Disco>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Se essa pasta não existir, a pasta é criada automaticamente durante a instalação. Você pode alterar a pasta de destino usando o botão **Procurar**.

Etapa 4. Instalar o Kaspersky Security Center Web Console

Esta etapa será exibida apenas se você estiver usando um sistema operacional de 64 bits. Caso contrário, essa etapa não é exibida, porque o Kaspersky Security Center Web Console não trabalha com sistemas operacionais de 32 bits.

Por padrão, o Kaspersky Security Center Web Console e o Console de Administração baseado no MMC serão instalados.

Se deseja instalar apenas o Kaspersky Security Center Web Console:

1. Selecione **Instalar apenas este**.
2. Escolha **console baseado na web** na lista suspensa.

A instalação do Kaspersky Security Center Web Console começa automaticamente após a conclusão da instalação do Servidor de Administração.

Se você desejar instalar apenas o Console de Administração baseado em MMC:

1. Selecione **Instalar apenas este**.
2. Escolha o **console baseado em MMC** na lista suspensa.

Etapa 5. Selecionando o tamanho da rede

Especifique o tamanho da rede na qual o Kaspersky Security Center deve ser instalado. Dependendo do número de dispositivos na rede, o assistente configura a instalação e a aparência da interface do aplicativo de maneira que eles coincidam.

A tabela seguinte lista as configurações de instalação do aplicativo e configurações de aspeto da interface que são ajustadas com base em vários tamanhos de rede.

Configurações de instalação dependendo do tamanho da rede

Configurações	1 a 100 dispositivos gerenciados	101 a 1.000 dispositivos gerenciados	1.001 a 5.000 dispositivos gerenciados	Mais de 5.000 dispositivos gerenciados
Exibição com o nó para Servidores de Administração secundários e virtuais e todas as configurações relacionadas com os Servidores de Administração secundários e virtuais na árvore do console (disponível apenas em um Console de Administração baseado em MMC)	Indisponível	Indisponível	Disponível	Disponível
Exibição com a sessão **Segurança** na janela de propriedades do Servidor de Administração e grupos de administração (disponível apenas em Consoles de Administração baseados em MMC)	Indisponível	Indisponível	Disponível	Disponível
Distribuição aleatória do tempo de inicialização para a tarefa de atualização em dispositivos cliente	Indisponível	Em um intervalo de 5 minutos	Em um intervalo de 10 minutos	Em um intervalo de 10 minutos

Se você conectar o Servidor de Administração com um servidor de banco de dados MySQL (versão 5.7) ou SQL Express, recomendamos evitar usar o aplicativo para gerenciar mais do que 10.000 dispositivos. Para o sistema de gerenciamento de banco de dados MariaDB, o número máximo recomendado de dispositivos gerenciados é 20.000.

Etapa 6. Seleção do banco de dados

Nesta etapa do assistente, selecione um dos sistemas de gerenciamento de banco de dados (DBMS) a seguir que serão usados para armazenar o banco de dados do Servidor de Administração:

- **Microsoft SQL Server ou SQL Server Express**
- **MySQL ou MariaDB**
- **PostgreSQL ou Postgres Pro**

Recomenda-se instalar o Servidor de Administração em um servidor dedicado em vez de um controlador de domínio. Porém, ao instalar o Kaspersky Security Center em um servidor que atua como controlador de domínio somente leitura (RODC), o Microsoft SQL Server (SQL Express) não deve estar instalado localmente (no mesmo dispositivo). Nesse caso, recomendamos que você instale o Microsoft SQL Server (SQL Express) remotamente (em um outro dispositivo) ou use MySQL, MariaDB ou PostgreSQL se precisar instalar o DBMS localmente.

A estrutura do banco de dados do Servidor de Administração é fornecida no arquivo klakdb.chm, localizado na pasta de instalação do Kaspersky Security Center. Esse arquivo também está disponível em um arquivo no portal Kaspersky: klakdb.zip.

Etapa 7. Configuração do servidor SQL

Nesta etapa do assistente, especifique as seguintes configurações de conexão, dependendo do sistema de gerenciamento de banco de dados (DBMS) selecionado:

- Se você selecionou **Microsoft SQL Server ou SQL Server Express** na etapa anterior:

  - No campo **Nome da instância do SQL Server**, especifique o nome do SQL Server na rede. Para visualizar uma lista de todos os servidores SQL que estão na rede, clique no botão **Procurar**. Este valor está vazio por padrão.

    Se você se conectar ao SQL Server por uma porta personalizada, juntamente com o nome do host do SQL Server, especifique o número da porta separado por vírgula, por exemplo:

    ```
    SQL_Server_host_name,1433
    ```

    Ao proteger a comunicação entre o Servidor de Administração e o SQL Server por meio de um certificado, especifique no campo **Nome da instância do SQL Server** o mesmo nome do host usado na geração do certificado. Ao usar uma instância nomeada do SQL Server, juntamente com o nome do host do SQL Server, especifique o número da porta separado por vírgula, por exemplo:

    ```
    SQL_Server_name,1433
    ```

    Ao usar várias instâncias do SQL Server no mesmo host, especifique adicionalmente o nome da instância separado por uma barra invertida, por exemplo:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Caso um SQL Server na rede corporativa tenha o recurso Always On ativado, especifique o nome do ouvinte do grupo de disponibilidade no campo **Nome da instância do SQL Server**. Observe que o Servidor de Administração é compatível apenas com o modo de disponibilidade de confirmação síncrona quando o recurso Always On estiver ativado.

  - No campo **Nome do banco de dados**, especifique o nome do DBMS que foi criado para armazenar dados do Servidor de Administração. O valor padrão é *KAV*.

  Se você desejar instalar o SQL Server em um dispositivo do qual você estiver instalando o Kaspersky Security Center, deverá parar a instalação e reiniciá-la após a instalação do SQL Server. As versões do SQL Server suportadas estão listadas nos requisitos do sistema.

  Se você deseja instalar o SQL Server em um dispositivo remoto, não há necessidade de interromper o Assistente de Instalação do Kaspersky Security Center. Instale o servidor SQL e retome a instalação do Kaspersky Security Center.

- Se você selecionou **MySQL ou MariaDB** na etapa anterior:

  - No campo **Nome da instância do SQL Server**, especifique o nome da instância do DBMS. Por padrão, o nome é o endereço IP do dispositivo no qual o Kaspersky Security Center deve ser instalado.

  - No campo **Porta**, especifique a porta de conexão do Servidor de Administração ao DBMS. O número da porta padrão é 3306.

  - No campo **Nome do banco de dados**, especifique o nome do DBMS que foi criado para armazenar dados do Servidor de Administração. O valor padrão é *KAV*.

- Se você selecionou **PostgreSQL ou Postgres Pro** na etapa anterior:

  - No campo **Servidor PostgreSQL ou Postgres Pro**, especifique o nome da instância do DBMS. Por padrão, o nome é o endereço IP do dispositivo no qual o Kaspersky Security Center deve ser instalado.

- No campo **Porta**, especifique a porta de conexão do Servidor de Administração ao DBMS. O número da porta padrão é 5432.

- No campo **Nome do banco de dados**, especifique o nome do DBMS que foi criado para armazenar dados do Servidor de Administração. O valor padrão é *KAV*.

Etapa 8. Seleção do modo de autenticação

Determine o modo de autenticação que será usado durante a conexão do Servidor de Administração ao sistema de gerenciamento do banco de dados (DBMS).

Dependendo do DBMS selecionado, será possível selecionar um dos seguintes modos de autenticação:

- Para SQL Express ou Microsoft SQL Server, selecione uma das seguintes opções:

  - **Modo de Autenticação do Microsoft Windows**. A verificação de direitos usa a conta usada para iniciar o Servidor de Administração.

  - **Modo de Autenticação do SQL Server**. Se selecionar essa opção, a conta especificada na janela será usada para verificar os direitos de acesso. Preencha os campos **Conta** e **Senha**.

    Para ver a senha inserida, mantenha pressionado o botão **Exibir**.

  Para ambos os modos de autenticação, o aplicativo verifica se o banco de dados está disponível. Você precisa fornecer as credenciais corretas, pois receberá uma mensagem de erro caso o banco de dados não esteja disponível.

  Se o banco de dados de Servidor de Administração estiver armazenado em outro dispositivo e a conta do Servidor de Administração não tiver acesso ao servidor do banco de dados, você deve usar o modo de autenticação do SQL Server instalando ou atualizando o Servidor de Administração. Isso pode ocorrer quando o dispositivo que armazena os bancos de dados estiver fora do domínio ou quando o Servidor de Administração estiver instalado sob uma conta do LocalSystem.

- Para MySQL, MariaDB, PostgreSQL ou Postgres Pro, especifique a conta e a senha.

Etapa 9. Selecionar a conta para iniciar o Servidor de Administração

Selecione a conta que será usada para iniciar o Servidor de Administração como um serviço:

- **Gerar a conta automaticamente**. O aplicativo cria uma conta denominada KL-AK-*, sob a qual o serviço kladminserver será executado.

  Você pode selecionar esta opção se planeja localizar a pasta compartilhada e o DBMS no mesmo dispositivo como o Servidor de Administração.

- **Selecione uma conta**. O serviço do Servidor de Administração (kladminserver) será executado sob a conta que você selecionou.

  Você terá que selecionar uma conta de domínio se, por exemplo, planeja usar o DBMS como uma instância do SQL Server de qualquer versão, incluindo o SQL Express, que esteja localizado em outro dispositivo, e/ou se estiver planejando localizar a pasta compartilhada em outro dispositivo.

  O Kaspersky Security Center dá suporte a contas de serviço gerenciadas (MSA) e contas de serviço gerenciadas em grupo (gMSA). Se esses tipos de contas forem usados no seu domínio, é possível selecionar um deles como a conta para o serviço do Servidor de Administração.

  Antes de especificar a MSA ou gMSA, é necessário instalar a conta no mesmo dispositivo em que deseja instalar o Servidor de Administração. Se a conta ainda não estiver instalada, cancele a instalação do Servidor de Administração, instale a conta e reinicie a instalação do Servidor de Administração. Para detalhes sobre a instalação de contas de serviço gerenciadas em um dispositivo local, consulte a documentação oficial da Microsoft.

  Para especificar a MSA ou gMSA:

  1. Clique no botão **Procurar**.
  2. Na janela que se abre, clique no botão **Tipo de objeto**.
  3. Selecionar o tipo **Conta para serviços** e clique em **OK**.
  4. Selecione a conta relevante e clique em **OK**.

A conta que você selecionou deve ter permissões diferentes, dependendo do DBMS que planeja usar.

Para motivos de segurança, não atribua o status privilegiado à conta sob a qual você executa o Servidor de Administração.

A conta do Servidor de Administração não poderá ser alterada posteriormente. É preciso reinstalar o cluster de failover para usar outra conta do Servidor de Administração.

Etapa 10. Selecionar a conta para a execução dos serviços do Kaspersky Security Center

Selecione a conta sob a qual os serviços do Kaspersky Security Center serão executados neste dispositivo:

- **Gerar a conta automaticamente**. O Kaspersky Security Center cria uma conta local denominada KlScSvc neste dispositivo no grupo kladmins. Os serviços do Kaspersky Security Center serão executados sob a conta que foi criada.

- **Selecione uma conta**. Os serviços do Kaspersky Security Center serão executados sob a conta que você selecionou.

  Você terá de selecionar uma conta de domínio se, por exemplo, pretende salvar relatórios em uma pasta localizada em um dispositivo diferente ou se isto for necessário pela política de segurança da sua organização. Também deverá selecionar uma conta de domínio se você instalar o Servidor de Administração em um cluster de correção da falha.

Para motivos de segurança, não conceda o status privilegiado à conta soba a qual os serviços são executados.

O serviço de proxy da KSN (ksnproxy), o serviço do servidor proxy de ativação da Kaspersky (klactprx) e o serviço do portal de autenticação da Kaspersky (klwebsrv) serão executados sob a conta selecionada.

Etapa 11. Seleção de uma pasta compartilhada

Defina a localização e o nome da pasta compartilhada que será usada para realizar as seguintes ações:

- Armazene os arquivos necessários para a instalação remota dos aplicativos (os arquivos serão copiados para o Servidor de Administração durante a criação dos pacotes de instalação).

- Armazenar atualizações que foram baixadas de uma fonte de atualização para o Servidor de Administração.

O compartilhamento de arquivos (somente leitura) será ativado para todos os usuários.

Você pode selecionar uma das seguintes opções:

- **Criar pasta compartilhada**. Criação de uma nova pasta. Na caixa de texto, especifique o caminho para a pasta.

- **Selecionar uma pasta compartilhada existente**. Selecione uma pasta compartilhada que já existe.

A pasta compartilhada pode ser uma pasta local no dispositivo que é usado para a instalação ou em diretório remoto em qualquer dispositivo cliente na rede corporativa. Você pode usar o botão **Procurar** para selecionar a pasta compartilhada ou especificá-la manualmente ao inserir seu caminho UNC (por exemplo, \\server\Share) no campo correspondente.

Por padrão, o instalador cria uma subpasta KLSHARE local na pasta do programa contendo os componentes do Kaspersky Security Center.

É possível definir uma pasta compartilhada posteriormente, caso seja necessário.

Etapa 12. Configuração de conexão ao Servidor de Administração

Configurar a conexão ao Servidor de Administração:

- **Porta**

  O número da porta usada para conectar ao Servidor de Administração.

  O número da porta padrão é 14000.

- **Porta SSL**

  Número da porta SSL (Secure Sockets Layer) usada para conectar em segurança ao Servidor de Administração, através do SSL.

  O número da porta padrão é 13000.

- **Comprimento da chave de criptografia**

  Selecione o comprimento da chave de criptografia: 1024 bits ou 2048 bits.

  Uma chave de criptografia de 1024 bits coloca uma carga menor na CPU, mas se considera ser obsoleta porque ela não pode fornecer uma criptografia confiável devido às suas especificações técnicas. Também, o hardware existente provavelmente resultará ser incompatível com certificados SSL que tenham chaves de 1024 bits.

  Uma chave de criptografia de 2048 bits atende todos os padrões de criptografia estado da arte. No entanto, o uso de uma chave de criptografia de 2048 bits pode adicionar à carga em uma CPU.

  Por padrão, **2048 bits (melhor segurança)** é selecionado.

Você também pode alterar os parâmetros para conectar-se ao Servidor de Administração posteriormente da seguinte forma:

- É possível alterar os números da porta e da porta SSL na seção **Portas de conexão** das propriedades do Servidor de Administração. Para obter mais informações sobre as portas de conexão do Servidor de Administração, consulte Portas usadas pelo Kaspersky Security Center.

- Você pode alterar o comprimento da chave de criptografia ao substituir o certificado do Servidor de Administração pelo utilitário klsetsrvcert usando o parâmetro `-o RsaKeyLen:<comprimento da chave>`.

Etapa 13. Definição do endereço do Servidor de Administração

Especifique o endereço do Servidor de Administração usando uma das seguintes formas:

- **Nome do domínio DNS**. É possível usar o método se a rede incluir um servidor DNS e se os dispositivos cliente puderem usá-lo para receber o endereço do Servidor de Administração.
- **Nome NetBIOS**. É possível usar o método se os dispositivos cliente receberem o endereço do Servidor de Administração por meio do protocolo NetBIOS ou houver um servidor WINS disponível na rede.
- **Endereço IP**. É possível usar o método se o Servidor de Administração possuir um endereço IP estático que não será mudado no futuro.

Caso o Kaspersky Security Center seja instalado no nó ativo do cluster de failover do Kaspersky Security Center e um adaptador de rede secundário tenha sido criado ao preparar os nós do cluster, especifique o endereço IP desse adaptador. Caso contrário, insira o endereço IP do balanceador de carga de terceiros em uso.

Etapa 14. Endereço do Servidor de Administração para conexão de dispositivos móveis

Essa etapa do Assistente de Instalação está disponível se você selecionar o Gerenciamento de Dispositivos Móveis para instalação.

Na janela **Endereço para conexão de dispositivos móveis**, especifique o endereço externo do Servidor de Administração para a conexão de dispositivos móveis que estão fora da rede local. É possível especificar o endereço IP ou o Domain Name System (DNS) do Servidor de Administração.

Etapa 15. Seleção dos plugins de gerenciamento de aplicativos

Selecione os plugins de gerenciamento de aplicativos que devem ser instalados com o Kaspersky Security Center.

Para a facilidade da pesquisa, os plugins são divididos em grupos dependendo do tipo de objeto tornado seguro.

Etapa 16. Descompactação e instalação dos arquivos no disco rígido

Após a instalação dos componentes do Kaspersky Security Center, você pode iniciar a instalação dos arquivos no disco rígido.

Se a instalação requerer programas adicionais, o Assistente de instalação vai notificá-lo, na página **Pré-requisitos de instalação**, antes de iniciar a instalação do Kaspersky Security Center. Os programas requeridos serão instalados automaticamente após você clicar no botão **Avançar**.

Na última página, você pode selecionar qual console iniciar para uso com o Kaspersky Security Center:

- **Iniciar Console de Administração baseado em MMC**
- **Iniciar o Kaspersky Security Center Web Console**

  Esta opção estará disponível somente se você tiver optado por instalar o Kaspersky Security Center Web Console em uma das etapas anteriores.

Você também pode clicar em **Concluir** para fechar o assistente sem iniciar o trabalho com o Kaspersky Security Center. Você pode iniciar o trabalho depois, a qualquer momento.

No momento da primeira inicialização do Console de Administração ou Kaspersky Security Center Web Console, você poderá executar a configuração inicial do aplicativo.

Implementação do cluster de failover do Kaspersky Security Center

Esta seção contém informações gerais sobre o cluster de failover do Kaspersky Security Center e instruções sobre a preparação e implementação do cluster de failover do Kaspersky Security Center em sua rede.

Cenário: implantação de um cluster de failover do Kaspersky Security Center

Um cluster de failover do Kaspersky Security Center garante a alta disponibilidade do Kaspersky Security Center e minimiza o tempo de inatividade do Servidor de Administração, em caso de falha. O cluster de failover é baseado em duas instâncias idênticas do Kaspersky Security Center, instaladas em dois computadores. Uma das instâncias funciona como o nó ativo e a outra, como o nó passivo. O nó ativo gerencia a proteção dos dispositivos clientes, enquanto o passivo está preparado para assumir todas as funções do nó ativo caso o nó ativo falhe. Quando ocorre uma falha, o nó passivo torna-se ativo e o nó ativo torna-se passivo.

Pré-requisitos

Você possui hardware que atende aos requisitos para o cluster de failover.

Fases

A implementação dos aplicativos da Kaspersky é feita em fases:

1. **Como criar uma conta para os serviços do Kaspersky Security Center**

   Crie um novo grupo de domínio (neste cenário, o nome 'KLAdmins' é usado para esse grupo) e conceda as permissões de administrador local ao grupo em ambos os nós e no servidor de arquivos. Em seguida, crie duas novas contas de usuário de domínio (neste cenário, os nomes 'ksc' e 'rightless' são usados para essas contas) e adicione as contas ao grupo de domínio KLAdmins.

   Adicione a conta de usuário sob a qual o Kaspersky Security Center será instalado ao grupo de domínio KLAdmins criado anteriormente.

2. **Preparação do servidor de arquivos**

Prepare o servidor de arquivos para funcionar como um componente do cluster de failover do Kaspersky Security Center. Certifique-se de que o servidor de arquivos atenda aos requisitos de hardware e software, crie duas pastas compartilhadas para os dados do Kaspersky Security Center e configure as permissões para acessar as pastas compartilhadas.

Instruções: Preparando um servidor de arquivos para o cluster de failover do Kaspersky Security Center

3. **Preparação de nós ativos e passivos**

   Prepare dois dispositivos com hardware e software idênticos para funcionarem como nós ativos e passivos.

   Instruções: Preparando nós para o cluster de failover do Kaspersky Security Center

4. **Instalação do sistema de gerenciamento de banco de dados (DBMS)**

   Selecione qualquer um dos DBMS compatíveis e instale o DBMS em um dispositivo dedicado. Para obter informações sobre como instalar o DBMS, consulte a sua documentação.

5. **Instalação do Kaspersky Security Center**

   Instale o Kaspersky Security Center no modo de cluster de failover em ambos os nós. Primeiro, é necessário instalar o Kaspersky Security Center no dispositivo que será o host ativo e, em seguida, instalá-lo no host passivo.

   É necessário instalar o Kaspersky Security Center Web Console em um dispositivo separado que não seja um nó de cluster.

   Instruções: Instalando o Kaspersky Security Center nos nós do cluster de failover do Kaspersky Security Center

6. **Como testar o cluster de failover**

   Verifique se você configurou o cluster de failover corretamente e se ele funciona corretamente. Por exemplo, você pode interromper um dos serviços do Kaspersky Security Center no nó ativo: kladminserver, klnagent, ksnproxy, klactprx ou klwebsrv. Após o serviço ser interrompido, o gerenciamento de proteção deve ser alternado automaticamente para o nó passivo.

Resultados

O cluster de failover do Kaspersky Security Center é implementado. Familiarize-se com os eventos que levam à alternância entre os nós ativos e passivos.

Sobre o cluster de failover do Kaspersky Security Center

Um cluster de failover do Kaspersky Security Center garante a alta disponibilidade do Kaspersky Security Center e minimiza o tempo de inatividade do Servidor de Administração, em caso de falha. O cluster de failover é baseado em duas instâncias idênticas do Kaspersky Security Center, instaladas em dois computadores. Uma das instâncias funciona como o nó ativo e a outra, como o nó passivo. O nó ativo gerencia a proteção dos dispositivos clientes, enquanto o passivo está preparado para assumir todas as funções do nó ativo caso o nó ativo falhe. Quando ocorre uma falha, o nó passivo torna-se ativo e o nó ativo torna-se passivo.

O uso do cluster de failover não afeta os cálculos baseados na Guia de dimensionamento.

Use o recurso Log de eventos Kaspersky para a resolução de problemas.

Condições de alternância

O cluster de failover alterna o gerenciamento de proteção dos dispositivos clientes do nó ativo para o nó passivo se qualquer um dos seguintes eventos ocorrer no nó ativo:

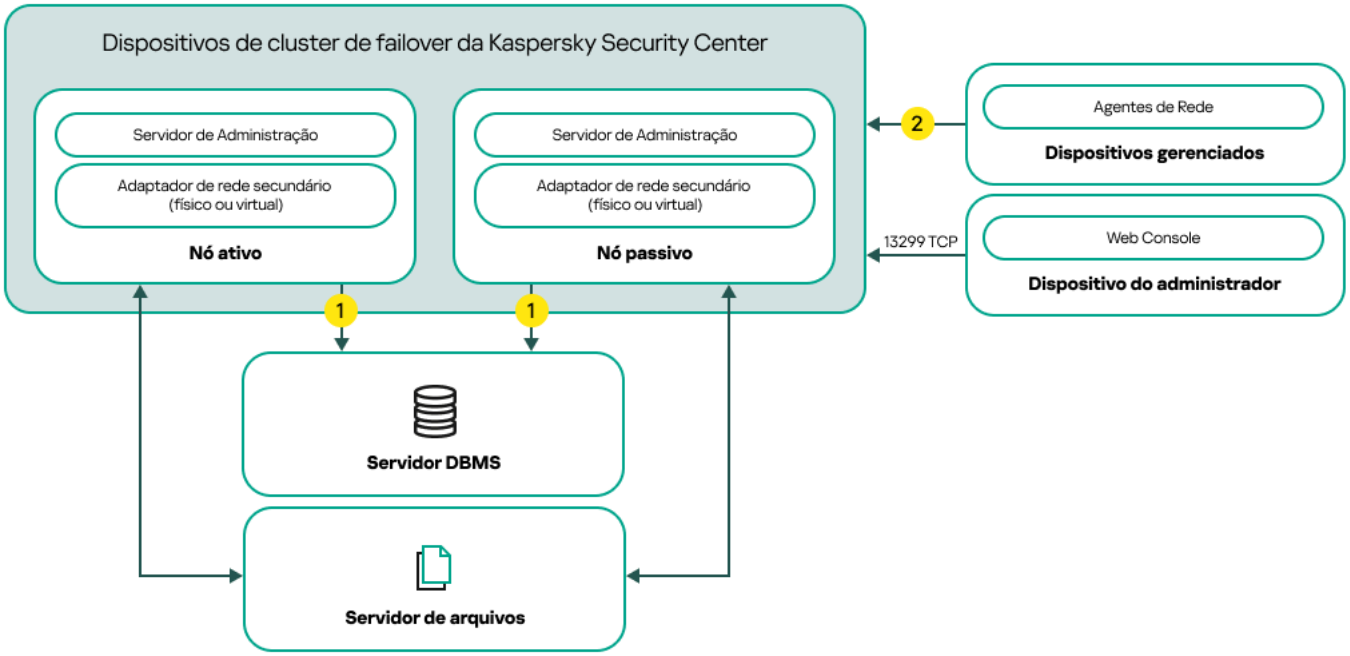
- O nó ativo foi interrompido devido a uma falha de software ou hardware.
- O nó ativo foi temporariamente interrompido por atividades de manutenção.
- Pelo menos um dos serviços (ou processos) do Kaspersky Security Center falhou ou foi encerrado deliberadamente pelo usuário. Os serviços do Kaspersky Security Center são os seguintes: kladminserver, klnagent, klactprx e klwebsrv.
- A conexão de rede entre o nó ativo e o armazenamento no servidor de arquivos foi interrompida ou encerrada.

O cluster de failover da Kaspersky Security Center gerencia todos os serviços da Kaspersky Security Center de forma automática. Não reinicie os serviços manualmente.

Esquemas de implementação

É possível escolher um dos seguintes esquemas para implementar o cluster de failover do Kaspersky Security Center:

- Um esquema que usa um adaptador de rede secundário.
- Um esquema que usa um balanceador de carga de terceiros.

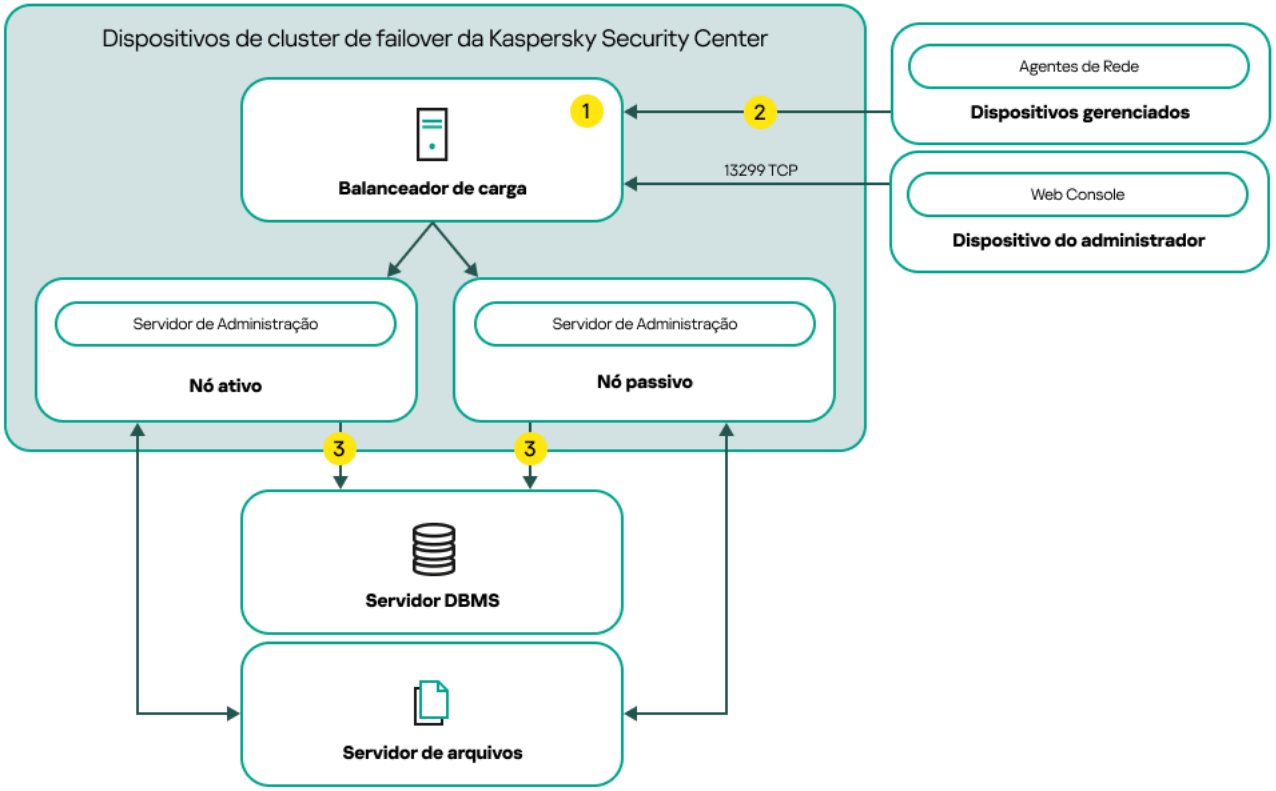


Um esquema que usa um adaptador de rede secundário

Legenda do esquema:

1 O Servidor de Administração envia dados para o banco de dados. Abra as portas necessárias no dispositivo onde o banco de dados está localizado, por exemplo, a porta 3306 para o MySQL Server ou a porta 1433 para o Microsoft SQL Server. Consulte a documentação do DBMS para obter informações relevantes.

2 Nos dispositivos gerenciados, abra as seguintes portas: TCP 13000, UDP 13000 e TCP 17000.



Um esquema que usa um balanceador de carga de terceiros

Legenda do esquema:

1 No dispositivo do balanceador de carga, abra todas as portas do Servidor de Administração: TCP 13000, UDP 13000, TCP 13299 e TCP 17000.

> Caso deseje usar o utilitário klakaut para automatização, você também deve abrir a porta TCP 13291.

2 Nos dispositivos gerenciados, abra as seguintes portas: TCP 13000, UDP 13000 e TCP 17000.

3 O Servidor de Administração envia dados para o banco de dados. Abra as portas necessárias no dispositivo onde o banco de dados está localizado, por exemplo, a porta 3306 para o MySQL Server ou a porta 1433 para o Microsoft SQL Server. Consulte a documentação do DBMS para obter informações relevantes.

Preparando um servidor de arquivos para um cluster de failover do Kaspersky Security Center

Um servidor de arquivos funciona como um componente necessário de um cluster de failover do Kaspersky Security Center.

Para preparar um servidor de arquivos:

1. Certifique-se de que o servidor de arquivos atenda aos requisitos de hardware e software.
2. Certifique-se de que o servidor de arquivos e ambos os nós (ativo e passivo) estejam incluídos no mesmo domínio ou que o servidor de arquivos é o controlador de domínio.

3. No servidor de arquivos, crie duas pastas compartilhadas. Uma delas é usada para manter informações sobre o estado do cluster de failover. A outra é usada para armazenar os dados e configurações do Kaspersky Security Center. Você especificará caminhos para as pastas compartilhadas ao configurar a instalação do Kaspersky Security Center.

4. Conceda permissões de acesso total (permissões de compartilhamento e permissões de NTFS) às pastas compartilhadas criadas para as seguintes contas de usuário e grupos:

   - Grupo de domínio KLAdmins.
   - Contas de usuário $<node1> e $<node2>. Neste caso, <node1> e <node2> são os nomes dos dispositivos dos nós ativos e passivos.

O servidor de arquivos está preparado. Para implantar o cluster de failover do Kaspersky Security Center, siga as instruções adicionais neste cenário.

Preparando nós para um cluster de failover do Kaspersky Security Center

Prepare dois dispositivos para funcionarem como nós ativos e passivos para um cluster de failover do Kaspersky Security Center.

Para preparar nós para um cluster de failover do Kaspersky Security Center:

1. Certifique-se de ter dois dispositivos que atendam aos requisitos de hardware e software. Esses dispositivos atuarão como nós ativos e passivos do cluster de failover.

2. Certifique-se de que o servidor de arquivos e ambos os nós estejam incluídos no mesmo domínio.

3. Execute uma das seguintes ações:

   - Em cada um dos nós, configure um adaptador de rede secundário.

     Um adaptador de rede secundário pode ser físico ou virtual. Caso queira usar um adaptador de rede físico, conecte-o e configure-o com as ferramentas padrão do sistema operacional. Caso queira usar um adaptador de rede virtual, crie-o usando um software de terceiros.

     Certifique-se de que as seguintes condições sejam atendidas:

     - Os adaptadores de rede secundários estão desativados.

       É possível criar os adaptadores de rede secundários, no estado desativado, ou desativá-los após a criação.

     - Os adaptadores de rede secundários em ambos os nós devem ter o mesmo endereço IP.

   - Use um balanceador de carga de terceiros. Por exemplo, você pode usar um servidor nginx. Nesse caso, faça o seguinte:

     a. Forneça um dispositivo dedicado baseado em Linux com nginx instalado.

     b. Configure o balanceamento de carga. Defina o nó ativo como o servidor principal e o nó passivo como o servidor de backup.

     c. No servidor nginx, abra todas as portas do Servidor de Administração: TCP 13000, UDP 13000, TCP 13299 e TCP 17000.

        Caso deseje usar o utilitário klakaut para automatização, você também deve abrir a porta TCP 13291.

4. Reinicie os nós e o servidor de arquivos.

5. Mapeie as duas pastas compartilhadas, que você criou durante a etapa de preparação do servidor de arquivos, para cada um dos nós. Você deve mapear as pastas compartilhadas como unidades de rede. Ao mapear as pastas, você pode selecionar qualquer letra de unidade vazia. Para acessar as pastas compartilhadas, use as credenciais da conta de usuário criadas durante a etapa 1 do cenário.

Os nós estão preparados. Para implantar o cluster de failover do Kaspersky Security Center, siga as instruções adicionais do cenário.

Instalando o Kaspersky Security Center nos nós do cluster de failover do Kaspersky Security Center

O Kaspersky Security Center é instalado separadamente em ambos os nós do cluster de failover do Kaspersky Security Center. Primeiro, você instala o aplicativo no nó ativo e, em seguida, no passivo. Ao instalar, você escolhe qual nó ficará ativo e qual será passivo.

Apenas um usuário do grupo de domínio KLAdmins pode instalar o Kaspersky Security Center em cada nó.

Para instalar o Kaspersky Security Center no nó ativo do cluster de failover do Kaspersky Security Center:

1. Execute o arquivo executável ksc_14.2_<número da compilação>_full_<idioma>.exe.

   Uma janela é aberta, solicitando que você selecione os aplicativos Kaspersky para instalar. Na janela de seleção do aplicativo, clique no link **Instalar o Servidor de Administração do Kaspersky Security Center** para iniciar o Assistente de instalação do Servidor de Administração. Siga as instruções do Assistente.

2. Leia cuidadosamente o Contrato de Licença e a Política de privacidade. Se você concordar com todos os termos do Contrato de Licença e da Política de Privacidade, selecione as seguintes caixas de seleção na seção **Eu confirmo que li, entendi e aceito todo o seguinte**:

   - **Os termos e condições deste EULA**
   - **Política de Privacidade que descreve o manuseio de dados**

   A Instalação do aplicativo no seu dispositivo continuará após você selecionar ambas as caixas de seleção.

   Se você não concordar com o Contrato de Licença ou a Política de Privacidade, cancele a instalação clicando no botão **Cancelar**.

3. Selecione **Nó primário do Kaspersky Failover Cluster** para instalar o aplicativo no nó ativo.

4. Na janela **Pasta compartilhada**, defina o seguinte:

   - Nos campos **Compartilhamento de estado** e **Compartilhamento de dados**, especifique os caminhos para as pastas compartilhadas que você criou no servidor de arquivos durante a preparação.
   - Nos campos **Unidade do compartilhamento de estado** e **Unidade do compartilhamento de dados**, selecione as unidades de rede para as quais você mapeou as pastas compartilhadas durante a preparação dos nós.
   - Selecione o modo de conectividade do cluster: por um adaptador de rede secundário ou um balanceador de carga de terceiros.

5. Execute outras etapas da instalação personalizada, começando com a etapa 3.

   Na etapa 13, especifique o endereço IP de um adaptador de rede secundário, caso tenha criado um adaptador ao preparar os nós do cluster. Caso contrário, insira o endereço IP do balanceador de carga de terceiros em uso.

O Kaspersky Security Center é instalado no nó ativo.

Para instalar o Kaspersky Security Center no nó passivo do cluster de failover do Kaspersky Security Center:

1. Execute o arquivo executável ksc_14.2_<número da compilação>_full_<idioma>.exe.

   Uma janela é aberta, solicitando que você selecione os aplicativos Kaspersky para instalar. Na janela de seleção do aplicativo, clique no link **Instalar o Servidor de Administração do Kaspersky Security Center** para iniciar o Assistente de instalação do Servidor de Administração. Siga as instruções do Assistente.

2. Leia cuidadosamente o Contrato de Licença e a Política de privacidade. Se você concordar com todos os termos do Contrato de Licença e da Política de Privacidade, selecione as seguintes caixas de seleção na seção **Eu confirmo que li, entendi e aceito todo o seguinte**:

   - **Os termos e condições deste EULA**
   - **Política de Privacidade que descreve o manuseio de dados**

   A Instalação do aplicativo no seu dispositivo continuará após você selecionar ambas as caixas de seleção.

   Se você não concordar com o Contrato de Licença ou a Política de Privacidade, cancele a instalação clicando no botão **Cancelar**.

3. Selecione **Nó secundário do Kaspersky Failover Cluster** para instalar o aplicativo no nó passivo.

4. Na janela **Pasta compartilhada**, no campo **Compartilhamento de estado**, especifique um caminho para a pasta compartilhada com informações sobre o estado do cluster criado no servidor de arquivos durante a preparação.

5. Clique no botão **Instalar**. Quando a instalação terminar, clique no botão **Concluir**.

O Kaspersky Security Center é instalado no nó passivo. Agora, é possível testar o cluster de failover do Kaspersky Security Center para verificar se ele foi configurado e funciona corretamente.

Iniciando e interrompendo nós de cluster manualmente

Pode ser necessário interromper todo o cluster de failover do Kaspersky Security Center ou desvincular temporariamente um dos nós do cluster para manutenção. Nesse caso, siga as instruções nesta seção. Não tente iniciar ou interromper os serviços ou processos relacionados ao cluster de failover usando qualquer outro meio. Isso pode causar a perda de dados.

Iniciando e interrompendo todo o cluster de failover para manutenção

Para iniciar ou interromper todo o cluster de failover:

1. No nó ativo, vá para <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Abra a linha de comando e execute um dos seguintes comandos:

   - Para interromper o cluster, execute: `klfoc -stopcluster --stp klfoc`
   - Para iniciar o cluster, execute: `klfoc -startcluster --stp klfoc`

O cluster de failover é iniciado ou interrompido, de acordo com o comando executado.

Mantendo um dos nós

Para manter um dos nós:

1. No nó ativo, interrompa o cluster de failover usando o comando `klfoc -stopcluster --stp klfoc`.
2. No nó que deseja manter, vá para <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
3. Abra a linha de comando e desvincule o nó do cluster executando o comando `detach_node.cmd`.
4. No nó ativo, inicie o cluster de failover usando o comando `klfoc -startcluster --stp klfoc`.
5. Execute as atividades de manutenção.
6. No nó ativo, interrompa o cluster de failover usando o comando `klfoc -stopcluster --stp klfoc`.
7. No nó mantido, vá para <Disk>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
8. Abra a linha de comando e vincule o nó ao cluster executando o comando `attach_node.cmd`.
9. No nó ativo, inicie o cluster de failover usando o comando `klfoc -startcluster --stp klfoc`.

O nó é mantido e conectado ao cluster de failover.

Instalação do Servidor de Administração em um cluster de failover da Microsoft

O procedimento de instalação do Servidor de Administração em um cluster de failover difere da instalação padrão e personalizada em um dispositivo independente.

Execute o procedimento descrito nesta seção no nó que contém um armazenamento de dados comum do cluster.

Para instalar o Servidor de Administração do Kaspersky Security Center em um cluster:

Execute o arquivo ksc_<número da versão>.<número de build>_full_<idioma de localização>.exe.

Uma janela é exibida, solicitando que você selecione os aplicativos Kaspersky para instalar. Na janela de seleção do aplicativo, clique no link **Instalar o Servidor de Administração do Kaspersky Security Center** para executar o assistente de instalação do Servidor de Administração. Siga as instruções do Assistente.

Etapa 1. Leitura do Contrato de Licença e da Política de Privacidade

Nessa etapa do Assistente de instalação, você deve ler o Contrato de Licença, o qual é celebrado entre você e a Kaspersky, assim como a Política de Privacidade.

Também é possível que seja solicitado que leia os Contrato de Licença e as Políticas de Privacidade dos plugins de gerenciamento disponíveis no kit de distribuição do Kaspersky Security Center.

Leia cuidadosamente o Contrato de Licença e a Política de privacidade. Caso concorde com todos os termos do Contrato de licença e da Política de Privacidade, confirme tudo isso marcando as caixas de seleção apropriadas.

A Instalação do aplicativo no seu dispositivo continuará após você selecionar ambas as caixas de seleção.

Se você não concordar com o Contrato de Licença ou a Política de Privacidade, cancele a instalação clicando no botão **Cancelar**.

Etapa 2. Selecionando o tipo de instalação em um cluster

Selecione o tipo de instalação no cluster:

- **Cluster (instalar em todos os nós do cluster)**

  Esta é a opção recomendada. Se você selecionar esta opção, o Servidor de Administração será instalado em todos os nós do cluster simultaneamente.

  > Na etapa de seleção do Console de Administração para instalação, será necessário selecionar o console a ser instalado no nó do cluster atual. Caso um console seja instalado apenas no nó do cluster, em caso de falha do nó, o acesso ao Servidor de Administração será perdido. Recomendamos que durante esta etapa, você selecione o console de administração baseado em MMC para instalação em todos os nós do cluster. Depois de instalar o Servidor de Administração, instale o Kaspersky Security Center Web Console em um dispositivo separado que não seja um nó de cluster. Isso permite o gerenciamento do Servidor de Administração pelo Kaspersky Security Center Web Console caso o nó do cluster falhe.

- **Localmente (instale apenas neste dispositivo)**

  Se você selecionar esta opção, o Servidor de Administração será instalado apenas no nó atual, como se fosse um servidor independente, e não funcionará como um aplicativo com reconhecimento de cluster. Por exemplo, é possível escolher esta opção para economizar espaço de armazenamento compartilhado, caso a tolerância a falhas não seja necessária para o Servidor de Administração. No caso de falha do nó atual, você terá que instalar o Servidor de Administração em outro nó e restaurar o estado do Servidor de Administração a partir de um backup.

As etapas seguintes são idênticas às usadas no método de instalação padrão ou personalizado, começando na etapa de seleção do método de instalação.

Etapa 3. Especificando o nome do Servidor de Administração virtual

Especifique o nome da rede do novo Servidor de Administração virtual. Você poderá usar este nome para conectar o Console de Administração ou o Kaspersky Security Center Web Console ao Servidor de Administração.

O nome especificado deve ser diferente do nome do cluster.

Etapa 4. Especificando os detalhes da rede do Servidor de Administração virtual

Para especificar os detalhes da rede da nova instância do Servidor de Administração virtual:

1. Em **Rede a ser usada,** selecione a rede de domínio à qual o nó do cluster atual está conectado.
2. Execute alguma das seguintes ações:
   - Se o DHCP for usado na rede selecionada para atribuir endereços IP, selecione a opção **Usar DHCP**.
   - Se o protocolo DHCP não for usado na rede selecionada, especifique o endereço IP necessário.

     O endereço IP especificado deve ser diferente do endereço IP do cluster.
3. Clique em **Adicionar** para aplicar as configurações especificadas.

Você poderá usar o endereço IP atribuído automaticamente ou especificado para conectar o Console de Administração ou Kaspersky Security Center Web Console ao Servidor de Administração.

Etapa 5. Especificando um grupo de cluster

Um grupo de cluster é uma função de cluster de failover especial que contém recursos comuns para todos os nós. Você tem duas opções:

- Criar um novo grupo de clusters.

  Esta opção é recomendada na maioria dos casos. O novo grupo de cluster conterá todos os recursos comuns relacionados à instância do Servidor de Administração.

- Selecionar um grupo de clusters existente.

  Selecione esta opção se desejar usar um recurso comum que já está associado a um grupo de clusters existente. Por exemplo, você pode querer usar esta opção se quiser usar um armazenamento associado a um grupo de cluster existente e se não houver outro armazenamento disponível para um novo grupo de cluster.

Etapa 6. Selecionando um armazenamento de dados de cluster

Para selecionar um armazenamento de dados em cluster:

1. Em **Repositórios disponíveis**, selecione o armazenamento de dados no qual os recursos comuns da instância do Servidor de Administração virtual serão instalados.
2. Se o armazenamento de dados selecionado contiver vários volumes, em **Seções disponíveis na unidade de disco**, selecione o volume necessário.
3. Em **Caminho de instalação**, insira o caminho no armazenamento de dados comum no qual os recursos da instância do Servidor de Administração virtual serão instalados.

O armazenamento de dados é selecionado.

Etapa 7. Especificando uma conta para instalação remota

Especifique o nome de usuário e a senha que serão usados para instalação remota da instância do Servidor de Administração virtual em um nó passivo do cluster.

A conta especificada deve ter privilégios administrativos em todos os nós do cluster.

Etapa 8. Seleção dos componentes a serem instalados

Selecione os componentes do Servidor de Administração do Kaspersky Security Center que você deseja instalar:

- **Gerenciamento de Dispositivos Móveis**. Selecione esta caixa de seleção, se você deve criar pacotes de instalação para dispositivos móveis quando o Assistente de instalação do Kaspersky Security Center estiver em execução. Você também pode criar pacotes de instalação para dispositivos móveis manualmente, após a instalação do Servidor de Administração, usando as ferramentas do Console de Administração.

- **Agente SNMP**. O componente recebe as informações estatísticas para o Servidor de Administração através do protocolo SNMP. O componente está disponível se o aplicativo estiver instalado em um dispositivo com o SNMP instalado.

  Após a instalação do Kaspersky Security Center, os arquivos .mib necessários para recuperar as estatísticas estarão localizados na subpasta SNMP da pasta de instalação do aplicativo.

O Agente de Rede e o Console de Administração não são exibidos na lista de componentes. Esses componentes são instalados automaticamente e você não pode cancelar sua instalação.

Nessa etapa, você deve especificar uma pasta para instalação dos componentes do Servidor de Administração. Por padrão, os componentes são instalados em <Disco>:\Program Files\Kaspersky Lab\Kaspersky Security Center. Se essa pasta não existir, a pasta é criada automaticamente durante a instalação. Você pode alterar a pasta de destino usando o botão **Procurar**.

Etapa 9. Selecionando o tamanho da rede

Especifique o tamanho da rede na qual o Kaspersky Security Center deve ser instalado. Dependendo do número de dispositivos na rede, o assistente configura a instalação e a aparência da interface do aplicativo de maneira que eles coincidam.

A tabela seguinte lista as configurações de instalação do aplicativo e configurações de aspeto da interface que são ajustadas com base em vários tamanhos de rede.

Configurações de instalação dependendo do tamanho da rede

Configurações	1 a 100 dispositivos gerenciados	101 a 1.000 dispositivos gerenciados	1.001 a 5.000 dispositivos gerenciados	Mais de 5.000 dispositivos gerenciados
Exibição com o nó para Servidores de Administração secundários e virtuais e todas as configurações relacionadas com os Servidores de Administração secundários e virtuais na árvore do console (disponível apenas em um Console de Administração baseado em MMC)	Indisponível	Indisponível	Disponível	Disponível
Exibição com a sessão **Segurança** na janela de propriedades do Servidor de Administração e grupos de administração (disponível apenas em Consoles de Administração baseados em MMC)	Indisponível	Indisponível	Disponível	Disponível
Distribuição aleatória do tempo de inicialização para a tarefa de atualização em dispositivos cliente	Indisponível	Em um intervalo de 5 minutos	Em um intervalo de 10 minutos	Em um intervalo de 10 minutos

Se você conectar o Servidor de Administração com um servidor de banco de dados MySQL (versão 5.7) ou SQL Express, recomendamos evitar usar o aplicativo para gerenciar mais do que 10.000 dispositivos. Para o sistema de gerenciamento de banco de dados MariaDB, o número máximo recomendado de dispositivos gerenciados é 20.000.

Etapa 10. Seleção do banco de dados

Nesta etapa do assistente, selecione um dos sistemas de gerenciamento de banco de dados (DBMS) a seguir que serão usados para armazenar o banco de dados do Servidor de Administração:

- **Microsoft SQL Server ou SQL Server Express**
- **MySQL ou MariaDB**
- **PostgreSQL ou Postgres Pro**

Recomenda-se instalar o Servidor de Administração em um servidor dedicado em vez de um controlador de domínio. Porém, ao instalar o Kaspersky Security Center em um servidor que atua como controlador de domínio somente leitura (RODC), o Microsoft SQL Server (SQL Express) não deve estar instalado localmente (no mesmo dispositivo). Nesse caso, recomendamos que você instale o Microsoft SQL Server (SQL Express) remotamente (em um outro dispositivo) ou use MySQL, MariaDB ou PostgreSQL se precisar instalar o DBMS localmente.

A estrutura do banco de dados do Servidor de Administração é fornecida no arquivo klakdb.chm, localizado na pasta de instalação do Kaspersky Security Center. Esse arquivo também está disponível em um arquivo no portal Kaspersky: klakdb.zip.

Etapa 11. Configuração do servidor SQL

Nesta etapa do assistente, especifique as seguintes configurações de conexão, dependendo do sistema de gerenciamento de banco de dados (DBMS) selecionado:

- Se você selecionou **Microsoft SQL Server ou SQL Server Express** na etapa anterior:

  - No campo **Nome da instância do SQL Server**, especifique o nome do SQL Server na rede. Para visualizar uma lista de todos os servidores SQL que estão na rede, clique no botão **Procurar**. Este valor está vazio por padrão.

    Se você se conectar ao SQL Server por uma porta personalizada, juntamente com o nome do host do SQL Server, especifique o número da porta separado por vírgula, por exemplo:

    ```
    SQL_Server_host_name,1433
    ```

    Ao proteger a comunicação entre o Servidor de Administração e o SQL Server por meio de um certificado, especifique no campo **Nome da instância do SQL Server** o mesmo nome do host usado na geração do certificado. Ao usar uma instância nomeada do SQL Server, juntamente com o nome do host do SQL Server, especifique o número da porta separado por vírgula, por exemplo:

    ```
    SQL_Server_name,1433
    ```

    Ao usar várias instâncias do SQL Server no mesmo host, especifique adicionalmente o nome da instância separado por uma barra invertida, por exemplo:

    ```
    SQL_Server_name\SQL_Server_instance_name,1433
    ```

    Caso um SQL Server na rede corporativa tenha o recurso Always On ativado, especifique o nome do ouvinte do grupo de disponibilidade no campo **Nome da instância do SQL Server**. Observe que o Servidor de Administração é compatível apenas com o modo de disponibilidade de confirmação síncrona quando o recurso Always On estiver ativado.

  - No campo **Nome do banco de dados**, especifique o nome do DBMS que foi criado para armazenar dados do Servidor de Administração. O valor padrão é *KAV*.

  Se você desejar instalar o SQL Server em um dispositivo do qual você estiver instalando o Kaspersky Security Center, deverá parar a instalação e reiniciá-la após a instalação do SQL Server. As versões do SQL Server suportadas estão listadas nos requisitos do sistema.

  Se você deseja instalar o SQL Server em um dispositivo remoto, não há necessidade de interromper o Assistente de Instalação do Kaspersky Security Center. Instale o servidor SQL e retome a instalação do Kaspersky Security Center.

- Se você selecionou **MySQL ou MariaDB** na etapa anterior:

  - No campo **Nome da instância do SQL Server**, especifique o nome da instância do DBMS. Por padrão, o nome é o endereço IP do dispositivo no qual o Kaspersky Security Center deve ser instalado.

  - No campo **Porta**, especifique a porta de conexão do Servidor de Administração ao DBMS. O número da porta padrão é 3306.

  - No campo **Nome do banco de dados**, especifique o nome do DBMS que foi criado para armazenar dados do Servidor de Administração. O valor padrão é *KAV*.

- Se você selecionou **PostgreSQL ou Postgres Pro** na etapa anterior:

  - No campo **Servidor PostgreSQL ou Postgres Pro**, especifique o nome da instância do DBMS. Por padrão, o nome é o endereço IP do dispositivo no qual o Kaspersky Security Center deve ser instalado.

- No campo **Porta**, especifique a porta de conexão do Servidor de Administração ao DBMS. O número da porta padrão é 5432.

No campo **Nome do banco de dados**, especifique o nome do DBMS que foi criado para armazenar dados do Servidor de Administração. O valor padrão é *KAV*.

Etapa 12. Seleção do modo de autenticação

Determine o modo de autenticação que será usado durante a conexão do Servidor de Administração ao sistema de gerenciamento do banco de dados (DBMS).

Dependendo do DBMS selecionado, será possível selecionar um dos seguintes modos de autenticação:

- Para SQL Express ou Microsoft SQL Server, selecione uma das seguintes opções:

  - **Modo de Autenticação do Microsoft Windows**. A verificação de direitos usa a conta usada para iniciar o Servidor de Administração.

  - **Modo de Autenticação do SQL Server**. Se selecionar essa opção, a conta especificada na janela será usada para verificar os direitos de acesso. Preencha os campos **Conta** e **Senha**.

    Para ver a senha inserida, mantenha pressionado o botão **Exibir**.

  Para ambos os modos de autenticação, o aplicativo verifica se o banco de dados está disponível. Você precisa fornecer as credenciais corretas, pois receberá uma mensagem de erro caso o banco de dados não esteja disponível.

  Se o banco de dados de Servidor de Administração estiver armazenado em outro dispositivo e a conta do Servidor de Administração não tiver acesso ao servidor do banco de dados, você deve usar o modo de autenticação do SQL Server instalando ou atualizando o Servidor de Administração. Isso pode ocorrer quando o dispositivo que armazena os bancos de dados estiver fora do domínio ou quando o Servidor de Administração estiver instalado sob uma conta do LocalSystem.

Para MySQL, MariaDB, PostgreSQL ou Postgres Pro, especifique a conta e a senha.

Etapa 13. Selecionar a conta para iniciar o Servidor de Administração

Selecione a conta que será usada para iniciar o Servidor de Administração como um serviço:

- **Gerar a conta automaticamente**. O aplicativo cria uma conta denominada KL-AK-*, sob a qual o serviço kladminserver será executado.

  Você pode selecionar esta opção se planeja localizar a pasta compartilhada e o DBMS no mesmo dispositivo como o Servidor de Administração.

- **Selecione uma conta**. O serviço do Servidor de Administração (kladminserver) será executado sob a conta que você selecionou.

  Você terá que selecionar uma conta de domínio se, por exemplo, planeja usar o DBMS como uma instância do SQL Server de qualquer versão, incluindo o SQL Express, que esteja localizado em outro dispositivo, e/ou se estiver planejando localizar a pasta compartilhada em outro dispositivo.

  O Kaspersky Security Center dá suporte a contas de serviço gerenciadas (MSA) e contas de serviço gerenciadas em grupo (gMSA). Se esses tipos de contas forem usados no seu domínio, é possível selecionar um deles como a conta para o serviço do Servidor de Administração.

  Antes de especificar a MSA ou gMSA, é necessário instalar a conta no mesmo dispositivo em que deseja instalar o Servidor de Administração. Se a conta ainda não estiver instalada, cancele a instalação do Servidor de Administração, instale a conta e reinicie a instalação do Servidor de Administração. Para detalhes sobre a instalação de contas de serviço gerenciadas em um dispositivo local, consulte a documentação oficial da Microsoft.

  Para especificar a MSA ou gMSA:

  1. Clique no botão **Procurar**.
  2. Na janela que se abre, clique no botão **Tipo de objeto**.
  3. Selecionar o tipo **Conta para serviços** e clique em **OK**.
  4. Selecione a conta relevante e clique em **OK**.

A conta que você selecionou deve ter permissões diferentes, dependendo do DBMS que planeja usar.

Para motivos de segurança, não atribua o status privilegiado à conta sob a qual você executa o Servidor de Administração.

A conta do Servidor de Administração não poderá ser alterada posteriormente. É preciso reinstalar o cluster de failover para usar outra conta do Servidor de Administração.

Etapa 14. Selecionar a conta para a execução dos serviços do Kaspersky Security Center

Selecione a conta sob a qual os serviços do Kaspersky Security Center serão executados neste dispositivo:

- **Gerar a conta automaticamente**. O Kaspersky Security Center cria uma conta local denominada KlScSvc neste dispositivo no grupo kladmins. Os serviços do Kaspersky Security Center serão executados sob a conta que foi criada.

- **Selecione uma conta**. Os serviços do Kaspersky Security Center serão executados sob a conta que você selecionou.

  Você terá de selecionar uma conta de domínio se, por exemplo, pretende salvar relatórios em uma pasta localizada em um dispositivo diferente ou se isto for necessário pela política de segurança da sua organização. Também deverá selecionar uma conta de domínio se você instalar o Servidor de Administração em um cluster de correção da falha.

Para motivos de segurança, não conceda o status privilegiado à conta soba a qual os serviços são executados.

O serviço de proxy da KSN (ksnproxy), o serviço do servidor proxy de ativação da Kaspersky (klactprx) e o serviço do portal de autenticação da Kaspersky (klwebsrv) serão executados sob a conta selecionada.

Etapa 15. Seleção de uma pasta compartilhada

Defina a localização e o nome da pasta compartilhada que será usada para realizar as seguintes ações:

- Armazene os arquivos necessários para a instalação remota dos aplicativos (os arquivos serão copiados para o Servidor de Administração durante a criação dos pacotes de instalação).

- Armazenar atualizações que foram baixadas de uma fonte de atualização para o Servidor de Administração.

O compartilhamento de arquivos (somente leitura) será ativado para todos os usuários.

Você pode selecionar uma das seguintes opções:

- **Criar pasta compartilhada**. Criação de uma nova pasta. Na caixa de texto, especifique o caminho para a pasta.

- **Selecionar uma pasta compartilhada existente**. Selecione uma pasta compartilhada que já existe.

A pasta compartilhada pode ser uma pasta local no dispositivo que é usado para a instalação ou em diretório remoto em qualquer dispositivo cliente na rede corporativa. Você pode usar o botão **Procurar** para selecionar a pasta compartilhada ou especificá-la manualmente ao inserir seu caminho UNC (por exemplo, \\server\Share) no campo correspondente.

Por padrão, o instalador cria uma subpasta KLSHARE local na pasta do programa contendo os componentes do Kaspersky Security Center.

É possível definir uma pasta compartilhada posteriormente, caso seja necessário.

Etapa 16. Configuração de conexão ao Servidor de Administração

Configurar a conexão ao Servidor de Administração:

- **Porta**

  O número da porta usada para conectar ao Servidor de Administração.

  O número da porta padrão é 14000.

- **Porta SSL**

  Número da porta SSL (Secure Sockets Layer) usada para conectar em segurança ao Servidor de Administração, através do SSL.

  O número da porta padrão é 13000.

- **Comprimento da chave de criptografia**

  Selecione o comprimento da chave de criptografia: 1024 bits ou 2048 bits.

  Uma chave de criptografia de 1024 bits coloca uma carga menor na CPU, mas se considera ser obsoleta porque ela não pode fornecer uma criptografia confiável devido às suas especificações técnicas. Também, o hardware existente provavelmente resultará ser incompatível com certificados SSL que tenham chaves de 1024 bits.

  Uma chave de criptografia de 2048 bits atende todos os padrões de criptografia estado da arte. No entanto, o uso de uma chave de criptografia de 2048 bits pode adicionar à carga em uma CPU.

  Por padrão, **2048 bits (melhor segurança)** é selecionado.

Você também pode alterar os parâmetros para conectar-se ao Servidor de Administração posteriormente da seguinte forma:

- É possível alterar os números da porta e da porta SSL na seção **Portas de conexão** das propriedades do Servidor de Administração. Para obter mais informações sobre as portas de conexão do Servidor de Administração, consulte Portas usadas pelo Kaspersky Security Center.

- Você pode alterar o comprimento da chave de criptografia ao substituir o certificado do Servidor de Administração pelo utilitário klsetsrvcert usando o parâmetro `-o RsaKeyLen:<comprimento da chave>`.

Etapa 17. Definição do endereço do Servidor de Administração

Definição do endereço do Servidor de Administração. Você pode selecionar uma das seguintes opções:

- **Nome do domínio DNS**. É possível usar o método se a rede incluir um servidor DNS e se os dispositivos cliente puderem usá-lo para receber o endereço do Servidor de Administração.
- **Nome NetBIOS**. É possível usar o método se os dispositivos cliente receberem o endereço do Servidor de Administração por meio do protocolo NetBIOS ou houver um servidor WINS disponível na rede.
- **Endereço IP**. É possível usar o método se o Servidor de Administração possuir um endereço IP estático que não será mudado no futuro.

Etapa 18. Endereço do Servidor de Administração para conexão de dispositivos móveis

Essa etapa do Assistente de Instalação está disponível se você selecionar o Gerenciamento de Dispositivos Móveis para instalação.

Na janela **Endereço para conexão de dispositivos móveis**, especifique o endereço externo do Servidor de Administração para a conexão de dispositivos móveis que estão fora da rede local. É possível especificar o endereço IP ou o Domain Name System (DNS) do Servidor de Administração.

Etapa 19. Descompactação e instalação dos arquivos no disco rígido

Após a instalação dos componentes do Kaspersky Security Center, você pode iniciar a instalação dos arquivos no disco rígido.

Se a instalação requerer programas adicionais, o Assistente de instalação vai notificá-lo, na página **Pré-requisitos de instalação**, antes de iniciar a instalação do Kaspersky Security Center. Os programas requeridos serão instalados automaticamente após você clicar no botão **Avançar**.

Na última página, você pode selecionar qual console iniciar para uso com o Kaspersky Security Center:

- **Iniciar Console de Administração baseado em MMC**
- **Iniciar o Kaspersky Security Center Web Console**

  Esta opção estará disponível somente se você tiver optado por instalar o Kaspersky Security Center Web Console em uma das etapas anteriores.

Você também pode clicar em **Concluir** para fechar o assistente sem iniciar o trabalho com o Kaspersky Security Center. Você pode iniciar o trabalho depois, a qualquer momento.

No momento da primeira inicialização do Console de Administração ou Kaspersky Security Center Web Console, você poderá executar a configuração inicial do aplicativo.

Instalar o Servidor de Administração no modo silencioso

O Servidor de Administração pode ser instalado em modo silencioso, ou seja, sem a inserção interativa das configurações de instalação.

Para instalar o Servidor de Administração em um dispositivo local no modo silencioso:

1. Leia o Contrato de Licença do Usuário Final. Use o comando abaixo somente entende e aceita os termos do Contrato de Licença do Usuário Final.

2. Leia a Política de Privacidade. Use o comando abaixo somente se você entende e concorda que seus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade.

3. Execute o comando
   `setup.exe /s /v"DONT_USE_ANSWER_FILE=1 EULA=1 PRIVACYPOLICY=1 <setup_parameters>"`

onde `setup_parameters` corresponde a uma lista de parâmetros e seus valores respetivos separados por vírgulas (`PARAM1=PARAM1VAL PARAM2=PARAM2VAL`). O arquivo setup.exe está localizado na pasta Servidor, que faz parte do kit de distribuição do Kaspersky Security Center.

Os nomes e valores possíveis para parâmetros que podem ser usados quando Servidor de Administração é instalado no modo silencioso são listados na tabela abaixo.

Parâmetros da instalação do Servidor de Administração no modo silencioso

Nome do parâmetro	Descrição do parâmetro	Valores disponíveis
EULA	Aceitação dos termos do Contrato de Licença.	• 1 – Eu li, entendo e aceito por completo os termos do Contrato de Licença do Usuário Final. • Outro valor ou nenhum valor – Não aceito os termos do Contrato de Licença (a instalação não é executada).
PRIVACYPOLICY	Aceitação dos termos da Política de Privacidade.	• 1 – Estou ciente e concordo que meus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade. Confirmo que Eu li e entendo por completo a Política de Privacidade. • Outro valor ou nenhum valor – Não aceito os termos da Política de Privacidade (a instalação não é executada).
INSTALLATIONMODETYPE	Tipo de instalação do Servidor de Administração.	• Padrão – Instalação padrão. • Personalizada – Instalação personalizada.
INSTALLDIR	Caminho para a pasta de instalação do Servidor de Administração.	Valor da sequência de caracteres.
ADDLOCAL	Lista de componentes do Servidor de Administração (separados por vírgulas) a instalar.	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Lista mínima de componentes suficientes para a instalação correta do Servidor de Administração: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86.`

Nome do parâmetro	Descrição do parâmetro	Valores disponíveis
NETRANGETYPE	Tamanho da rede (número de dispositivos na rede).	• NRT_1_100 – De 1 a 100 dispositivos. • NRT_100_1000 – De 101 a 1000 dispositivos. • NRT_GREATER_1000 – Mais de 1000 dispositivos.
SRV_ACCOUNT_TYPE	Modo de especificar uma conta em que o Servidor de Administração será executado como um serviço.	• SrvAccountDefault – A conta é criada automaticamente. • SrvAccountUser – A conta é especificada manualmente. Neste caso, é necessário especificar valores para os parâmetros `SERVERACCOUNTNAME` e `SERVERACCOUNTPWD`.
SERVERACCOUNTNAME	Nome da conta em que o Servidor de Administração será executado como um serviço. Você deve especificar um valor para o parâmetro se SRV_ACCOUNT_TYPE=SrvAccountUser.	Valor da sequência de caracteres.
SERVERACCOUNTPWD	Senha da conta que será usada para iniciar o Servidor de Administração como um serviço. Você deve especificar um valor para o parâmetro se SRV_ACCOUNT_TYPE=SrvAccountUser.	Valor da sequência de caracteres.
SERVERCER	Tamanho da chave para o certificado do Servidor de Administração (bits).	• 1 – O tamanho da chave para o certificado do Servidor de Administração é de 2048 bits. • Nenhum valor – O tamanho da chave para o certificado do Servidor de Administração é de 1024 bits.
DBTYPE	O tipo de um banco de dados que será usado para armazenar o banco de dados do Servidor de Administração. Este parâmetro é obrigatório.	• MySQL – Um banco de dados MySQL ou MariaDB será usado. Neste caso, é necessário especificar valores para os parâmetros `MYSQLSERVERNAME`, `MYSQLSERVERPORT`, `MYSQLDBNAME`, `MYSQLACCOUNTNAME` e `MYSQLACCOUNTPWD`. • MSSQL – Um banco de dados do Microsoft SQL Server (SQL Express) será usado. Neste caso, é necessário especificar valores para os parâmetros `MSSQLSERVERNAME`, `MSSQLDBNAME` e `MSSQLAUTHTYPE`. • POSTGRES – Um banco de dados PostgreSQL ou Postgres Pro será usado. Neste caso, é necessário especificar valores para os parâmetros `POSTGRESSERVERNAME`, `POSTGRESSERVERPORT`, `POSTGRESDBNAME`, `POSTGRESACCOUNTNAME` e `POSTGRESACCOUNTPWD`.
MYSQLSERVERNAME	Nome completo do SQL Server. Você deve especificar um valor para o parâmetro se DBTYPE=MySQL.	Valor da sequência de caracteres.
MYSQLSERVERPORT	Número da porta para conectar-se ao SQL Server. Você deve especificar um valor para o parâmetro se DBTYPE=MySQL.	Valor numérico.
MYSQLDBNAME	O nome de um banco de dados que será criado para armazenar os dados do Servidor de Administração. Você deve especificar um valor para o parâmetro se DBTYPE=MySQL.	Valor da sequência de caracteres.
MYSQLACCOUNTNAME	Nome da conta para conectar-se ao banco de dados. Você deve especificar um valor para o parâmetro se DBTYPE=MySQL.	Valor da sequência de caracteres.
MYSQLACCOUNTPWD	Senha da conta para conectar-se ao banco de dados. Você deve especificar um valor para o parâmetro se DBTYPE=MySQL.	Valor da sequência de caracteres.
MSSQLSERVERNAME	Nome completo do SQL Server. Você deve especificar um valor para o parâmetro se DBTYPE=MSSQL.	Valor da sequência de caracteres.
MSSQLDBNAME	Nome do banco de dados. Você deve especificar um valor para o parâmetro se DBTYPE=MSSQL.	Valor da sequência de caracteres.

Nome do parâmetro	Descrição do parâmetro	Valores disponíveis
MSSQLAUTHTYPE	Tipo de autorização ao conectar-se ao SQL Server. Você deve especificar um valor para o parâmetro se DBTYPE=MSSQL.	• Windows – Modo de Autenticação do Microsoft Windows. • SQLServer – Modo de Autenticação do SQL Server. Neste caso, é necessário especificar valores para os parâmetros `MSSQLACCOUNTNAME` e `MSSQLACCOUNTPWD`.
MSSQLACCOUNTNAME	Nome da conta para conexão ao SQL Server. Você deve especificar um valor para o parâmetro se MSSQLAUTHTYPE=SQLServer.	Valor da sequência de caracteres.
MSSQLACCOUNTPWD	Senha da conta para conexão ao SQL Server. Você deve especificar um valor para o parâmetro se MSSQLAUTHTYPE=SQLServer.	Valor da sequência de caracteres.
CREATE_SHARE_TYPE	Método para especificar a pasta compartilhada.	• Create – Criar uma nova pasta compartilhada. Neste caso, é necessário especificar valores para os parâmetros `SHARELOCALPATH` e `SHAREFOLDERNAME`. • ChooseExisting – Selecione uma pasta existente. Neste caso, é necessário especificar um valor para o parâmetro `EXISTSHAREFOLDERNAME`.
SHARELOCALPATH	Caminho completo a uma pasta local. Você deve especificar um valor para o parâmetro se CREATE_SHARE_TYPE=Create	Valor da sequência de caracteres.
SHAREFOLDERNAME	Nome da rede de uma pasta compartilhada. Você deve especificar um valor para o parâmetro se CREATE_SHARE_TYPE=Create.	Valor da sequência de caracteres.
EXISTSHAREFOLDERNAME	Caminho completo para uma pasta compartilhada existente. Você deve especificar um valor para o parâmetro se CREATE_SHARE_TYPE=ChooseExisting.	Valor da sequência de caracteres.
SERVERPORT	O número da porta usado para conectar ao Servidor de Administração.	Valor numérico.
SERVERSSLPORT	Número da porta para a conexão criptografada ao Servidor de Administração usando protocolo SSL.	Valor numérico.
SERVERADDRESS	Endereço do Servidor de Administração.	Valor da sequência de caracteres.
MOBILESERVERADDRESS	Endereço do Servidor de Administração para conexão de dispositivos móveis.	Valor da sequência de caracteres.

Para obter uma descrição detalhada dos parâmetros de configuração do Servidor de Administração, consulte a seção Instalação personalizada.

Instalação do Console de Administração na estação de trabalho do administrador

Você pode instalar o Console de Administração na estação de trabalho do administrador em separado e gerenciar o Servidor de Administração através da rede usando esse Console.

Para instalar o Console de Administração na estação de trabalho do administrador:

1. Executar o arquivo executável setup.exe.

   Uma janela é exibida, solicitando que você selecione os aplicativos Kaspersky para instalar.

2. Na janela de seleção do aplicativo, clique no link **Instalar somente o Console de Administração do Kaspersky Security Center** para executar o assistente de instalação do Console de Administração. Siga as instruções do Assistente.

3. Selecione uma pasta de destino. Por padrão, será <Disco>:\Program Files\Kaspersky Lab\Kaspersky Security Center Console. Se essa pasta não existir, ela é criada automaticamente durante a instalação. Você pode alterar a pasta de destino usando o botão **Procurar**.

4. Na última página do Assistente de Instalação, clique no botão **Iniciar** para iniciar a instalação do Console de Administração.

Quando o assistente concluir suas operações, o Console de Administração será instalado na estação de trabalho do administrador.

Para instalar o Console de Administração em uma estação de trabalho do administrador no modo silencioso:

1. Leia o Contrato de Licença do Usuário Final. Use o comando abaixo somente entende e aceita os termos do Contrato de Licença do Usuário Final.

2. Na pasta `Distrib\Console` do kit de distribuição do Kaspersky Security Center, execute o arquivo setup.exe usando o seguinte comando:

   ```
   setup.exe /s /v"EULA=1"
   ```

   Caso deseje instalar todos os plugins de gerenciamento da pasta `Distrib\Console\Plugins` junto com o Console de Administração, execute o seguinte comando:

   ```
   setup.exe /s /v"EULA=1" /pALL
   ```

   Caso deseje especificar quais plugins de gerenciamento instalar da pasta `Distrib\Console\Plugins` junto com o Console de Administração, especifique os plugins após a tecla "/p" e separe-os com um ponto e vírgula:

   ```
   setup.exe /s /v"EULA=1" /pP1;P2;P3
   ```

   onde `P1`, `P2` e `P3` são nomes de plugins que correspondem aos nomes da pasta de plugins, na pasta `Distrib\Console\Plugins`. Por exemplo:

   ```
   setup.exe /s /v"EULA=1" /pKES4Mac;KESS;MDM4IOS
   ```

O Console de Administração e os plugins de gerenciamento (caso houver) serão instalados na estação de trabalho do administrador.

Após instalar o Console de Administração, você deve conectar ao Servidor de Administração. Para fazer isso, execute o Console de Administração e, na janela que for aberta, especifique o nome ou o endereço IP do dispositivo no qual o Servidor de Administração está instalado, assim como as configurações da conta de usuário para a conexão. Após estabelecer conexão ao Servidor de Administração, você pode gerenciar o sistema de proteção antivírus usando esse Console de Administração.

Você pode remover o Console de Administração com as ferramentas padrão de adicionar / remover do Microsoft Windows.

Alterações no sistema após a instalação do Kaspersky Security Center

Ícone Console de Administração

Após o Console de Administração ter sido instalado em seu dispositivo, seu ícone é exibido e pode ser usado para iniciar o Console de Administração. O Console de Administração encontra-se no menu **Iniciar** → **Programas** → **Kaspersky Security Center**.

Serviços do Servidor de Administração e Agente de Rede

O Servidor de Administração e o Agente de Rede serão instalados no dispositivo como serviços com as propriedades listadas abaixo. A tabela contém também os atributos de outros serviços que se aplicam ao dispositivo após a instalação do Servidor de Administração.

Propriedades dos serviços do Kaspersky Security Center

Componente	Nome do serviço	Nome do serviço exibido	Conta
Servidor de Administração	kladminserver	Servidor de Administração do Kaspersky Security Center	A conta não-privilegiada definida pelo usuário ou dedicada no formato KL-AK-* criada durante a instalação
Agente de Rede	klnagent	Agente de Rede do Kaspersky Security Center	Sistema local
Servidor da Web para acessar o Kaspersky Security Center Web Console e administrar a intranet da organização	klwebsrv	Servidor da Web da Kaspersky	Conta dedicada KlScSvc sem privilégios
Servidor proxy de ativação	klactprx	Servidor proxy de ativação da Kaspersky	Conta dedicada KlScSvc sem privilégios
Servidor Proxy da KSN	ksnproxy	Servidor proxy do Kaspersky Security Network	Conta dedicada KlScSvc sem privilégios

Caso instale o Kaspersky Security Center nos nós do cluster de failover da Kaspersky Security Center, o serviço klfocsvc_klfoc ficará disponível. Os serviços klnagent_klfoc e klfocsvc_klfoc são executados na conta do sistema local. O serviço kladminserver_klfoc deve ser executado na conta 'ksc' e outros serviços executados na conta 'rightless'. As contas 'ksc' e 'rightless' devem ser adicionadas ao grupo KLAdmins com as permissões do administrador local. Para o funcionamento correto do Kaspersky Security Center, será necessário usar somente as contas 'ksc' e 'rightless' para executar serviços. Não recomendamos usar outras contas com os mesmos direitos. A tabela abaixo contém as propriedades dos serviços aplicados no dispositivo depois que o Servidor de Administração é instalado no cluster de failover da Kaspersky Security Center.

Propriedades dos serviços do Kaspersky Security Center instalados no cluster de failover da Kaspersky Security Center

Componente	Nome do serviço	Nome do serviço exibido	Conta
Servidor de Administração	kladminserver_klfoc	Servidor de Administração do Kaspersky Security Center	ksc
Agente de Rede	klnagent_klfoc	Agente de Rede do Kaspersky Security Center	Sistema local
Servidor da Web para acessar o Kaspersky Security Center Web Console e administrar a intranet da organização	klwebsrv_klfoc	Servidor da Web da Kaspersky	rightless
Servidor proxy de ativação	klactprx_klfoc	Servidor proxy de ativação da Kaspersky	rightless

Servidor Proxy da KSN	ksnproxy_klfoc	Servidor proxy do Kaspersky Security Network	rightless
Cluster de failover do Kaspersky Security Center	klfocsvc_klfoc	Cluster de failover do Kaspersky Security Center	Sistema local

Serviços do Kaspersky Security Center Web Console

Se você instalar o Kaspersky Security Center Web Console no dispositivo, os seguintes serviços serão implementados (consulte a tabela abaixo):

Serviços do Kaspersky Security Center Web Console

Nome do serviço exibido	Conta
Kaspersky Security Center Service Web Console	NT Service/KSCSvcWebConsole
Kaspersky Security Center Web Console	Serviço de rede
Servidor de plugins de produto do Kaspersky Security Center	NT Service/KSCWebConsolePlugin
Serviço de gerenciamento do Kaspersky Security Center Web Console	Sistema local
Fila de mensagens do Kaspersky Security Center Web Console	NT Service/KSCWebConsoleMessageQueue

Versão do servidor do Agente de Rede

A versão do servidor do Agente de Rede será instalada no dispositivo junto com o Servidor de Administração. A versão de servidor do Agente de Rede é parte do Servidor de Administração, é instalado e removido em conjunto com o Servidor de Administração e pode somente interagir com um Servidor de Administração instalado localmente. Você não tem que configurar a conexão do Agente de Rede ao Servidor de Administração: a configuração é implementada através dos recursos do programa pois os componentes estão instalados no mesmo dispositivo. A versão de servidor do Agente de Rede é instalada com as mesmas propriedades do Agente de Rede padrão e executa as mesmas funções de gerenciamento de aplicativos. Esta versão será gerenciada pela política do grupo de administração ao qual o dispositivo cliente do Servidor de Administração pertence. Para a versão de servidor do Agente de Rede todas as tarefas são criadas a partir do escopo das tarefas fornecidas para o Servidor de Administração, exceto para a tarefa de alteração de servidor.

O Agente de Rede não pode ser instalado separadamente em um dispositivo que já tenha o Servidor de Administração instalado.

Você pode visualizar as propriedades de cada serviço do Servidor de Administração, Agente de Rede, assim como monitorar sua operação usando as ferramentas de gerenciamento padrão do Microsoft Windows: Gerenciamento do computador\Serviços. As informações sobre a atividade do serviço do Servidor de Administração da Kaspersky são armazenadas no registro de sistema do Microsoft Windows em uma ramificação separada do Log de Eventos Kaspersky no dispositivo onde o Servidor de Administração estiver instalado.

Recomendamos que você evite iniciar e parar os serviços manualmente e deixar as contas de serviço nas configurações do serviço inalteradas. Se necessário, você pode modificar a conta do serviço do Servidor de Administração usando o utilitário klsrvswch. Observe que é necessário iniciar o utilitário klsrvswch no dispositivo do Servidor de Administração com a conta com direitos administrativos que foi usada para instalar o Servidor de Administração.

Contas de usuário e grupos de segurança

O Instalador do Servidor de Administração cria as seguintes contas por padrão:

- KL-AK-*: Conta do serviço do Servidor de Administração
- KlScSvc: Contas para outros serviços do grupo de Servidores de Administração
- KlPxeUser: Conta para a implementação de sistemas operacionais

Se você selecionou outras contas para o serviço do Servidor de Administração e para outros serviços ao executar o Instalador, as contas especificadas serão usadas.

Grupos de usuários locais denominados KLAdmins e KLOperators com seus respectivos conjuntos de direitos também serão criados automaticamente no dispositivo onde o Servidor de Administração estiver instalado.

Não é recomendável instalar o Servidor de Administração em um controlador de domínio; no entanto, ao instalar o Servidor de Administração no controlador do domínio, será necessário iniciar o instalador com os direitos do administrador do domínio. Neste caso, o instalador automaticamente cria grupos de segurança de domínio denominados KLAdmins e KLOperators. Se você instalar o Servidor de Administração em um dispositivo que não seja o controlador do domínio, deverá iniciar o instalador com os direitos do administrador local. Neste caso, o instalador automaticamente cria grupos de segurança locais denominados KLAdmins e KLOperators.

Ao configurar as notificações de e-mail, você poderá ter de criar uma conta no servidor de correio para autenticação ESMTP.

Removendo o aplicativo

Você pode remover o Kaspersky Security Center com as ferramentas padrão de adicionar / remover do Microsoft Windows. A remoção do aplicativo requer iniciar um Assistente que remove todos os componentes de aplicativo do dispositivo (incluindo plugins). O Assistente faz com que seu navegador padrão abra uma página da web com uma enquete onde você pode nos dizer por que optou por interromper o uso do Kaspersky Security Center. Se você não tiver selecionado a remoção da pasta compartilhada (KLSHARE) durante a operação do Assistente, você pode executar sua exclusão manual depois da conclusão de todas as tarefas relacionadas.

Após o aplicativo ter sido removido, alguns de seus arquivos podem permanecer na pasta temporária do sistema.

O Assistente de criação da tarefa de remoção de aplicativos vai sugerir que você armazene uma cópia backup do Servidor de Administração.

Durante a remoção do aplicativo no Microsoft Windows 7 e Microsoft Windows 2008, o término prematuro do Assistente de criação da tarefa de remoção de aplicativos pode ocorrer. Isso pode ser evitado ao desativar o Controle da Conta de Usuário (UAC, User Account Control) no sistema operacional e reiniciar a remoção de aplicativo.

Sobre atualizar o Kaspersky Security Center

Esta seção contém informações sobre como atualizar uma versão anterior do Kaspersky Security Center. É possível atualizar o Kaspersky Security Center de diferentes maneiras, dependendo se o Kaspersky Security Center está instalado localmente ou em nós do cluster de failover do Kaspersky Security Center.

Durante a atualização, o uso simultâneo do DBMS pelo Servidor de Administração e outro aplicativo é estritamente proibido.

Ao atualizar o Kaspersky Security Center de uma versão anterior, todos os plugins instalados dos aplicativos compatíveis são mantidos. O plugin do Servidor de Administração e o plugin do Agente de Rede recebe upgrade automaticamente (o Console de Administração e o Kaspersky Security Center Web Console).

Cenário: atualização do Kaspersky Security Center e de aplicativos de segurança gerenciados

Esta seção descreve o breve cenário principal de upgrade do Kaspersky Security Center e dos aplicativos de segurança gerenciados.

A atualização do Kaspersky Security Center e dos aplicativos de segurança gerenciados prossegue em estágios:

1. **Verificando os requisitos de hardware e software**

   Verifique e confirme se seu hardware atende aos requisitos e instale as atualizações necessárias.

2. **Planejar os recursos**

   Avalie quanto do disco o seu banco de dados ocupa. Certifique-se de que tenha espaço em disco suficiente para armazenar a cópia backup das configurações do Servidor de Administração e do banco de dados.

3. **Aquisição do arquivo do instalador para o Kaspersky Security Center**

   Adquira o arquivo executável da versão atual do Kaspersky Security Center e salve-o no dispositivo que funcionará como o Servidor de Administração. Leia as Notas de Versão da versão do Kaspersky Security Center que deseja usar.

4. **Criação de uma cópia backup da versão anterior**

   Use o utilitário de backup e recuperação de dados para criar uma cópia backup dos dados do Servidor de Administração. Também é possível criar uma tarefa de backup.

   Recomenda-se exportar a lista de plug-ins instalados.

5. **Execução do instalador**

   Execute o arquivo executável da versão mais recente do Kaspersky Security Center. Ao executar o arquivo, especifique que você tem uma cópia backup e especifique o local dela. Os dados serão restaurados do backup.

6. **Atualizar os aplicativos gerenciados**

Você poderá fazer o upgrade do aplicativo se houver uma versão mais recente disponível. Ler a lista de aplicativos Kaspersky suportados e certifique-se de que a sua versão do Kaspersky Security Center seja compatível com este aplicativo. Em seguida, execute o upgrade do aplicativo como descrito em suas notas de versão.

Resultados

Após a conclusão do cenário de atualização, assegure-se de que a nova versão do Servidor de Administração esteja instalada com êxito no Console de Gerenciamento da Microsoft. Clique em **Ajuda** → **Sobre o Kaspersky Security Center**. A versão é exibida.

Para garantir o uso da versão mais recente do Servidor de Administração no Kaspersky Security Center Web Console clique no ícone Configurações (), no topo da tela, ao lado do nome do Servidor de Administração. Na janela de propriedades do Servidor de Administração que se abre, na guia **Geral**, selecione a seção **Geral**. A versão é exibida.

Caso precise recuperar os dados do Servidor de Administração, siga as etapas descritas no tópico a seguir: backup e recuperação de dados no modo interativo.

Se você tiver atualizado um aplicativo de segurança gerenciado, assegure-se de que ele esteja corretamente instalado nos dispositivos gerenciados. Para obter mais informações, consulte a documentação deste aplicativo.

Atualização do Kaspersky Security Center a partir de uma versão anterior

O tópico a seguir descreve as etapas de preparação recomendadas para a atualização: atualização do Kaspersky Security Center e dos aplicativos de segurança gerenciados.

É possível instalar a verão 14.2 do Servidor de Administração em um dispositivo que tenha uma versão anterior do Servidor de Administração instalada (a partir da versão 11 (11.0.0.1131b)). Ao atualizar para a versão 14.2, todos os dados e configurações da versão anterior do Servidor de Administração são salvos.

Se problemas ocorrerem durante a instalação do Servidor de Administração, você pode restaurar a versão anterior do Servidor de Administração usando a cópia backup de dados do Servidor de Administração criados antes da atualização.

Se ao menos um Servidor de Administração da nova versão for instalado na rede, você pode fazer o upgrade de outros Servidores de Administração na rede usando a tarefa de instalação remota que usa o pacote de instalação do Servidor de Administração.

Caso tenha implantado o cluster de failover do Kaspersky Security Center, também é possível atualizar o Kaspersky Security Center em seus nós.

Para atualizar para uma versão anterior do Servidor de Administração para a versão 14.2:

1. Execute o arquivo de instalação ksc_14.2_<número da compilação>_full_<idioma>.exe da versão 14.2 (baixe o arquivo do site da Kaspersky).

2. Na janela que se abre, clique no link **Instalar o Kaspersky Security Center 14.2** para iniciar o Assistente de instalação do Servidor de Administração. Siga as instruções do Assistente.

3. Leia o Contrato de Licença e a Política de Privacidade. Se você concordar com todos os termos do Contrato de Licença e da Política de Privacidade, selecione as seguintes caixas de seleção na seção **Eu confirmo que li, entendi e aceito todo o seguinte**:

   - **Os termos e condições deste EULA**
   - **Política de Privacidade que descreve o manuseio de dados**

   A Instalação do aplicativo no seu dispositivo continuará após você selecionar ambas as caixas de seleção. O Assistente de instalação solicita a criação de um backup dos dados do Servidor de Administração para a versão anterior.

   O Kaspersky Security Center suporta a recuperação dos dados a partir de um backup criado com uma versão anterior do Servidor de Administração.

4. Se você deseja criar um backup dos dados do Servidor de Administração, especifique isso na janela **Backup do Servidor de Administração** que se abre.

   Um backup é criado pelo utilitário klbackup. Este utilitário está incluído no kit de distribuição e está localizado na raiz da pasta de instalação do Kaspersky Security Center.

5. Instale o Servidor de Administração versão 14.2, de acordo com o Assistente de instalação.

   Se for exibida uma mensagem de que o Kaspersky Security Center Web Console está ocupado, clique no botão **Ignorar** na janela do assistente.

   > Recomendamos que você evite cancelar a operação do Assistente de instalação. Se você cancelar a atualização na etapa da instalação do Servidor de Administração, isso pode causar a falha da versão atualizada do Kaspersky Security Center.

6. Para dispositivos nos quais uma versão anterior do Agente de Rede estiver instalada, crie e execute a tarefa para instalação remota da nova versão do Agente de Rede.

   > Recomendamos atualizar o Agente de Rede para Linux para a mesma versão do Kaspersky Security Center.

   Após a conclusão da tarefa de instalação remota, a versão do Agente de Rede será atualizada.

   Execute os seguintes comandos em ativos baseados em Linux para remover dependências que não são mais necessárias:

   - Para ativos baseados em Debian, execute um dos seguintes comandos:
     - `apt-get -y autoremove`
     - `apt -y autoremove`
   - Para ativos baseados em RPM, execute um dos seguintes comandos:
     - `dnf autoremove`
     - `yum autoremove`

Atualização do Kaspersky Security Center a partir de nós do cluster de failover do Kaspersky Security Center

É possível instalar o Servidor de Administração versão 14.2 em cada nó do cluster de failover do Kaspersky Security Center que tenha uma versão anterior do Servidor de Administração instalada (a partir da versão 13.2). Ao atualizar para a versão 14.2, todos os dados e configurações da versão anterior do Servidor de Administração são salvos.

Se o Kaspersky Security Center já tiver sido instalado localmente em alguns dispositivos, também é possível atualizar o Kaspersky Security Center nesses dispositivos.

Para atualizar o Kaspersky Security Center nos nós do cluster de failover do Kaspersky Security Center:

1. Execute as seguintes ações no nó ativo do cluster:

   a. Execute o arquivo executável ksc_14.2_<número da compilação>_full_<idioma>.exe.

   Uma janela é aberta, solicitando que você selecione os aplicativos Kaspersky para atualizar. Clique no link **Instalar o Servidor de Administração do Kaspersky Security Center** para iniciar o Assistente de instalação do Servidor de Administração. Siga as instruções do assistente.

   b. Leia o Contrato de Licença e a Política de Privacidade. Se você concordar com todos os termos do Contrato de Licença e da Política de Privacidade, selecione as seguintes caixas de seleção na seção **Eu confirmo que li, entendi e aceito todo o seguinte**:

   - **Os termos e condições deste EULA**
   - **Política de Privacidade que descreve o manuseio de dados**

   Marque ambas as caixas de seleção para continuar a instalação.

   Se você não aceitar o Contrato de Licença ou a Política de Privacidade, clique no botão **Cancelar** para cancelar a atualização.

2. Execute as mesmas ações no nó passivo do cluster de failover do Kaspersky Security Center que no nó ativo.

3. Iniciar o cluster.

Assim, a versão mais recente do Servidor de Administração nos nós do cluster de failover do Kaspersky Security Center é instalada.

Configuração inicial do Kaspersky Security Center

Esta seção descreve as etapas que você deve seguir depois da instalação do Kaspersky Security Center para executar sua configuração inicial.

Guia de Proteção

O Guia de Proteção é voltado para os profissionais que instalam e administram o Kaspersky Security Center, assim como a todos as pessoas que fornecem suporte técnico para as organizações que usam o Kaspersky Security Center.

O Guia de Proteção descreve as recomendações e recursos de configuração do Kaspersky Security Center e seus componentes com o objetivo de reduzir os riscos de seu comprometimento.

Antes de configurar, crie uma cópia de backup do Servidor de Administração do Kaspersky Security Center com o uso da tarefa Backup de dados do Servidor de Administração ou o utilitário klbackup e salve-a em um local seguro.

O Guia de Proteção inclui as seguintes informações:

- Seleção da arquitetura do Servidor de Administração
- Configuração de uma conexão segura com o Servidor de Administração
- Configuração de contas para acesso ao Servidor de Administração
- Gerenciamento da proteção do Servidor de Administração e dispositivos clientes
- Configuração da proteção para aplicativos gerenciados
- Manutenção do Servidor de Administração
- Transferência de informações para aplicativos de terceiros

Antes de começar a trabalhar com o Servidor de Administração, o Kaspersky Security Center solicita que a versão resumida do Guia de Proteção seja lida.

Observe que não é possível usar o Servidor de Administração até confirmar que o Guia de Proteção foi lido.

Para ler o Guia de Proteção:

1. Abra o Console de Administração ou o Kaspersky Security Center Web Console e faça login no console. O console verifica se a leitura da versão atual do Guia de Proteção foi confirmada.

   Caso ainda não tenha lido o Guia de Proteção, uma janela será aberta e exibirá uma breve versão dele.

2. Execute uma das seguintes ações:

   - Caso queira visualizar a versão resumida do Guia de Proteção como um documento de texto, clique no link **Open in new window**.
   - Caso queira visualizar a versão completa do Guia de proteção, clique no link **Open Hardening guide in Online Help**.

3. Depois de ler o Guia de Proteção, marque a caixa de seleção **I confirm that I have fully read and understand the Hardening guide** e, em seguida, clique no botão **Accept**.

Agora, é possível trabalhar com o Servidor de Administração.

Quando uma nova versão do Guia de Proteção aparecer, o Kaspersky Security Center solicitará a sua leitura.

Assistente de Início Rápido do Servidor de Administração

Esta seção fornece informações sobre o Assistente de início rápido do Servidor de Administração.

Sobre o Assistente de Início Rápido

Esta seção fornece informações sobre o Assistente de início rápido do Servidor de Administração.

O Assistente de início rápido do Servidor de Administração permite criar um mínimo de tarefas e políticas necessárias, ajustar um mínimo de configurações, baixar e instalar plugins para aplicativos gerenciados da Kaspersky e criar pacotes de instalação de aplicativos gerenciados da Kaspersky. Quando o assistente estiver em execução, você pode fazer as seguintes modificações ao aplicativo:

- Faça o download e instale plugins para aplicativos gerenciados. Após a conclusão do Assistente de início rápido, a lista de plugins de gerenciamento instalados é exibida na seção **Avançado → Detalhes dos plug-ins de gerenciamento de aplicativos instalados** da janela Propriedades do Servidor de Administração.

- Criar pacotes de instalação para aplicativos gerenciados da Kaspersky. Após a conclusão do Assistente de início rápido, os pacotes de instalação do Agente de Rede para Windows e dos aplicativos gerenciados da Kaspersky são exibidos na lista **Servidor de Administração → Avançado → Instalação remota → Pacotes de instalação**.

- Adicione arquivos de chaves ou insira códigos de ativação que podem ser distribuídas automaticamente para os dispositivos dentro de grupos de administração. Após a conclusão do Assistente de início rápido, as informações sobre as chaves de licença são exibidas na lista **Servidor de Administração → Licenças** da Kaspersky e na seção **Chaves de licença** da janela Propriedades do Servidor de Administração.

- Configure a interação com a Kaspersky Security Network (KSN).

- Defina entrega de notificações por e-mail sobre os eventos que ocorrem durantes a operação do Servidor de Administração e de aplicativos gerenciados (a entrega com êxito da notificação requer que o serviço Messenger continue a estar em execução no Servidor de Administração e nos dispositivos de todos os destinatários). Após a conclusão do Assistente de início rápido, as configurações de notificações por e-mail são exibidas na seção **Notificação** janela Propriedades do Servidor de Administração.

- Ajuste as configurações de atualização e de correções de vulnerabilidade para os aplicativos instalados nos dispositivos.

- Crie uma política de proteção para estações de trabalho e servidores, assim como tarefas de verificação de malwares, tarefas de download de atualização e tarefas de backup dos dados, para o nível superior da hierarquia de dispositivos gerenciados. Após a conclusão do Assistente de início rápido, as tarefas criadas são exibidas na lista **Servidor de Administração → Tarefas**, as políticas correspondentes aos plugins para aplicativos gerenciados são exibidas na lista **Servidor de Administração → Políticas**.

O Assistente de início rápido cria políticas para aplicativos gerenciados, tal como o Kaspersky Endpoint Security for Windows, a menos que tais políticas sejam criadas para o grupo de **Dispositivos gerenciados**. O Assistente de Início Rápido cria tarefas se tarefas com o mesmo nome não existirem para o grupo de **Dispositivos gerenciados**.

No Console de Administração, o Kaspersky Security Center solicita automaticamente que você execute o Assistente de início rápido após iniciá-lo pela primeira vez. Você também pode iniciar o Assistente de início rápido manualmente a qualquer momento.

Iniciar o Assistente de início rápido do Servidor de Administração

O aplicativo solicita automaticamente que você execute o Assistente de início rápido após a instalação do Servidor de Administração, na primeira conexão a ele. Você também pode iniciar o Assistente de início rápido manualmente a qualquer momento.

Para iniciar o Assistente de Início Rápido manualmente:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No menu de contexto do nó, selecione **Todas as tarefas → Assistente de início rápido do Servidor de Administração**.

   O assistente solicita que você execute a configuração inicial do Servidor de Administração. Siga as instruções do Assistente.

Se você inicializar o Assistente de início rápido novamente, as tarefas e políticas criadas na execução anterior não poderão ser recriadas.

Etapa 1. Configurar um servidor proxy

Especifique as configurações de acesso à Internet para o Servidor de Administração. Você deve configurar o acesso à Internet para usar a Kaspersky Security Network e baixar atualizações de bancos de dados antivírus para o Kaspersky Security Center e aplicativos Kaspersky gerenciados.

Selecione a opção **Usar o servidor proxy** caso queira usar um servidor proxy para se conectar com a Internet. Se essa opção estiver selecionada, os campos estarão disponíveis para inserir configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:

- **Endereço**

  Endereço do servidor proxy usado para conexão do Kaspersky Security Center à Internet.

- **Número da porta**

  Número da porta pela qual a conexão proxy do Kaspersky Security Center será estabelecida.

- **Ignorar servidor proxy para endereços locais**

  Nenhum servidor proxy será usado para conectar-se aos dispositivos na rede local.

- **Autenticação do servidor proxy**

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

  Este campo de entrada está disponível se a caixa de seleção **Usar o servidor proxy** estiver marcada.

- **Nome do usuário**

  Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

- **Senha**

  A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

  Para ver a senha inserida, mantenha pressionado o botão **Exibir** pelo tempo que você desejar.

É possível configurar o acesso à Internet posteriormente, de modo separado, a partir do assistente de início rápido.

Etapa 2. Selecionando o método de ativação do aplicativo

Selecione uma das seguintes opções de ativação do Kaspersky Security Center:

- **Ao inserir o seu código de ativação**

  Código de ativação é uma sequência única de 20 caracteres alfanuméricos. Você insere um código de ativação para adicionar uma chave que ativa o Kaspersky Security Center. Você recebe o código de ativação através do endereço de e-mail especificado após a compra do Kaspersky Security Center.

  Para ativar o aplicativo com um código de ativação, é necessário acesso à Internet para estabelecer a conexão com os servidores de ativação da Kaspersky.

  Caso tenha selecionado essa opção de ativação, é possível ativar a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

  Se esta opção estiver ativada, a chave de licença será implementada automaticamente para os dispositivos gerenciados.

  Se esta opção estiver desativada, você pode implementar a chave de licença para dispositivos gerenciados posteriormente, no nó **Licenças Kaspersky** na árvore do Console de Administração.

  Caso a ativação pela inserção do código de ativação não funcione por qualquer motivo, é possível ativar o aplicativo especificando um arquivo de chave.

- **Especificando um arquivo de chave**

  O *Arquivo de chave* é um arquivo com a extensão .key fornecido a você pela Kaspersky. O objetivo do arquivo de chave é adicionar uma chave que ativa o aplicativo.

  Os métodos de obtenção de arquivos de chave são descritos na seção a seguir: Sobre o arquivo de chave.

  Para ativar o aplicativo usando um arquivo de chave, não é necessário conectar-se aos servidores de ativação da Kaspersky.

  Caso tenha selecionado essa opção de ativação, é possível ativar a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

  Se esta opção estiver ativada, a chave de licença será implementada automaticamente para os dispositivos gerenciados.

  Se esta opção estiver desativada, você pode implementar a chave de licença para dispositivos gerenciados posteriormente, no nó **Licenças Kaspersky** na árvore do Console de Administração.

- **Ao adiar a ativação do aplicativo**

  O aplicativo não funcionará com a funcionalidade básica, sem o Gerenciamento de Dispositivos Móveis e sem o Gerenciamento de patches e vulnerabilidades.

Caso tenha decidido adiar a ativação do aplicativo, será possível adicionar uma chave de licença depois e a qualquer momento.

Etapa 3. Seleção das áreas de proteção e sistemas operacionais

Selecione as áreas de proteção e os sistemas operacionais que estão em uso na sua rede. Ao selecionar essas opções, você especifica os filtros para plugins de gerenciamento de aplicativos e pacotes de distribuição nos servidores da Kaspersky que podem ser baixados para instalação nos dispositivos clientes em sua rede. Selecione as opções:

- **Áreas**

  Você pode selecionar as seguintes áreas de proteção:

  - **Estações de trabalho**. Selecione esta opção se desejar proteger as estações de trabalho na sua rede. Por padrão, a opção Estação de trabalho está selecionada.
  - **Servidores de arquivos e armazenamento**. Selecione esta opção se desejar proteger servidores de arquivos na sua rede.
  - **Dispositivos móveis**. Selecione esta opção se desejar proteger os dispositivos móveis pertencentes à empresa ou aos seus funcionários. Se você selecionar essa opção, mas não tiver fornecido uma licença com o recurso de Gerenciamento de Dispositivos Móveis, será exibida uma mensagem informando sobre a necessidade de fornecer uma licença com o recurso Gerenciamento de Dispositivos Móveis. Se você não fornecer uma licença, não poderá usar o recurso de dispositivo móvel.
  - **Virtualização**. Selecione esta opção se você quiser proteger máquinas virtuais em sua rede.
  - **Kaspersky Anti-Spam**. Selecione esta opção se desejar proteger os servidores de correio da sua organização contra spam, fraude e malware.

- **Sistemas operacionais**

  Você pode selecionar as seguintes plataformas:

  - Microsoft Windows
  - Linux
  - macOS
  - Android
  - Outro

  Para obter informações sobre os sistemas operacionais suportados, consulte os requisitos de hardware e software.

Você pode selecionar os pacotes de aplicativos Kaspersky na lista de pacotes disponíveis posteriormente, separadamente do Assistente de início rápido. Para simplificar a busca pelos pacotes necessários, você pode filtrar a lista de pacotes disponíveis pelos seguintes critérios:

- Área de proteção
- Tipo de software baixado (pacote de distribuição, utilitário, plugin ou plugin da Web)
- Versão do aplicativo Kaspersky
- Idioma de localização do aplicativo Kaspersky

Etapa 4. Selecionar os plugins para os aplicativos gerenciados

Selecione os plugins para os aplicativos gerenciados a ser instalados. Uma lista de plugins localizados nos servidores da Kaspersky é exibida. A lista é filtrada de acordo com as opções selecionadas na etapa anterior do assistente. Por padrão, uma lista completa inclui plugins de todos os idiomas. Para exibir apenas o plugin de idioma específico, selecione o idioma na lista suspensa **Mostrar o idioma localizado do Console de Administração ou**. A lista de plugins inclui as seguintes colunas:

- **Nome do aplicativo**

  Os plugins, dependendo das áreas de proteção e das plataformas que você selecionou na etapa anterior, são selecionados.

- **Versão do aplicativo**

  A lista inclui plugins de todas as versões colocadas nos servidores da Kaspersky. Por padrão, os plugins das versões mais recentes são selecionados.

- **Idioma de localização**

  Por padrão, o idioma de localização de um plugin é definido pelo idioma do Kaspersky Security Center que você selecionou na instalação. Você pode especificar outros idiomas na lista suspensa **Mostrar o idioma localizado do Console de Administração ou**.

Após a seleção dos plugins, sua instalação é iniciada automaticamente em uma janela separada. Para instalar alguns plugins, você deve aceitar os termos do EULA. Leia o texto do EULA, selecione a opção **Eu aceito os termos do Contrato de Licença** e clique no botão **Instalar**. Se você não aceitar os termos do EULA, o plugin não será instalado.

Após a conclusão da instalação, feche a janela de instalação.

Você também pode selecionar os plugins de gerenciamento posteriormente, separadamente do Assistente de início rápido.

Etapa 5. Baixando os pacote de distribuição e criando pacotes de instalação

O Kaspersky Endpoint Security for Windows inclui uma ferramenta de criptografia para as informações armazenadas nos dispositivos cliente. Para baixar um pacote de distribuição do Kaspersky Endpoint Security for Windows válido para as necessidades da sua organização, consulte a legislação do país em que os dispositivos cliente da sua organização estão localizados.

Na janela **Tipo de criptografia**, selecione um dos seguintes tipos de criptografia:

- Criptografia forte (AES256). Esse tipo de criptografia usa o comprimento de chave de 256 bits.
- Criptografia leve (AES56). Esse tipo de criptografia usa o comprimento de chave de 56 bits.

A janela **Tipo de criptografia** é exibida apenas se você tiver selecionado **Estações de trabalho** como escopo da proteção e **Microsoft Windows** como plataforma.

Após selecionar um tipo de criptografia, a lista dos pacotes de distribuição dos dois tipos de criptografia é exibida. Um pacote de distribuição com o tipo de criptografia selecionado está selecionado na lista. O idioma do pacote de distribuição corresponde ao idioma do Kaspersky Security Center. Se não existir um pacote de distribuição do Kaspersky Endpoint Security for Windows para o idioma do Kaspersky Security Center, o pacote de distribuição em inglês será selecionado.

Na lista, você pode selecionar os idiomas dos pacotes de distribuição por meio da lista suspensa **Mostrar o idioma localizado do Console de Administração ou**.

As distribuições de aplicativos gerenciados podem exigir a instalação de uma versão mínima específica do Kaspersky Security Center.

Na lista, você pode selecionar pacotes de distribuição de qualquer tipo de criptografia, diferente daquele que você selecionou na janela **Tipo de criptografia**. Depois de selecionar um pacote de distribuição para o Kaspersky Endpoint Security for Windows, o download dos pacotes de distribuição, correspondentes aos componentes e plataformas, é iniciado. Você pode monitorar o progresso do download na coluna **Status do download**. Após a conclusão do Assistente de início rápido, os pacotes de instalação do Agente de Rede para Windows e dos aplicativos gerenciados da Kaspersky são exibidos na lista **Servidor de Administração → Avançado → Instalação remota → Pacotes de instalação**.

Para concluir o download de alguns pacotes de distribuição, você deve aceitar o EULA. Quando você clica no botão **Aceitar**, o texto do EULA é exibido. Para prosseguir para a próxima etapa do assistente, você deve aceitar os termos e condições do EULA e os termos e condições da Política de Privacidade da Kaspersky. Selecione as caixas de seleção relacionadas ao EULA e à Política de Privacidade da Kaspersky e clique no botão **Aceitar tudo**. Se você não aceitar os termos e condições, o download do pacote será cancelado.

Após aceitar os termos e condições do EULA e os termos e condições da Política de Privacidade da Kaspersky, o download dos pacotes de distribuição continua. Quando o download terminar, o status **O pacote de instalação foi criado** é exibido. Posteriormente, você pode suar os pacotes de instalação para implementar aplicativos Kaspersky em dispositivos cliente.

É possível criar pacotes de instalação manualmente, de modo separado, a partir do assistente de início rápido. Vá para **Servidor de Administração → Avançado → Instalação remota → Pacotes de instalação** na árvore do Console de Administração.

Etapa 6. Configurando o uso da Kaspersky Security Network

É possível obter acesso aos bancos de dados de reputação do Kaspersky Security Network para garantir uma resposta mais rápida dos aplicativos Kaspersky a ameaças, melhorar a efetividade de alguns componentes de proteção e reduzir o risco de falsos positivos.

Leia a Declaração da KSN, que é exibida na janela. Especifique as configurações para encaminhar informações sobre as operações do Kaspersky Security Center à Base de conhecimento da Kaspersky Security Network. Selecione uma das seguintes opções:

- **Concordo em usar a Kaspersky Security Network**

  O Kaspersky Security Center e os aplicativos gerenciados instalados nos dispositivos cliente transferem automaticamente seus detalhes de operação para o Kaspersky Security Network. A participação na Kaspersky Security Network assegura atualizações mais rápidas dos bancos de dados que contêm informações sobre vírus e outras ameaças, que assegura uma resposta mais rápida a ameaças de segurança emergentes.

- **Não concordo em usar a Kaspersky Security Network**

  O Kaspersky Security Center e os aplicativos gerenciados não fornecerão informações ao Kaspersky Security Network.

  Se você selecionar esta opção, o uso da Kaspersky Security Network será desativado.

Se você baixou o plugin do Kaspersky Endpoint Security for Windows, ambas as Declarações da KSN para o Kaspersky Security Center e para o Kaspersky Endpoint Security for Windows serão exibidas. As Declarações da KSN para outros aplicativos Kaspersky gerenciados cujos plugins foram baixados são exibidas em janelas separadas e você deve aceitar (ou recusar) cada uma delas separadamente.

Você também pode configurar o acesso do Servidor de Administração à Kaspersky Security Network (KSN) posteriormente na janela de propriedades do Servidor de Administração do Console de Administração.

Etapa 7. Configurar notificações por e-mail

Configure o envio de notificações sobre os eventos registrados durante a operação dos aplicativos Kaspersky em dispositivos gerenciados. Essas configurações são usadas como padrão para o Servidor de Administração.

Para configurar a entrega de notificações sobre os eventos que ocorrem nos aplicativos Kaspersky, use as seguintes configurações:

- **Destinatários (endereços de e-mail)**

  Os endereços de e-mail de usuários aos quais o aplicativo enviará notificações. Você pode inserir um ou vários endereços; se inserir mais de um endereço, separe-os com um ponto-e-vírgula.

- **Servidores SMTP**

  O endereço ou os endereços dos servidores de e-mail da sua organização.

  Se você inserir mais de um endereço, separe-os com um ponto-e-vírgula. Você pode usar os seguintes parâmetros:

  - Endereço IPv4 ou IPv6
  - Nome da rede Windows (nome NetBIOS) do dispositivo
  - Nome de DNS do servidor SMTP

- **Porta do servidor SMTP**

  Número da porta de comunicação do servidor SMTP. Se você usar vários servidores SMTP, a conexão com eles será estabelecida por meio da porta de comunicação especificada. O número da porta padrão é 25.

- **Usar a autenticação ESMTP**

  Ativa o suporte da autenticação ESMTP. Após selecionar a caixa de seleção, nos campos **Nome do usuário** e **Senha**, você poderá especificar as configurações de autenticação ESMTP. Por padrão, esta caixa de seleção está desmarcada.

- **Configurações**

  Especificar as seguintes configurações:

  - **Assunto** (assunto de uma mensagem de e-mail)
  - **Endereço de e-mail do remetente**
  - **Configurações TLS para servidor SMTP**

  Você pode especificar as configurações TLS para um servidor SMTP:

  Você pode desativar o uso de TLS, usar o TLS se o servidor SMTP for compatível com este protocolo ou pode forçar o uso de TLS apenas. Se optar por usar apenas TLS, especifique um certificado para autenticação do servidor SMTP e escolha se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, se optar por usar apenas TLS, poderá especificar um certificado para autenticação de cliente no servidor SMTP.

  - Procurar por um arquivo de certificado do servidor SMTP:

  Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

  - Procurar um arquivo de certificado de cliente:

  Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer autoridade de certificação confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

  - Certificado X-509:

  Especifique o arquivo com o certificado e o arquivo com a chave privada. Você pode carregar esses arquivos em qualquer ordem. Quando os dois arquivos são carregados, especifique a senha para descriptografar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver criptografada.

  - Contêiner pkcs12:

  Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

Você pode testar as novas configurações de notificação por e-mail clicando no botão **Enviar mensagem de teste**.

Você também pode configurar notificações de eventos posteriormente, de modo separado do Assistente de início rápido.

Etapa 8. Configurar o Gerenciamento de atualizações

Defina as configurações para gerenciar as atualizações de aplicativos instalados em dispositivos cliente.

Você pode definir essas configurações somente se tiver fornecido uma chave de licença com a opção de Gerenciamento de Patches e Vulnerabilidades.

No grupo de configurações **Pesquisar por atualizações e instalá-las**, você pode selecionar um modo de pesquisa e instalação das atualizações do Kaspersky Security Center:

- **Search for required updates**

  A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente, caso você não tenha uma.

  Esta opção está marcada por padrão.

- **Encontrar e instalar as atualizações necessárias**

  As tarefas *Encontrar as vulnerabilidades e as atualizações necessárias* e *Instalar as atualizações necessárias e corrigir vulnerabilidades* são criadas automaticamente, se ainda não existirem.

No grupo de configurações **Serviços de atualização do Windows Server**, você pode selecionar uma fonte de sincronização de atualizações:

- **Use fontes de atualização definidas na política de domínio**

  Os dispositivos clientes baixarão as atualizações do Windows Update, de acordo com as configurações de diretiva de domínio. A política do Agente de Rede é criada automaticamente, se você não tiver uma.

- **Usar Servidor de Administração como servidor WSUS**

  Os dispositivos clientes baixarão as atualizações do Windows Update no Servidor de Administração. A tarefa *Executar a sincronização com o Windows Update* e a política do Agente de Rede são criadas automaticamente, se ainda não existirem.

É possível criar as tarefas *Encontrar vulnerabilidades e atualizações necessárias*, *Instalar as atualizações necessárias e corrigir as vulnerabilidades* separadamente a partir do assistente de início rápido. Para usar o Servidor de Administração como o servidor WSUS, crie a tarefa *Perform Windows Update synchronization* e selecione a opção **Usar Servidor de Administração como servidor WSUS** na política do Agente de Rede.

Etapa 9. Criar uma configuração da proteção inicial

A janela **Configurar a proteção inicial**, exibe uma lista de políticas e tarefas criadas automaticamente. As seguintes políticas e tarefas são criadas:

- Política do Agente de Rede do Kaspersky Security Center
- Políticas para aplicativos gerenciados da Kaspersky cujos plugins de gerenciamento foram instalados anteriormente
- Tarefa Manutenção do Servidor de Administração
- Tarefa Backup de dados do Servidor de Administração
- Tarefa Baixar atualizações no repositório do Servidor de Administração
- Tarefa Encontrar as vulnerabilidades e as atualizações necessárias
- Tarefa Instalar a atualização

Espere pela conclusão da criação de políticas e tarefas antes de prosseguir à etapa seguinte do assistente.

Se você baixou e instalou o plugin do Kaspersky Endpoint Security para Windows 10 Service Pack 1 e posterior até a 11.0.1, durante a criação de políticas e tarefas, uma janela é aberta para a configuração inicial da zona confiável do Kaspersky Endpoint Security for Windows. O aplicativo solicitará a adicionar fornecedores verificados pela Kaspersky na zona confiável com os objetivos de excluir os seus aplicativos de verificações para impedi-los de serem acidentalmente bloqueados. Você pode criar exclusões recomendadas agora ou criar uma lista de exclusões em outro momento selecionando o seguinte na árvore do console: **Políticas** → menu Propriedades do Kaspersky Endpoint Security → **Proteção avançada contra ameaças** → **Zona confiável** → **Configurações** → **Adicionar**. A lista de exclusões da verificação está disponível para edição a qualquer momento ao usar o aplicativo.

> Estas operações na zona confiável são efetuadas usando ferramentas integradas no Kaspersky Endpoint Security for Windows. Para obter instruções detalhadas sobre como efetuar operações e uma descrição da funcionalidade de criptografia, consulte a Ajuda on-line do Kaspersky Endpoint Security for Windows.

Para concluir a configuração inicial da zona de confiança e voltar ao assistente, clique em **OK**.

Clique em **Avançar**. Este botão se torna disponível após todas as políticas e tarefas necessárias tiverem sido criadas.

Você também pode criar as tarefas e as políticas necessárias posteriormente, de modo separado do Assistente de início rápido.

Etapa 10. Conectar dispositivos móveis

Se você tiver selecionado anteriormente o escopo de proteção **Dispositivos Móveis** nas configurações do assistente, especifique as configurações para a conexão dos dispositivos móveis corporativos da organização gerenciada. Se você não ativou o escopo da proteção **Dispositivos Móveis**, esta etapa será ignorada.

Nessa etapa do assistente, proceda da seguinte maneira:

- Configure portas para a conexão de dispositivos móveis
- Configure a autenticação do Servidor de Administração
- Crie ou gerencie certificados
- Configure a emissão, atualização automática e criptografia de certificados de tipo geral
- Crie uma regra de migração para dispositivos móveis

Para definir as portas para a conexão de dispositivos móveis:

1. Clique no botão **Configurar** à direita do campo **Conexão de dispositivo móvel**.
2. Na lista suspensa, selecione **Configurar as portas**.
   Na janela de propriedades do Servidor de Administração que for aberta, exibindo a seção **Portas adicionais**.

3. Na seção **Portas adicionais**, você pode especificar as configurações de conexão de dispositivo móvel:

- **Porta SSL para servidor proxy de ativação**

  O número de uma porta SSL para conexão do Kaspersky Endpoint Security for Windows aos servidores de ativação da Kaspersky.

  O número da porta padrão é 17000.

- **Abrir porta para dispositivos móveis**

  Uma porta é aberta para os dispositivos móveis conectarem-se ao Servidor de Licenciamento. Você pode definir o número da porta e outras configurações nos campos abaixo.

  Por padrão, esta opção está ativada.

- **Porta para sincronização de dispositivos móveis**

  O número da porta através da qual os dispositivos móveis conectam-se ao Servidor de Administração e trocam dados com o mesmo. O número da porta padrão é 13292.

  Você pode atribuir uma porta diferente se a porta 13292 estiver sendo usada para outros propósitos.

- **Porta para ativação de dispositivos móveis**

  A porta para conexão do Kaspersky Endpoint Security for Android para os servidores de ativação da Kaspersky.

  O número da porta padrão é 17100.

- **Abrir porta para os dispositivos de proteção UEFI e dispositivos KasperskyOS**

  Os dispositivos de proteção UEFI poderão ser conectados ao Servidor de Administração.

- **Porta para os dispositivos de proteção UEFI e dispositivos KasperskyOS**

  Você pode alterar o número da porta se a opção **Abrir porta para os dispositivos de proteção UEFI e dispositivos KasperskyOS** estiver ativada. O número da porta padrão é 13294.

- **Abrir porta para Prometheus**

  A porta para solicitações pull do Prometheus. O número da porta padrão é 13296.

4. Clique em **OK** para salvar as alterações e voltar ao Assistente de início rápido.

Você terá que configurar a autenticação do Servidor de Administração por dispositivos móveis e a autenticação de dispositivos móveis pelo Servidor de Administração. Se você desejar, poderá configurar a autenticação mais tarde, separadamente do Assistente de início rápido.

Para configurar a autenticação do Servidor de Administração por dispositivos móveis:

1. Clique no botão **Configurar** à direita do campo **Conexão de dispositivo móvel**.

2. Na lista suspensa, selecione **Configurar a autenticação**.

   Na janela de propriedades do Servidor de Administração que for aberta, exibindo a seção **Certificados**.

3. Selecione a opção de autenticação para dispositivos móveis no grupo de configurações **Autenticação do Servidor de Administração por dispositivos móveis**, e selecione a opção de autenticação para dispositivos de proteção UEFI no grupo de configurações **Autenticação do Servidor de Administração por dispositivos de proteção UEFI**.

   Quando o Servidor de Administração troca dados com dispositivos cliente, ele é autenticado através do uso de um certificado.

   Por padrão, o Servidor de Administração usa o certificado que foi criado durante a instalação do Servidor de Administração. Se quiser, você pode adicionar um novo certificado.

Para adicionar um novo certificado (opcional):

1. Selecione **Outro certificado**.

   O botão **Procurar** aparece.

2. Clique no botão **Procurar**.

3. Na janela que for aberta, especifique as configurações do certificado:

- Tipo de certificado

  Na lista suspensa, você pode selecionar um tipo de certificado:

  - **Certificado X.509**. Se esta opção estiver selecionada, você deve especificar a chave privada de um certificado e um certificado open source:
    - **Chave privada (.prk, .pem)**. Neste campo, clique no botão **Procurar** para especificar a chave privada de um formato de certificado PKCS #8 (*.prk).
    - **Chave pública (.cer)**. Neste campo, clique no botão **Procurar** para especificar uma chave pública no formato PEM (*.cer).
  - **Contêiner PKCS#12**. Se você selecionar esta opção, você pode especificar um arquivo de certificado no formato P12 ou PFX ao clicar no botão **Procurar** e preencher o campo **Arquivo de certificado**.

- Hora da ativação:
  - Imediatamente

    O certificado atual será imediatamente substituído pelo novo após você clicar em **OK**.

    Os dispositivos móveis anteriormente conectados não serão capazes de conectar-se ao Servidor de Administração.

  - Após a expiração deste período, dias

    Se você selecionar esta opção, um certificado de reserva será gerado. O certificado atual será substituído pelo novo no número especificado de dias. A data efetiva do certificado de reserva é exibida na seção **Certificados**.

    É recomendável planejar a reemissão com antecedência. O certificado de reserva deve ser baixado para os dispositivos móveis antes que o período especificado expire. Após o certificado atual ter sido substituído pelo novo, os dispositivos móveis conectados anteriormente que não possuam o certificado de reserva não serão capazes de se conectar ao Servidor de Administração.

4. Clique no botão **Propriedades** para exibir as configurações do certificado do Servidor de Administração selecionado.

Para reemitir certificado emitido através do Servidor de Administração:

1. Selecione **Certificado emitido através do Servidor de Administração**.
2. Clique no botão **Reemitir**.
3. Na janela que for aberta, especifique as seguintes configurações:

- Endereço da conexão:
  - Usar o endereço de conexão antigo

O endereço do Servidor de Administração ao qual os dispositivos móveis se conectam permanece inalterado.

Esta opção está marcada por padrão.

- Alterar o endereço de conexão para

  Se quiser que os dispositivos móveis se conectem a um endereço diferente, especifique o endereço relevante neste campo.

  Se o endereço da conexão de dispositivo móvel tiver sido alterado, um novo certificado deve ser emitido. O certificado antigo se torna inválido em todos os dispositivos móveis conectados. Os dispositivos anteriormente conectados não serão capazes de conectar-se ao Servidor de Administração, portanto eles se tornam mão gerenciáveis.

- Hora da ativação:

  - Imediatamente

    O certificado atual será imediatamente substituído pelo novo após você clicar em **OK**.

    Os dispositivos móveis anteriormente conectados não serão capazes de conectar-se ao Servidor de Administração.

  - Após a expiração deste período, dias

    Se você selecionar esta opção, um certificado de reserva será gerado. O certificado atual será substituído pelo novo no número especificado de dias. A data efetiva do certificado de reserva é exibida na seção **Certificados**.

    É recomendável planejar a reemissão com antecedência. O certificado de reserva deve ser baixado para os dispositivos móveis antes que o período especificado expire. Após o certificado atual ter sido substituído pelo novo, os dispositivos móveis conectados anteriormente que não possuam o certificado de reserva não serão capazes de se conectar ao Servidor de Administração.

4. Clique em **OK** para salvar as modificações e voltar para a janela **Certificados**.

5. Clique em **OK** para salvar as alterações e voltar ao Assistente de início rápido.

Para configurar a emissão, atualização automática e a criptografia de certificados de tipo geral para a identificação de dispositivos móveis pelo Servidor de Administração:

1. Clique no botão **Configurar** à direita do campo **Autenticação do dispositivo móvel**.

   A janela **Regras de emissão do certificado** se abre, exibindo a seção **Emissão de certificados móveis**.

2. Se necessário, especifique as seguintes configurações na seção **Configurações de emissão**:

   - **Tempo de validade do certificado, dias**

     Período de vida do certificado em dias. O tempo de vida padrão de um certificado é de 365 dias. Quando este período expirar, o dispositivo móvel não será capaz de conectar-se ao Servidor de Administração.

   - **Origem do certificado**

     Selecionar a origem de certificados de tipo geral para dispositivos móveis: os certificados são emitidos pelo Servidor de Administração ou eles são especificados manualmente.

     Você pode modificar os modelos de certificado se a integração com a infraestrutura de chaves públicas (PKI) tiver sido configurada na seção **Integração com PKI**. Neste caso, os seguintes campos de seleção de modelo estão disponíveis:

   - **Modelo padrão**

     Usar um certificado emitido por uma origem de certificado externa – Centro de Certificado – sob o modelo padrão.

     Por padrão, esta opção está selecionada.

   - **Outros modelos**

     Selecione um modelo usado para emitir certificados. Você pode especificar modelos de certificado no domínio. Clicar no botão **Atualizar a lista** atualiza a lista de modelos de certificados.

3. Se necessário, especifique as seguintes configurações para a emissão automática de certificados na seção **Configurações das Atualizações Automáticas**:

   - **Renovar quando o certificado estiver prestes a expirar em (dias)**

     O número de dias que restam até a expiração do certificado atual durante o qual o Servidor de Administração deve emitir um novo certificado. Por exemplo, se o valor do campo for 4, o Servidor de Administração emite um novo certificado quatro dias antes que o certificado atual expire. O valor padrão é 7.

   - **Reemitir o certificado automaticamente se possível**

     Selecione a opção para reemitir um certificado automaticamente pelo número de dias especificado no campo **Renovar quando o certificado estiver prestes a expirar em (dias)**. Caso um certificado tenha sido definido manualmente, ele não pode ser renovado automaticamente e a opção habilitada não funcionará.

     Por padrão, esta opção está desativada.

   Os certificados são automaticamente reemitidos por uma Autoridade de Certificação.

4. Se necessário, na seção **Proteção por senha**, especifique as configurações para descriptografar os certificados durante a instalação.

   Selecione a opção **Solicitar a senha durante a instalação do certificado** para solicitar ao usuário a senha quando o certificado for ser instalado em um dispositivo móvel. A senha somente é usada uma vez – Durante a instalação do certificado no dispositivo móvel.

   A senha será automaticamente gerada pelo Servidor de Administração e enviada ao endereço de e-mail que você especificou. Você pode especificar o endereço de e-mail do usuário ou o seu próprio endereço de e-mail se desejar usar outro método para encaminhar a senha ao usuário.

   Você pode usar o controle deslizante para especificar o número de caracteres na senha de descriptografia do certificado.

   A opção de solicitação da senha é necessária, por exemplo, para proteger um certificado compartilhado em um pacote de instalação independente do Kaspersky Endpoint Security for Android. A proteção por senha impedirá um intruso de obter o acesso ao certificado compartilhado por meio do roubo do pacote de instalação independente do Kaspersky Security Center Web Server.

   Se esta opção estiver desativada, o certificado é automaticamente descriptografado durante a instalação e o usuário não será solicitado a fornecer uma senha. Por padrão, esta opção está desativada.

5. Clique em **OK** para salvar as modificações e voltar ao Assistente de início rápido.

   Clique no botão **Cancelar** para voltar ao Assistente de início rápido sem salvar qualquer modificação feita.

Par ativar a função para migrar dispositivos móveis para um grupo de administração de sua escolha,

No menu **Mudança automática de dispositivos móveis**, selecione a opção **Criar uma regra de migração de dispositivos móveis**.

Se a opção **Criar uma regra de migração de dispositivos móveis** estiver selecionada, o aplicativo cria automaticamente um regra de mover que move os dispositivos sendo executados no Android e iOS para o grupo **Dispositivos gerenciados**:

- Com sistemas operacionais Android nos quais o Kaspersky Endpoint Security for Android e um certificado móvel estão instalados
- Com sistemas operacionais iOS nos quais o perfil MDM do iOS com um certificado compartilhado está instalado

Se tal regra já existir, o aplicativo não a cria novamente.

Por padrão, esta opção está desativada.

A Kaspersky não dá mais suporte ao Kaspersky Safe Browser.

Etapa 11. Baixar atualizações

As atualizações dos bancos de dados antivírus do Kaspersky Security Center e dos aplicativos gerenciados da Kaspersky são baixadas automaticamente. As atualizações necessárias são baixadas dos servidores da Kaspersky.

Para baixar atualizações separadamente do Assistente de início rápido, crie e configure a tarefa *Baixar as atualizações ao repositório do Servidor de Administração*.

Etapa 12. Localização dos dispositivos

A janela **Sondagem da rede** exibe as informações sobre o status da sondagem da rede executada pelo Servidor de Administração.

Você pode exibir os dispositivos na rede detectados pelo Servidor de Administração e receber a ajuda no trabalho com a janela **Descoberta de dispositivos** clicando nos links na parte inferior da janela.

É possível sondar a rede posteriormente, de modo separado, a partir do assistente de início rápido. Use o Console de Administração para configurar a sondagem de domínios do Windows, Active Directory, intervalos de IP e redes IPv6.

Etapa 13. Fechar o Assistente de início rápido

Na janela de conclusão do Assistente de início rápido, selecione a opção **Executar o Assistente de instalação remota** se desejar iniciar a instalação automática de aplicativos antivírus e/ou do Agente de Rede em dispositivos na sua rede.

Para concluir o Assistente, pressione o botão **Concluir**.

Configurar a conexão do Console de Administração ao Servidor de Administração

O Console de Administração está conectado ao Servidor de Administração por meio da porta SSL TCP 13291. A mesma porta pode ser usada por objetos de automação klakaut.

A Porta TCP 14000 somente poderá ser usada para conectar o Console de Administração, pontos de distribuição, Servidores de Administração secundários e objetos de automação klakaut, assim como para receber dados de dispositivos cliente.

Normalmente, a porta SSL TCP 13000 pode ser usada somente pelo Agente de Rede, um Servidor de Administração secundário e o Servidor de Administração principal na DMZ. Em alguns casos, o Console de Administração precisa ser conectado através da porta SSL 13000:

- Se uma porta SSL única for provavelmente usada tanto para o Console de Administração como para outras atividades (recebendo dados de dispositivos de cliente, conectando pontos de distribuição, conectando Servidores de Administração secundários).
- Se um objeto de automação klakaut não estiver conectado ao Servidor de Administração diretamente, mas através de um ponto de distribuição na DMZ.

Para permitir a conexão do Console de Administração através da porta 13000:

1. Abra o registro do sistema do dispositivo cliente no qual o Servidor de Administração está instalado (por exemplo, usando o comando regedit no menu **Iniciar** → **Executar**).
2. Vá ao seguinte hive:
   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Para a chave LP_ConsoleMustUsePort13291 (DWORD), defina 00000000 como o valor.

   O valor padrão especificado para esta chave é 1.
4. Reinicie o serviço do Servidor de Administração.

Você será capaz de conectar o Console de Administração ao Servidor de Administração através da porta 13000.

Definição das configurações de acesso à Internet para o Servidor de Administração

É preciso configurar o acesso à Internet para usar a Kaspersky Security Network e baixar atualizações de bancos de dados de antivírus para o Kaspersky Security Center e aplicativos Kaspersky gerenciados.

Para especificar as configurações de acesso à Internet para o Servidor de Administração:

1. Na árvore do console, selecione o nó **Servidor de Administração**.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, vá para **Avançado → Configurando acesso à internet**.
4. Selecione a opção **Usar o servidor proxy** caso queira usar um servidor proxy para se conectar com a Internet. Se essa opção estiver selecionada, os campos estarão disponíveis para inserir configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:

   - **Endereço**

     Endereço do servidor proxy usado para conexão do Kaspersky Security Center à Internet.

   - **Número da porta**

     Número da porta pela qual a conexão proxy do Kaspersky Security Center será estabelecida.

   - **Ignorar servidor proxy para endereços locais**

     Nenhum servidor proxy será usado para conectar-se aos dispositivos na rede local.

   - **Autenticação do servidor proxy**

     Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

     Este campo de entrada está disponível se a caixa de seleção **Usar o servidor proxy** estiver marcada.

   - **Nome do usuário**

     Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

   - **Senha**

     A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

     Para ver a senha inserida, mantenha pressionado o botão **Exibir** pelo tempo que você desejar.

Também é possível configurar o acesso à Internet usando o assistente de início rápido.

Conectando dispositivos fora do escritório

Esta seção descreve como conectar dispositivos externos (ou seja, dispositivos gerenciados localizados fora da rede principal) ao Servidor de Administração.

Cenário: Conectando dispositivos externos por meio de um gateway de conexão

Este cenário descreve como conectar dispositivos gerenciados localizados fora da rede principal ao Servidor de Administração.

Pré-requisitos

O cenário tem os seguintes prerrequisitos:

- Uma zona desmilitarizada (DMZ) é organizada na rede da organização.
- O Servidor de Administração do Kaspersky Security Center é implementado na rede corporativa.

Fases

O cenário segue em etapas:

1. **Selecionando um dispositivo cliente na DMZ**

   Este dispositivo será usado como um gateway de conexão. O dispositivo selecionado deve atender aos requisitos de gateways de conexão.

2. **Instalando o Agente de Rede na função de gateway de conexão**

   Recomendamos que você use a instalação local para instalar o Agente de Rede no dispositivo selecionado.

   Por padrão, o arquivo de instalação está localizado em: \\<nome do servidor.>\KLSHARE\PkgInst\NetAgent_<número da versão>

   Na janela **Gateway de conexão** do Assistente de Instalação do Agente de Rede, selecione **Usar o Agente de Rede como um gateway de conexão na DMZ**. Esse modo ativa simultaneamente a função de gateway de conexão e sinaliza ao Agente de Rede para aguardar as conexões do Servidor de Administração em vez de estabelecer conexões com o Servidor de Administração.

   Alternativamente, você pode instalar o Agente de Rede em um dispositivo Linux e configurá-lo para funcionar como um gateway de conexão, mas atente para a lista de limitações do Agente de Rede em execução em dispositivos Linux.

3. **Permitindo conexões em firewalls no gateway de conexão**

   Para certificar-se de que o Servidor de Administração pode realmente se conectar ao gateway de conexão na DMZ, permita conexões com a porta TCP 13000 em todos os firewalls entre o Servidor de Administração e o gateway de conexão.

   Se o gateway de conexão não tiver um endereço IP real na Internet, mas estiver localizado atrás da Tradução de Endereço de Rede (NAT), configure uma regra para encaminhar as conexões por meio da NAT.

4 **Criando um grupo de administração para dispositivos externos**

Criar um novo grupo no grupo **Dispositivos gerenciados**. Esse novo grupo conterá dispositivos externos gerenciados.

5 **Conectando o gateway de conexão a um Servidor de Administração**

O gateway de conexão configurado está esperando por uma conexão vinda do Servidor de Administração. No entanto, o Servidor de Administração não lista o dispositivo com o gateway de conexão entre os dispositivos gerenciados. Isso ocorre porque o gateway de conexão não tentou estabelecer uma conexão com o Servidor de Administração. Portanto, você precisa de um procedimento especial para garantir que o Servidor de Administração inicie uma conexão com o gateway de conexão.

Faça o seguinte:

1. Adicione o gateway de conexão como um ponto de distribuição.
2. Mova o gateway de conexão do grupo **Dispositivos não atribuídos** para o grupo que criado para dispositivos externos.

O gateway de conexão está conectado e configurado.

6 **Conexão de dispositivos de desktop externos ao Servidor de Administração**

Normalmente, os dispositivos de desktop externos não são movidos dentro do perímetro. Portanto, você precisa configurá-los para se conectarem ao Servidor de Administração por meio do gateway ao instalar o Agente de Rede.

7 **Configuração de atualizações para os dispositivos de desktop externos**

Se as atualizações de aplicativos de segurança forem configuradas para serem baixadas do Servidor de Administração, os dispositivos externos baixarão as atualizações por meio do gateway de conexão. Isso apresenta duas desvantagens:

- Tráfego desnecessário é gerado, o que ocupa a largura de banda do canal de comunicação via Internet da empresa.
- Essa não é necessariamente a maneira mais rápida de obter atualizações. É muito provável que seja mais barato e rápido para os dispositivos externos receberem atualizações dos servidores de atualização Kaspersky.

Faça o seguinte:

1. Mova todos os dispositivos externos para o grupo de administração separado criado anteriormente.
2. Exclua o grupo com dispositivos externos da tarefa de atualização.
3. Crie uma tarefa de atualização separada para o grupo com dispositivos externos.

8 **Conectando laptops em trânsito ao Servidor de Administração**

Laptops itinerantes encontram-se às vezes dentro da rede e fora e outras ocasiões. Para um gerenciamento eficaz, é necessário que eles se conectem ao Servidor de Administração de maneira diferente dependendo de sua localização. Para um uso eficiente do tráfego, eles também precisam receber atualizações de diferentes fontes dependendo de sua localização.

É necessário configurar regras para usuários ausentes: perfis de conexão e descrições de local de rede. Cada regra define o Servidor de Administração, a instância à qual os laptops itinerantes devem se conectar, dependendo de sua localização e do Servidor de Administração a partir do qual devem receber atualizações.

Cenário: conectando dispositivos ausentes do escritório por meio de um Servidor de Administração secundário na DMZ

Caso queira conectar dispositivos gerenciados e localizados fora da rede principal ao Servidor de Administração, é possível fazer isso usando um Servidor de Administração secundário localizado na zona desmilitarizada (DMZ).

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- Uma DMZ é organizada na rede da organização.
- O Servidor de Administração do Kaspersky Security Center é implementado na rede corporativa.

Fases

O cenário segue em etapas:

1. **Selecionando um dispositivo cliente na DMZ**

   Na DMZ, selecione um dispositivo cliente que será usado como um Servidor de Administração secundário.

2. **Instalando o Servidor de Administração do Kaspersky Security Center**

   Instale o Servidor de Administração do Kaspersky Security Center neste dispositivo cliente.

3. **Criar uma hierarquia de Servidores de Administração**

   Caso queira colocar um Servidor de Administração secundário na DMZ, o Servidor de Administração secundário deve receber uma conexão do Servidor de Administração principal. É possível adicionar um novo Servidor de administração como secundário para que o Servidor de Administração principal se conecte ao Servidor de Administração secundário pela porta 13000. Ao combinar dois Servidores de Administração em uma hierarquia, verifique e confirme se a porta 13291 está acessível em ambos os Servidores de Administração. O Console de Administração se conecta ao Servidor de Administração pela porta 13291.

4. **Conectando dispositivos gerenciados e ausentes do escritório ao Servidor de Administração secundário**

   É possível conectar dispositivos ausentes do escritório ao Servidor de Administração localizado na DMZ da mesma maneira que a conexão é estabelecida entre o Servidor de Administração e os dispositivos gerenciados localizados na rede principal. Os dispositivos gerenciados e ausentes do escritório iniciam a conexão pela porta 13000.

Sobre a conexão de dispositivos externos

Alguns dispositivos gerenciados encontram-se sempre localizados fora da rede principal (por exemplo, dispositivos nas filiais regionais da empresa; quiosques, caixas eletrônicos e terminais instalados em vários pontos de venda; dispositivos de funcionários em home-office). Alguns dispositivos saem do perímetro de vez em quando (por exemplo, laptops de usuários que visitam filiais regionais ou o escritório de um cliente).

Ainda é necessário monitorar e gerenciar a proteção de dispositivos ausentes – receber informações reais sobre seu status de proteção e manter os aplicativos de segurança neles atualizados. Isso é necessário porque, por exemplo, se tal dispositivo for comprometido enquanto estiver longe da rede principal, ele pode se tornar uma plataforma para a propagação de ameaças assim que se conectar à rede principal. Para conectar dispositivos externos ao Servidor de Administração, você pode usar dois métodos:

- Gateway de conexão na zona desmilitarizada (DMZ)

  Consulte o esquema de tráfego de dados: Servidor de Administração na LAN, dispositivos gerenciados na Internet, gateway de conexão em uso

- Servidor de Administração na DMZ

  Veja o esquema de tráfego de dados: Servidor de Administração na DMZ, dispositivos gerenciados na Internet

Um gateway de conexão na DMZ

Um método recomendado para conectar dispositivos externos ao Servidor de Administração é organizar uma DMZ na rede da organização e instalar um gateway de conexão na DMZ. Os dispositivos externos se conectarão ao gateway de conexão e o Servidor de Administração dentro da rede iniciará uma conexão aos dispositivos por meio do gateway de conexão.

Em comparação com o outro método, esse é mais seguro:

- Você não precisa abrir o acesso ao Servidor de Administração de fora da rede.
- Um gateway de conexão comprometido não representa um alto risco para a segurança dos dispositivos de rede. Na verdade, um gateway de conexão não realiza nenhum gerenciamento e não estabelece nenhuma conexão.

Além disso, um gateway de conexão não requer muitos recursos de hardware.

No entanto, esse método tem um processo de configuração mais complicado:

- Para fazer um dispositivo atuar como um gateway de conexão na DMZ, você precisa instalar o Agente de Rede e conectá-lo ao Servidor de Administração de uma maneira muito específica.
- Você não poderá usar o mesmo endereço para se conectar ao Servidor de Administração em todas as situações. Fora do perímetro, você precisará usar não apenas um endereço diferente (endereço do gateway de conexão), mas também um modo de conexão diferente: por meio de um gateway de conexão.
- Você também precisa definir configurações de conexão diferentes para laptops em locais diferentes.

Para adicionar um gateway de conexão a uma rede configurada anteriormente:

1. Instale o Agente de Rede na função de gateway de conexão.
2. Reinstale o Agente de Rede em dispositivos que deseja conectar ao gateway de conexão recém-adicionado.

Servidor de Administração na DMZ

Outro método é instalar um único Servidor de Administração na DMZ.

Essa configuração é menos segura do que o outro método. Para gerenciar laptops externos, neste caso, o Servidor de Administração deve aceitar conexões de qualquer endereço na Internet. Ele ainda irá gerenciar todos os dispositivos na rede interna, mas na DMZ. Portanto, um servidor comprometido pode causar uma enorme quantidade de danos, apesar da baixa probabilidade de tal evento.

O risco é significativamente reduzido se o Servidor de Administração na DMZ não gerenciar os dispositivos na rede interna. Essa configuração pode ser usada, por exemplo, por um provedor de serviços para gerenciar os dispositivos dos clientes.

Você pode querer usar esse método nos seguintes casos:

- Se tiver familiaridade com a instalação e configuração do Servidor de Administração e não deseja executar outro procedimento para instalar e configurar um gateway de conexão.
- Se precisar gerenciar mais dispositivos. A capacidade máxima do Servidor de Administração é de 100.000 dispositivos, enquanto um gateway de conexão pode suportar até 10.000 dispositivos.

Esta solução também tem possíveis dificuldades:

- O Servidor de Administração requer mais recursos de hardware e mais um banco de dados.
- As informações sobre os dispositivos serão armazenadas em dois bancos de dados não relacionados (para o Servidor de Administração dentro da rede e outro na DMZ), o que complica o monitoramento.
- Para gerenciar todos os dispositivos, o Servidor de Administração precisa ser unido em uma hierarquia, o que complica não apenas o monitoramento, mas também o gerenciamento. Uma instância do Servidor de Administração secundário impõe limitações às estruturas possíveis de grupos de administração. Você deve decidir como e quais tarefas e políticas distribuir para uma instância secundária do Servidor de Administração.
- Configurar dispositivos externos para usar o Servidor de Administração na DMZ externamente e para usar o Servidor de Administração principal internamente não é mais simples do que apenas configurá-los para usar uma conexão condicional por meio de um gateway.
- Riscos de segurança elevados. Uma instância do Servidor de Administração comprometida torna mais fácil comprometer seus laptops gerenciados. Se isso acontecer, os hackers precisam apenas esperar que um dos laptops retorne à rede corporativa para que possam continuar seu ataque à rede local.

Conexão de dispositivos de desktop externos ao Servidor de Administração

Os dispositivos de desktop que estão sempre fora da rede principal (por exemplo, computadores nas filiais regionais da empresa; quiosques, caixas eletrônicos e terminais instalados em vários pontos de venda; dispositivos de funcionários em home-office) não podem ser conectados diretamente ao Servidor de Administração. Esses devem ser conectados ao Servidor de Administração por meio de um gateway de conexão instalado na zona desmilitarizada (DMZ). Essa configuração é feita ao instalar o Agente de Rede nesses dispositivos.

Para conectar dispositivos de desktop externos ao Servidor de Administração:

1. Crie um novo pacote de instalação para o Agente de Rede.
2. Abra as propriedades do pacote de instalação criado, acesse a seção **Avançado** e selecione a opção **Conectar-se ao Servidor de Administração usando o gateway de conexão**.

   A configuração **Conectar-se ao Servidor de Administração usando o gateway de conexão** é incompatível com a configuração **Usar o Agente de Rede como um gateway de conexão na DMZ**. Não é possível ativar essas duas configurações ao mesmo tempo.

3. Em **Endereço do gateway de conexão**, especifique o endereço público do gateway de conexão.

   Se o gateway de conexão estiver localizado atrás da Tradução de Endereço de Rede (NAT) e não tiver seu próprio endereço público, configure uma regra de gateway NAT para encaminhar conexões do endereço público para o endereço interno do gateway de conexão.

4. Crie um pacote de instalação independente com base no pacote de instalação criado.
5. Forneça o pacote de instalação independente aos dispositivos de destino por meio eletrônico ou de uma unidade removível.
6. Instale o Agente de Rede a partir do pacote independente.

Os dispositivos de desktop externos são conectados com o Servidor de Administração.

Sobre a configuração de perfis de conexão para usuários ausentes

Os usuários ausentes de laptops (aqui também referidos como "dispositivos") podem precisar alterar o método da conexão a um Servidor de Administração ou alternar entre Servidores de Administração dependendo da localização atual do dispositivo na rede corporativa.

Os perfis de conexão têm suporte somente para dispositivos que executam Windows e macOS.

Usar endereços diferentes de um Servidor de Administração único

Os dispositivos com o Agente de Rede instalado podem conectar-se ao Servidor de Administração da intranet da organização ou a partir da Internet. Esta situação pode necessitar que o Agente de Rede use endereços diferentes para a conexão ao Servidor de Administração: o endereço do Servidor de Administração externo para a conexão com a Internet e o endereço do Servidor de Administração interno para a conexão da rede interna.

Para fazer isto, você deve adicionar um perfil (para a conexão ao Servidor de Administração a partir da Internet) à política do Agente de Rede. Adicione o perfil nas propriedades da política (Seção **Conectividade**, subsecção **Perfis de conexão**). Na janela de criação do perfil, você deve desativar a opção **Usar somente para receber atualizações** e selecionar a opção **Sincronizar as configurações de conexão com as configurações do Servidor de Administração especificadas nesse perfil**. Se você usa um gateway de conexão para acessar o Servidor de Administração (por exemplo, em uma configuração do Kaspersky Security Center que está descrita em No acesso à Internet: Agente de Rede como um gateway de conexão em DMZ), deverá especificar o endereço do gateway de conexão no campo correspondente do perfil de conexão.

Alternar entre Servidores de Administração dependendo da rede atual

Se a organização tiver múltiplos escritórios com diferentes Servidores de Administração e alguns dispositivos com o Agente de Rede instalado se moverem entre eles, você precisa do Agente de Rede para conectar-se ao Servidor de Administração da rede local no escritório onde o dispositivo está atualmente localizado.

Neste caso, você deve criar um perfil para a conexão ao Servidor de Administração nas propriedades da política do Agente de Rede de cada um dos escritórios, exceto para o escritório doméstico onde o Servidor de Administração mestre original esteja localizado. Você deve especificar os endereços dos Servidores de Administração em perfis de conexão e ativar ou desativar a opção **Usar somente para receber atualizações**:

- Selecione a opção se você precisar que o Agente de Rede seja sincronizado com o Servidor de Administração mestre, usando o Servidor local somente para baixar as atualizações.
- Desative a opção se for necessário que o Agente de Rede seja gerenciado completamente pelo Servidor de Administração local.

Após isso, você deve definir as condições da troca para os perfis recém criados: ao menos uma condição de cada um dos escritórios, exceto para o escritório doméstico. Cada propósito de condição consiste na detecção de itens que são específicos para o ambiente de rede de um escritório. Se uma condição for verdadeira, o perfil correspondente é ativado. Se nenhuma das condições for verdadeira, o Agente de Rede alterna para o Servidor de Administração mestre.

Criando um perfil de conexão para usuários ausentes

Um perfil de conexão do Servidor de Administração está disponível somente em dispositivos que executam Windows e macOS.

Para criar um perfil para a conexão do Agente de Rede ao Servidor de Administração para usuários fora do escritório:

1. Na árvore do console, selecione um grupo de administração para os dispositivos cliente para os quais você precisa criar um perfil de conexão do Agente de Rede ao Servidor de Administração.
2. Execute uma das seguintes ações:
   - Se você precisar criar um perfil de conexão para todos os dispositivos no grupo, selecione uma política do Agente de Rede no espaço de trabalho do grupo, na guia **Políticas**. Abra a janela Propriedades da política selecionada.
   - Se você precisar criar um perfil de conexão de para um dispositivo em um grupo, selecione aquele dispositivo no espaço de trabalho do grupo, na guia **Dispositivos**, e execute as seguintes ações:
     a. Abra a janela Propriedades do dispositivo selecionado.
     b. Na seção **Aplicativos** da janela Propriedades do dispositivo, selecione o Agente de Rede.
     c. Abra a janela de propriedades do Agente de Rede.
3. Na janela de propriedades, na seção **Conectividade**, selecione a subseção **Perfis de conexão**.

4. No grupo de configurações **Perfis de conexão do Servidor de Administração**, clique no botão **Adicionar**.

   Por padrão, a lista de perfis de conexão contém os perfis <Modo offline> e <Servidor de Administração principal>. O perfil não pode ser editado ou removido.

   O perfil <Modo offline> não especifica nenhum Servidor para conexão. Portanto, o Agente de Rede, quando alternado para esse perfil, não tentará fazer conexão com nenhum Servidor de Administração enquanto os aplicativos instalados nos dispositivos cliente forem executados sob políticas de ausência. O perfil <Modo offline> pode ser usado se os dispositivos estiverem desconectados da rede.

   O perfil <Servidor de Administração principal> especifica para a conexão o Servidor de Administração que foi selecionado durante a instalação do Agente de Rede. O perfil <Servidor de Administração principal> é aplicado quando um dispositivo for reconectado ao Servidor de Administração principal após que ele estava sendo executado em uma rede externa por algum tempo.

5. Na janela **Novo perfil** que se abre, configure o perfil de conexão:

- Nome do perfil

  No campo de entrada, é possível consultar ou alterar o nome do perfil de conexão.

- Servidor de Administração

  O endereço do Servidor de administração ao qual o dispositivo cliente deve conectar-se durante a ativação do perfil.

- Porta

  O número da porta que é usada para conexão.

- Porta SSL

  Número da porta para conexão com, uso do protocolo SSL.

- Usar SSL

  Se esta opção estiver ativada, a conexão é estabelecida através de uma porta segura, com o protocolo SSL.

  Por padrão, esta opção está ativada. Recomendamos não desativar a opção para que a conexão permaneça segura.

- Clique no link **Configurar conexão pelo servidor proxy** para configurar a conexão por meio de um servidor proxy. Selecione a opção **Usar o servidor proxy** caso queira usar um servidor proxy para se conectar com a Internet. Se essa opção estiver selecionada, os campos estarão disponíveis para inserir configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:

  - Endereço do servidor proxy

    Endereço do servidor proxy usado para conexão do Kaspersky Security Center à Internet.

  - Número da porta

    Número da porta pela qual a conexão proxy do Kaspersky Security Center será estabelecida.

  - Autenticação do servidor proxy

    Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

    Este campo de entrada está disponível se a caixa de seleção **Usar o servidor proxy** estiver marcada.

  - Nome do usuário (o campo está disponível caso a opção **Autenticação do servidor proxy** esteja selecionada)

Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

- **Senha** (o campo está disponível caso a opção **Autenticação do servidor proxy** esteja selecionada)

  A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

  Para ver a senha inserida, mantenha pressionado o botão **Exibir** pelo tempo que você desejar.

- **Configurações de gateway de conexão**

  O endereço do gateway através do qual os dispositivos cliente se conectam com o Servidor de Administração.

- **Ativar modo ausente**

  Se esta opção estiver marcada, no caso da conexão com este perfil, os aplicativos instalados no dispositivo cliente irão usar as políticas de ausência de escritório, assim como as políticas de ausência de escritório. Se a política de ausência não estiver definida para o aplicativo, a política ativa será usada.

  Se esta opção estiver desativada, os aplicativos usarão as políticas ativas.

  Por padrão, esta opção está desativada.

- **Usar somente para receber atualizações**

  Se esta opção estiver ativada, o perfil somente será usado para baixar atualizações pelos aplicativos instalados no dispositivo cliente. Para outras operações, a conexão ao Servidor de Administração será estabelecida com as configurações de conexão iniciais definidas durante a instalação do Agente de Rede.

  Por padrão, esta opção está ativada.

- **Sincronizar as configurações de conexão com as configurações do Servidor de Administração especificadas nesse perfil**

  Se esta opção estiver ativada, o Agente de Rede se conecta ao Servidor de Administração utilizando as configurações especificadas nas propriedades do perfil.

  Se esta opção estiver desativada, o Agente de Rede se conecta ao Servidor de Administração utilizando as configurações originais que foram especificadas durante a instalação.

  Esta opção está disponível se a opção **Usar para receber atualizações somente** estiver desativada.

  Por padrão, esta opção está desativada.

6. Selecione a opção **Ativar modo ausente quando o Servidor de Administração não estiver disponível** para permitir aos aplicativos instalados em um dispositivo cliente usar perfis da política para dispositivos no modo de ausência de escritório, assim como políticas de ausência de escritório, no momento de qualquer tentativa de conexão se o Servidor de Administração não estiver disponível. Se a política de ausência do escritório não estiver definida para o aplicativo, a política ativa será usada.

Um perfil para conectar o Agente de Rede ao Servidor de Administração é criado para usuários fora do escritório. Quando o Agente de Rede se conectar ao Servidor de Administração usando esse perfil, os aplicativos instalados no dispositivo cliente usarão as políticas para dispositivos no modo ausente ou políticas de ausência.

Sobre a mudança do Agente de Rede para outro servidor de Administração

As configurações iniciais da conexão do Agente de Rede ao Servidor de Administração são definidas durante a instalação do Agente de Rede. Para alternar o Agente de Rede para outros Servidores de Administração, é possível usar as regras de alternância. Esse recurso é compatível apenas com Agentes de Rede instalados em dispositivos executando o Windows ou macOS.

As regras de alternância podem ser acionadas ao alterar os seguintes parâmetros de rede:

- Endereço do gateway padrão.
- Endereço IP do servidor Dynamic Host Configuration Protocol (DHCP).
- Sufixo DNS da sub-rede.
- Endereço IP do servidor DNS da rede.
- Acessibilidade do domínio do Windows. Esse parâmetro está disponível apenas para dispositivos que executam o Windows.
- Endereço de sub-rede e máscara.
- Endereço IP do servidor WINS da rede. Esse parâmetro está disponível apenas para dispositivos que executam o Windows.
- DNS ou nome NetBIOS do dispositivo cliente.
- Acessibilidade do endereço de conexão SSL.

Caso as regras de alteração do Agente de Rede para outros Servidores de Administração tenham sido criadas, o Agente de Rede responderá às alterações nos parâmetros de rede da seguinte maneira:

- Se as configurações de rede estiverem em conformidade com uma das regras criadas, o Agente de Rede conecta-se ao Servidor de Administração especificado nessa regra. Os aplicativos instalados nos dispositivos cliente mudam para as políticas de ausência de escritório, desde que tal comportamento esteja ativado por uma regra.
- Se nenhuma das regras se aplicarem, o Agente de Rede retorna para as configurações padrão de conexão ao Servidor de Administração especificadas durante a instalação. Os aplicativos instalados nos dispositivos cliente alternam de volta para as políticas ativas.
- Se o Servidor de Administração não estiver acessível, o Agente de Rede usa as políticas de ausência de escritório.

O Agente de Rede troca para a política de ausência somente se a opção **Ativar modo ausente quando o Servidor de Administração não estiver disponível** estiver ativada nas configurações da política do Agente de Rede.

As configurações da conexão do Agente de Rede ao Servidor de Administração são salvas em um perfil de conexão. No perfil de conexão, você poderá criar regras de troca de dispositivos clientes para políticas de ausência de escritório, assim como configurar o perfil para que ele possa ser usado apenas para baixar atualizações.

Criar uma regra de troca do Agente de Rede por localização da rede

A troca do Agente de Rede por localização da rede está disponível somente em dispositivos que executam Windows e macOS.

Para criar uma regra para a troca do Agente de Rede de um Servidor de Administração para outro se as configurações de rede forem alteradas:

1. Na árvore do console, selecione um grupo de administração que contenha os dispositivos para os quais você precisa de criar uma regra de troca do Agente de Rede pela descrição da localização da rede.
2. Execute uma das seguintes ações:
   - Se você precisar criar uma regra para todos os dispositivos no grupo, siga para o espaço de trabalho do grupo, e selecione uma política de Agente de Rede na guia **Políticas**. Abra a janela Propriedades da política selecionada.
   - Se você precisar criar uma regra para um dispositivo selecionado de um grupo, siga para o espaço de trabalho do grupo, selecione o dispositivo na guia **Dispositivos**, e execute as seguintes ações:
     a. Abra a janela Propriedades do dispositivo selecionado.
     b. Na seção **Aplicativos** da janela Propriedades do dispositivo, selecione o Agente de Rede.
     c. Abra a janela de propriedades do Agente de Rede.
3. Na janela de **Propriedades** que se abre, na seção **Conectividade**, selecione a subseção **Perfis de conexão**.
4. Na seção **Configurações do local de rede**, clique no botão **Adicionar**.
5. Na janela **Nova descrição** que se abre, configure a descrição da localização da rede e a regra de troca. Especifique as seguintes configurações de descrição da localização da rede:
   - Nome da descrição da localização da rede

     O nome de uma descrição da localização da rede não pode ter mais do que 255 caracteres nem conter símbolos especiais, tal como ("*<>?\/:|).
   - Usar perfil de conexão

     Na lista suspensa, é possível especificar o perfil de conexão usado pelo Agente de Rede para conectar ao Servidor de Administração. Este perfil será usado quando as condições da descrição da localização da rede forem atendidas. O perfil de conexão contém as configurações para a conexão do Agente de Rede ao Servidor de Administração; ele também define quando os dispositivos cliente devem alternar para as políticas de ausência de escritório. O perfil é usado somente para baixar atualizações.

6. Na seção **Condições de troca**, clique no botão **Adicionar** para criar uma lista de condições da descrição da localização da rede.

   As condições de uma regra se combinam através do uso do operador lógico AND. Para acionar uma regra de troca através da descrição da localização da rede, todas as condições de troca da regra devem ser atendidas.

7. Na lista suspensa, selecione o valor corresponde à alteração das características da rede à qual o dispositivo cliente está conectado:

   - **Endereço do gateway de conexão padrão** – O endereço do gateway da rede principal foi alterado.
   - **Endereço do servidor DHCP** – O endereço IP do servidor Dynamic Host Configuration Protocol (DHCP) da rede foi alterado.
   - **Domínio DNS** – O sufixo DNS da sub-rede foi alterado.
   - **Endereço do servidor DNS** – O endereço IP do servidor DNS da rede foi alterado.
   - **Acessibilidade do domínio do Windows (somente Windows)** – Altera o status do domínio do Windows ao qual um dispositivo cliente está conectado. Use essa configuração apenas para dispositivos que executam o Windows.
   - **Sub-rede** – Alterações no endereço e máscara da rede.
   - **Endereço do servidor WINS (somente Windows)** – O endereço IP do servidor WINS da rede foi alterado. Use essa configuração apenas para dispositivos que executam o Windows.
   - **Capacidade de resolução de nome** – O nome DNS ou NetBIOS do dispositivo cliente foi alterado.
   - **Acessibilidade do endereço de conexão SSL**: o dispositivo cliente pode ou não (dependendo da opção selecionada) estabelecer uma conexão SSL com um servidor especificado (nome:porta). Para cada servidor, é possível especificar adicionalmente um certificado SSL. Nesse caso, o Agente de Rede verifica o certificado do servidor, além de verificar a capacidade de uma conexão SSL. Se o certificado não for correspondente, a conexão falhará. A frequência de conexão é de uma vez por minuto.

8. Na janela que for aberta, especifique o valor da condição para o Agente de Rede ser trocado para outro Servidor de Administração. O nome da janela depende do valor selecionado durante a etapa anterior. Especifique as seguintes configurações para a condição de troca:

   - **Valor**

     Neste campo, é possível adicionar um ou vários valores para a condição que está sendo criada.

   - **Corresponde a pelo menos um valor da lista**

     Se esta opção estiver selecionada, a condição será cumprida independentemente de qualquer valor especificado na lista **Valor**.

     Por padrão, esta opção está selecionada.

   - **Não corresponde a nenhum dos valores da lista**

     Se esta opção estiver selecionada, a condição é cumprida se o respectivo valor não constar da lista **Valor**.

9. Na janela **Nova descrição**, selecione a opção **Descrição ativada**, para ativar o uso da nova descrição da localização da rede.

Uma nova regra de troca através da descrição da localização da rede é criada; sempre que as suas condições forem atendidas, o Agente de Rede usa o perfil de conexão especificado na regra para conectar-se ao Servidor de Administração.

As descrições da localização da rede são verificadas quanto a uma correspondência com o layout da rede na ordem de suas aparições na lista. Se uma rede corresponder a diversas descrições, a primeira será utilizada. Você poderá alterar a ordem das regras na lista usando os botões **Para cima** (⬆) e **Para baixo** (⬇).

Criptografar comunicação com TLS

Para a correção de vulnerabilidades na rede corporativa de sua organização, é possível ativar a criptografia de tráfego usando o protocolo TLS. É possível ativar os protocolos de criptografia TLS e os pacotes de codificação compatíveis no Servidor de Administração e no Servidor de MDM do iOS. O Kaspersky Security Center é compatível com as versões 1.0, 1.1 e 1.2. É possível selecionar o protocolo de criptografia e os pacotes de codificação requeridos.

O Kaspersky Security Center usa um certificado autoassinado. Configuração adicional dos dispositivos iOS não é necessitada. Você também pode usar seus próprios certificados. Os especialistas da Kaspersky recomendam usar certificados emitidos por autoridades de certificação confiáveis.

Servidor de Administração

Para configurar protocolos de criptografia e pacotes de codificação permitidos no Servidor de Administração:

1. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Use o sinalizador SrvUseStrictSslSettings para configurar os protocolos de criptografia e pacotes de codificação permitidos no Servidor de Administração. Digite o seguinte comando no prompt de comando do Windows:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n SrvUseStrictSslSettings -v <valor> -t d
   ```

   Especifique o parâmetro <valor> do sinalizador SrvUseStrictSslSettings:

   - `4` - apenas o protocolo TLS 1.2 está ativado. Também os pacotes de codificação com TLS_RSA_WITH_AES_256_GCM_SHA384 são ativados (esses pacotes de codificação são necessários para a compatibilidade com versões anteriores do Kaspersky Security Center 11). Esse é o valor padrão.

     Os pacotes de codificação compatíveis com o protocolo TLS 1.2:

     - ECDHE-RSA-AES256-GCM-SHA384
     - ECDHE-RSA-AES256-SHA384
     - ECDHE-RSA-CHACHA20-POLY1305
     - AES256-GCM-SHA384 (pacote de codificação com TLS_RSA_WITH_AES_256_GCM_SHA384)
     - ECDHE-RSA-AES128-GCM-SHA256
     - ECDHE-RSA-AES128-SHA256

   - `5` - somente o protocolo TLS 1.2 está ativado. Para o protocolo TLS 1.2, os pacotes de codificação específicos listados abaixo são compatíveis.

     Os pacotes de codificação compatíveis com o protocolo 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

   Não recomendamos usar 0, 1, 2 ou 3 como o valor do parâmetro do sinalizador SrvUseStrictSslSettings. Esses valores de parâmetro correspondem a versões inseguras do protocolo TLS (os protocolos TLS 1.0 e TLS 1.1) e pacotes de codificação inseguros. Eles são usados somente para compatibilidade com versões anteriores do Kaspersky Security Center.

3. Reinicie os seguintes serviços do Kaspersky Security Center 14.2:

- Servidor de Administração
- Servidor Web
- Proxy de ativação

Servidor MDM do iOS

A conexão entre os dispositivos iOS e o Servidor de MDM do iOS é criptografada por padrão.

Para configurar protocolos de criptografia e pacotes de codificação permitidos no Servidor de MDM do iOS:

1. Abra o registro do sistema do dispositivo cliente com o Servidor de MDM do iOS instalado (por exemplo, localmente, usando o comando regedit no menu **Iniciar** → **Executar**).
2. Vá ao seguinte hive:
   - Para sistemas de 32 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\Connectors\KLIOSMDM\1.0.0.0\Cor
   - Para sistemas de 64 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\Connectors\KLIOSI
3. Crie uma chave com o nome de `StrictSslSettings`.
4. Especifique `DWORD` como o tipo de chave.
5. Defina o valor da chave:
   - `2` - os protocolos TLS 1.0, TLS 1.1 e TLS 1.2 estão ativados.
   - `3` - somente o protocolo TLS 1.2 está ativado (valor padrão).
6. Reinicie o serviço do Servidor de MDM do iOS do Kaspersky Security Center.

Notificações de eventos

Esta seção descreve como selecionar um método para entregar notificações do administrador sobre eventos em dispositivos cliente, e como definir as configurações de notificação de evento.

Ele também descreve como testar a distribuição de notificações de evento usando o vírus de teste Eicar.

Configurar a notificação de evento

O Kaspersky Security Center lhe permite configurar o método de notificação ao administrador sobre os eventos que ocorrem em dispositivos cliente e para configurar a notificação:

- E-mail. Sempre que ocorre um evento, o aplicativo envia uma notificação para os endereços de e-mail especificados. Você pode editar o texto da notificação.
- SMS. Sempre que ocorre um evento, o aplicativo envia uma notificação para os números de telefone especificados. Você pode configurar o envio de notificações SMS através do gateway de correio.
- Arquivo executável. Sempre que ocorre um evento em um dispositivo, o arquivo executável é iniciado na estação de trabalho do administrador. Usando o arquivo executável, o administrador pode receber os parâmetros de qualquer evento tiver ocorrido.

Para configurar a notificação de eventos que ocorrem em dispositivos cliente:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Clique no link **Configurar notificações e exportação de eventos** e selecione o valor **Configurar notificações** na lista suspensa.

   Isso abre a janela **Propriedades: Eventos**.

4. Na seção **Notificação**, selecione um método de notificação (por e-mail, SMS ou a executar um arquivo executável) e defina as configurações da notificação:

   - **E-mail**

A guia **E-mail** permite configurar notificações de e-mail para eventos.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome da rede Windows (nome NetBIOS) do dispositivo
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Se você ativar a opção **Usar consulta de DNS MX**, pode usar vários registros MX dos endereços IP para o mesmo nome DNS do servidor SMTP. O mesmo nome DNS pode ter vários registros de MX com valores diferentes de prioridade de recebimento de mensagens de e-mail. O Servidor de Administração tenta enviar notificações por e-mail ao servidor SMTP em ordem crescente de prioridade dos registros MX. Por padrão, esta opção está desativada.

Se você ativar **Usar consulta de DNS MX** e não ativar o uso de configurações TLS, recomendamos que use as configurações DNSSEC em seu dispositivo de servidor como uma medida adicional de proteção para o envio de notificações por e-mail.

Clique no link **Configurações** para definir configurações de notificação adicionais:

- Nome do assunto (nome do assunto de uma mensagem de e-mail)
- Endereço de e-mail do remetente
- Configurações de autenticação ESMTP

Você deve especificar uma conta para autenticação em um servidor SMTP se a opção de autenticação ESMTP estiver ativada para o servidor SMTP.

- Configurações TLS para servidor SMTP:
  - **Não usar TLS**

    Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.
  - **Usar TLS se compatível com servidor SMTP**

    Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.
  - **Sempre usar TLS, verificar a validade do certificado do servidor**

    Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se escolher o valor **Sempre usar TLS, verificar a validade do certificado do servidor**, poderá especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar as configurações de TLS para um servidor SMTP:

- Procurar por um arquivo de certificado do servidor SMTP:

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

- Procurar um arquivo de certificado de cliente:

Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer autoridade de certificação confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

- Certificado X-509:

Você deve especificar um arquivo com o certificado e um arquivo com a chave privada. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Quando os dois arquivos são carregados, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- Contêiner pkcs12:

Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

O campo **Mensagem da notificação** contém o texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto inclui parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio. Você pode editar o texto da mensagem adicionando outros parâmetros substitutos com detalhes mais relevantes sobre o evento. A lista de parâmetros substitutos está disponível ao clicar no botão à direita do campo.

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clique no link **Configurar limite numérico de notificações** para especificar a quantidade máxima de notificações que o aplicativo pode enviar ao longo do intervalo de tempo especificado.

Clique no botão **Enviar mensagem de teste** para verificar se você configurou as notificações corretamente. O aplicativo deve enviar uma notificação de teste aos endereços de e-mail especificados.

- SMS

A guia **SMS** permite configurar a transmissão de notificações por SMS de vários eventos para um telefone celular. As mensagens SMS são enviadas por meio de um gateway de correio.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula. As notificações serão entregues aos números de telefone associados aos endereços de e-mail especificados.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome da rede Windows (nome NetBIOS) do dispositivo
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Clique no link **Configurações** para definir configurações de notificação adicionais:

- Nome do assunto (nome do assunto de uma mensagem de e-mail)
- Endereço de e-mail do remetente
- Configurações de autenticação ESMTP

Se necessário, você pode especificar uma conta para autenticação em um servidor SMTP se a opção de autenticação ESMTP estiver ativada para o servidor SMTP.

- Configurações TLS para um servidor SMTP

Você pode desativar o uso de TLS, usar o TLS se o servidor SMTP for compatível com este protocolo ou pode forçar o uso de TLS apenas. Se optar por usar apenas TLS, poderá especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, se optar por usar apenas TLS, poderá especificar um certificado para autenticação de cliente no servidor SMTP.

- Procurar um arquivo de certificado do servidor SMTP

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Kaspersky Security Center. O Kaspersky Security Center verifica se o certificado do servidor do sistema SIEM também é assinado por uma autoridade de certificação confiável ou não. O Kaspersky Security Center não pode se conectar ao servidor do sistema SIEM se o certificado do servidor do sistema SIEM não foi recebido de uma autoridade de certificação confiável.

Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada. O campo **Mensagem de notificação** contém texto padrão com informações sobre o evento enviado pelo aplicativo quando ocorre um evento. Este texto inclui parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio. Você pode editar o texto da mensagem adicionando outros parâmetros substitutos com detalhes mais relevantes sobre o evento. A lista de parâmetros substitutos está disponível ao clicar no botão à direita do campo.

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clique no link **Configurar limite numérico de notificações** para especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

Clique no botão **Enviar mensagem de teste** para verificar se as notificações foram configuradas corretamente. O aplicativo deve enviar uma notificação de teste aos destinatários especificados.

- Arquivo executável a ser executado

  Se este método de notificação estiver selecionado, no campo de entrada, você pode especificar o aplicativo que será iniciado quando ocorre um evento.

  Clicar no link **Configurar limite numérico de notificações** permite especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

  Clicar no botão **Enviar mensagem de teste** permite verificar se você configurou as notificações apropriadamente: o aplicativo envia uma notificação de teste aos endereços de e-mail que você especificou.

5. No campo **Mensagem de notificação**, insira o texto que o aplicativo enviará quando um evento ocorrer.

   Você pode usar a lista suspensa à direita do campo de texto para adicionar configurações de substituição com detalhes de evento (por exemplo, descrição de evento ou a hora da ocorrência).

   Se o texto de notificação contiver uma porcentagem (%), você deve especificá-lo duas vezes seguidas para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

6. Clique no botão **Enviar mensagem de teste** para verificar se a notificação foi configurada corretamente.

   O aplicativo envia uma notificação de teste ao usuário especificado.

7. Clique em **OK** para salvar as alterações.

As configurações de notificação reajustadas serão aplicadas à todos os eventos que ocorrem em dispositivos cliente.

Você pode ignorar as configurações de notificação de determinados eventos na seção **Configuração de eventos** das configurações do Servidor de Administração, das configurações de uma política ou das configurações de um aplicativo.

Testar as notificações

Para verificar se as notificações de eventos foram enviadas, o aplicativo usa a notificação da detecção de "vírus" de teste EICAR em dispositivos cliente.

Para verificar o envio das notificações de eventos:

1. Interrompa a tarefa de proteção em tempo real do sistema de arquivos no dispositivo cliente e copie o "vírus" de teste EICAR para o dispositivo cliente. Em seguida, ative novamente a proteção em tempo real no sistema de arquivos.

2. Execute uma tarefa de verificação para dispositivos cliente em um grupo de administração ou para dispositivos específicos, inclusive um com o "vírus" EICAR.

   Se a tarefa de verificação estiver configurada corretamente, o "vírus" de teste será detectado. Se as notificações estiverem configuradas corretamente, você será notificado que um vírus foi detectado.

   No espaço de trabalho do nó **Servidor de Administração**, na guia **Eventos**, a seleção **Eventos recentes** exibe um registro de detecção de um "vírus".

O "vírus" de teste de EICAR não contém nenhum código que possa danificar seu dispositivo. No entanto, a maioria dos aplicativos de segurança de fabricantes identifica esse arquivo como um vírus. Você pode fazer download do "vírus" de teste no site oficial da EICAR.

Notificações de evento exibidas executando um arquivo executável

O Kaspersky Security Center pode notificar o administrador sobre os eventos nos dispositivos cliente, executando um arquivo executável. O arquivo executável deve conter outro arquivo executável com marcadores de posição do evento para enviar ao administrador (consulte a tabela abaixo).

Marcadores de posição para descrever um evento

Marcador de posição	Descrição do marcador de posição
%SEVERITY%	Gravidade do evento. Valores possíveis: • **Informações** • **Advertência** • **Erro** • **Crítico**
%COMPUTER%	Nome do dispositivo onde ocorreu o evento. O comprimento máximo do nome do dispositivo é de 256 caracteres.
%DOMAIN%	Nome de domínio do dispositivo onde o evento ocorreu.
%EVENT%	Nome do tipo de evento. O comprimento máximo do nome do tipo de evento é de 50 caracteres.
%DESCR%	Descrição de evento. O comprimento máximo da descrição é de mil caracteres.
%RISE_TIME%	Tempo de criação do evento.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nome da tarefa. O comprimento máximo do nome da tarefa é de 100 caracteres.
%KL_PRODUCT%	Nome do aplicativo.
%KL_VERSION%	Número da versão do aplicativo.
%KLCSAK_EVENT_SEVERITY_NUM%	Número da gravidade do evento. Valores possíveis: • 1 - **Informações** • 2 - **Advertência** • 3 - **Erro** • 4 - **Crítico**

Marcador de posição	Descrição do marcador de posição
%HOST_IP%	Endereço IP do dispositivo onde o evento ocorreu.
%HOST_CONN_IP%	Endereço IP da conexão do dispositivo onde o evento ocorreu.

Exemplo:
As notificações de eventos são enviadas através de um arquivo executável (como script1.bat) dentro do qual outro arquivo executável (como script2.bat) com o marcador de posição %COMPUTER% é executado. Quando um evento ocorrer, o arquivo script1.bat é executado no dispositivo do administrador, o qual, por sua vez, executa o arquivo script2.bat com o marcador de posição %COMPUTER%. O administrador recebe o nome do dispositivo no qual o evento ocorreu.

Configurar interface

Você pode configurar a interface do Kaspersky Security Center:

- Exibir e ocultar os objetos na árvore do console, espaço de trabalho e janelas de propriedades de objetos (pastas, seções) dependendo dos recursos sendo utilizados.
- Exibir e ocultar elementos da janela principal (por exemplo, árvore do console ou menus padrão como **Ações** e **Exibir**).

Para configurar a interface do Kaspersky Security Center de acordo com o conjunto de recursos usados no momento:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No barra de menus da janela principal do aplicativo, selecione **Exibir** → **Configurar interface**.

3. Na janela **Configurar interface** que é exibida, configure a exibição de elementos da interface usando as caixas de seleção que se seguem:

- Exibir Gerenciamento de patches e vulnerabilidades

  Se esta opção estiver ativada, a pasta **Instalação remota** exibe a subpasta **Implementar imagens de dispositivos**, e a pasta **Repositórios** exibe a subpasta **Hardware**.

  Esta opção é desativada por padrão se o Assistente de início rápido não tiver sido concluído. Esta opção estiver ativada por padrão após a conclusão do Assistente de início rápido.

  Caso esta opção esteja desativada, os itens de menu **Criar sessões RDP** e **Windows Desktop Sharing** não estarão disponíveis, mesmo se você tiver uma Licença de gerenciamento de sistemas.

- Exibir a criptografia e a proteção dos dados

  Se esta opção estiver ativada, a árvore do console exibirá a pasta **Criptografia e proteção de dados**.

  Por padrão, esta opção está ativada.

- Exibir configurações de controle de endpoint

  Se esta opção estiver ativada, as subseções a seguir são exibidas na seção **Controles de Segurança** da janela de propriedades da política do Kaspersky Endpoint Security for Windows:

  - **Controle de Aplicativos**
  - **Controle de Dispositivo**
  - **Controle da Web**
  - **Controle Adaptativo de Anomalia**

  Se esta opção estiver desativada, essas subseções não são exibidas na seção **Controles de Segurança**.

  Por padrão, esta opção está ativada.

- Exibir Gerenciamento de Dispositivos Móveis

  Se esta opção estiver ativada, o recurso **Gerenciamento de Dispositivos Móveis** está disponível. Após reiniciar o aplicativo, a árvore do console exibe a pasta **Dispositivos móveis**.

  Por padrão, esta opção está ativada.

- Exibir Servidores de Administração secundários

  Se esta caixa de seleção for selecionada, a árvore do console exibe os nós dos Servidores de Administração secundários e virtuais nos grupos de administração. Os recursos conectados aos Servidores de Administração virtuais e secundários estão disponíveis para isso, como por exemplo, a criação de tarefas para a instalação remota de aplicativos em Servidores de Administração secundários.

  Por padrão, esta caixa de seleção está desmarcada.

- Exibir as seções das configurações de segurança

  Se esta opção estiver ativada, a seção **Segurança** é exibida nas propriedades do Servidor de Administração, grupos de administração e outros objetos. Esta opção permite conceder aos usuários e grupos de usuários permissões personalizadas para trabalhar com objetos.

  Por padrão, esta opção está desativada.

4. Clique em **OK**.

Para aplicar algumas das alterações, você tem que fechar a janela principal do aplicativo e, a seguir, abri-la de novo.

Para configurar a exibição de elementos na janela principal do aplicativo:

1. No barra de menus da janela principal do aplicativo, selecione **Exibir** → **Configurar**.
2. Na janela **Configurar a exibição** que é exibida, configure a exibição dos elementos da janela principal usando as caixas de seleção.
3. Clique em **OK**.

Localizar dispositivos na rede

Esta seção descreve as etapas que você deve seguir depois da instalação do Kaspersky Security Center.

Cenário: Localizar dispositivos na rede

Você deve executar a localização de dispositivos antes da instalação dos aplicativos de segurança. O Servidor de Administração recebe informações sobre dispositivos descobertos e permite o gerenciamento dos dispositivos por meio de políticas. Sondagens de rede regulares são necessárias para atualizar a lista de dispositivos disponíveis na rede.

Antes de iniciar a sondagem da rede, verifique e confirme se o protocolo SMB está ativado. Caso contrário, o Kaspersky Security Center não poderá descobrir dispositivos na rede submetida a sondagem. Para ativar o protocolo SMB, siga as instruções para o seu sistema operacional.

A descoberta de dispositivos em rede ocorre nos seguintes estágios:

1. **Descobrir dispositivos**

   O Assistente de início rápido lhe guia através da descoberta de dispositivos inicial e ajuda a localizar os dispositivos na rede, tal como computadores, tablets e celulares. Você também pode realizar a localização de dispositivos manualmente.

2. **Configurar sondagens agendadas**

Decida qual(is) tipo(s) de sondagem deseja usar regularmente. Ative os tipos desejados e configure o agendamento de sondagem. É possível se referir às recomendações para frequência de sondagem de rede.

3. **Configuração de regras para adicionar dispositivos descobertos aos grupos de administração (opcionais)**

   Se novos dispositivos aparecerem na sua rede, eles serão descobertos durante as sondagens regulares e automaticamente incluídos no grupo **Dispositivos não atribuídos**. É possível configurar regras de movimento de dispositivos para alocar automaticamente os dispositivos para o grupo **Dispositivos gerenciados**. Também é possível configurar regras de retenção.

   Caso a etapa 3 seja ignorada, os dispositivos recém-descobertos serão alocados para o grupo **Dispositivos não atribuídos**. Se quiser, você poderá mover esses dispositivos para o grupo **Dispositivos gerenciados** manualmente. Caso os dispositivos sejam movidos manualmente para o grupo **Dispositivos gerenciados**, é possível analisar as informações sobre cada dispositivo e decidir se deseja movê-lo para um grupo de administração e, neste caso, para qual grupo exatamente.

Resultados

A conclusão do cenário produz o seguinte:

- O Servidor de Administração do Kaspersky Security Center descobre os dispositivos que estão na rede e fornece informações sobre eles.
- As sondagens futuras são realizadas segundo o agendamento especificado.
- Os dispositivos recém-descobertos são organizados de acordo com as regras configuradas. (Ou, se nenhuma regra estiver configurada, os dispositivos permanecerão no grupo **Dispositivos não atribuídos**).

Dispositivos não atribuídos

Esta seção fornece informações sobre como gerenciar dispositivos em uma rede corporativa se eles não estiverem incluídos em um grupo de administração.

Localização dos dispositivos

Esta seção descreve os tipos de descoberta de dispositivos disponíveis no Kaspersky Security Center e fornece informações sobre o uso de cada tipo.

O Servidor de Administração recebe informações sobre a estrutura da rede e os dispositivos nessa rede por meio de sondagem regular. As informações são registradas no banco de dados do Servidor de Administração. O Servidor de Administração pode usar os seguintes tipos de sondagem:

- **Sondagem da rede do Windows**. O Servidor de Administração pode executar dois tipos de sondagem de rede do Windows: rápida e completa. Durante uma sondagem rápida, o Servidor de Administração somente recupera a informação da lista dos nomes de NetBIOS dos dispositivos em todos os domínios da rede e grupos de trabalho. Durante a sondagem completa, são solicitadas mais informações de cada dispositivo cliente, como nome do sistema operacional, endereço IP, nome DNS e nome NetBIOS. Por padrão, as sondagens rápida e completa estão ativadas. A sondagem de rede do Windows pode não conseguir descobrir dispositivos, por exemplo, se as portas UDP 137, UDP 138, TCP 139 estiverem fechadas no roteador ou forem fechadas pelo firewall.

- **Sondagem do Active Directory**. O Servidor de Administração recupera informações sobre a estrutura da unidade do Active Directory e sobre os nomes DNS dos dispositivos dos grupos do Active Directory. Por padrão, esse tipo de sondagem está ativado. Recomendamos usar a sondagem do Active Directory, caso o Active Directory seja usado; caso contrário, o Servidor de Administração não descobrirá nenhum dispositivo. Se você usar o Active Directory, mas alguns dos dispositivos em rede não forem listados como membros, esses dispositivos não poderão ser descobertos pela sondagem do Active Directory.

- **Sondagem de intervalos de IP**. O Servidor de Administração fará a sondagem dos conjuntos de IPs especificados usando pacotes ICMP ou o protocolo NBNS e compilará um conjunto de dados completo nos dispositivos dentro dos conjuntos de IPs. Por padrão, esse tipo de sondagem está desativado. Não se recomenda usar esse tipo de sondagem se você usar a sondagem da rede do Windows e/ou a sondagem do Active Directory.

- **Sondagem zeroconf**. Um ponto de distribuição que sonda a rede IPv6 usando rede zero configuração (também referida como *Zeroconf*). Por padrão, esse tipo de sondagem está desativado. Você pode usar a sondagem do Zeroconf se o ponto de distribuição executar Linux.

Se você tiver configurado e ativado as regras para migrar dispositivos, os dispositivos recentemente descobertos estarão automaticamente incluídos no grupo **Dispositivos gerenciados**. Se nenhuma regra de movimento tiver sido ativada, os dispositivos recentemente descobertos serão automaticamente incluídos no grupo **Dispositivos não atribuídos**.

Você pode modificar as configurações de descoberta de dispositivo para cada tipo. Por exemplo, é possível modificar o agendamento de amostragem ou definir se deve amostrar toda a floresta do Active Directory ou apenas um domínio específico.

Antes de iniciar a sondagem da rede, verifique e confirme se o protocolo SMB está ativado. Caso contrário, o Kaspersky Security Center não poderá descobrir dispositivos na rede submetida a sondagem. Para ativar o protocolo SMB, siga as instruções para o seu sistema operacional.

Sondagem da rede do Windows

Sobre a sondagem de rede do Windows

Durante uma sondagem rápida, o Servidor de Administração somente recupera a informação da lista dos nomes de NetBIOS dos dispositivos em todos os domínios da rede e grupos de trabalho. Durante uma sondagem completa, as seguintes informações são solicitadas de cada dispositivo cliente:

- Nome de sistema operacional
- Endereço IP
- Nome DNS
- Nome NetBIOS

As sondagens rápida e completa requerem o seguinte:

- Portas UDP 137/138, TCP 139, UDP 445, TCP 445 devem estar disponíveis na rede.
- O protocolo SMB está ativado.
- O serviço Microsoft Computer Browser deve ser usado, e o navegador principal do computador deve estar ativado no Servidor de Administração.
- O serviço Microsoft Computer Browser deve ser usado, e o navegador principal do computador deve estar ativado nos dispositivos cliente:
  - Em pelo menos um dispositivo, se o número de dispositivos em rede não exceder 32.
  - Em pelo menos um dispositivo para cada 32 dispositivos em rede.

A sondagem completa poderá ser executada apenas se a sondagem rápida tiver sido executada pelo menos uma vez.

Visualização e alteração das configurações para a sondagem da rede Windows

Para modificar as configurações para a sondagem da rede do Windows:

1. Na árvore do console, expanda a pasta **Descoberta de dispositivos**, e selecione a subpasta **Domínios**.

   Você pode prosseguir da pasta **Dispositivos não atribuídos** para a pasta **Descoberta de dispositivos** clicando no botão **Amostrar agora**.

   No espaço de trabalho da subpasta **Domínios**, a lista dos dispositivos é exibida.

2. Clique em **Sondar agora**.

   A janela Propriedades do domínio é exibida. Se quiser, modifique as configurações da sondagem de rede do Windows:

   - **Ativar sondagem da rede Windows**

     Esta opção está marcada por padrão. Se não quiser executar a sondagem de rede do Windows (por exemplo, se considerar que a sondagem do Active Directory é suficiente), você poderá desmarcar esta opção.

   - **Definir agendamento da sondagem rápida**

O período padrão é de 15 minutos.

Durante uma sondagem rápida, o Servidor de Administração somente recupera a informação da lista dos nomes de NetBIOS dos dispositivos em todos os domínios da rede e grupos de trabalho.

Os dados recebidos na próxima sondagem substituem completamente os dados antigos.

As seguintes opções de agendamento da sondagem estão disponíveis:

- **A cada N dias**

  A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

  Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

- **A cada N minutos**

  A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

  Por padrão, a sondagem é executada a cada cinco minutos, iniciando na hora atual do sistema.

- **Por dias da semana**

  A sondagem é executada regularmente, nos dias da semana e na hora especificados.

  Por padrão, a sondagem é executada todas as sextas-feiras às 18h.

- **Todo mês em dias especificados de semanas selecionadas**

  A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- **Executar tarefas ignoradas**

  Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

  Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

  Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

  Por padrão, esta opção está ativada.

- **Definir agendamento da sondagem completa**

O período padrão é de uma hora. Os dados recebidos na próxima sondagem substituem completamente os dados antigos.

As seguintes opções de agendamento da sondagem estão disponíveis:

- **A cada N dias**

  A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

  Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

- **A cada N minutos**

  A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

  Por padrão, a sondagem é executada a cada cinco minutos, iniciando na hora atual do sistema.

- **Por dias da semana**

  A sondagem é executada regularmente, nos dias da semana e na hora especificados.

  Por padrão, a sondagem é executada todas as sextas-feiras às 18h.

- **Todo mês em dias especificados de semanas selecionadas**

  A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- **Executar tarefas ignoradas**

  Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

  Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

  Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

  Por padrão, esta opção está ativada.

Se quiser executar a sondagem imediatamente, clique em **Sondar agora**. Ambos os tipos de sondagem serão iniciados.

No Servidor de Administração virtual, você pode visualizar e editar as configurações de sondagem da rede do Windows na janela Propriedades do ponto de distribuição, na seção **Descoberta de dispositivos**.

Sondagem do Active Directory

Use a sondagem do Active Directory se você usar o Active Directory; caso contrário, recomenda-se usar outros tipos de sondagem. Se você usar o Active Directory, mas alguns dos dispositivos em rede não forem listados como membros, esses dispositivos não poderão ser descobertos pela sondagem do Active Directory.

Os resultados da pesquisa do Active Directory são armazenados no Servidor de Administração por 30 dias, independentemente dos resultados das pesquisas subsequentes.

Antes de iniciar a sondagem da rede, verifique e confirme se o protocolo SMB está ativado. Caso contrário, o Kaspersky Security Center não poderá descobrir dispositivos na rede submetida a sondagem. Para ativar o protocolo SMB, siga as instruções para o seu sistema operacional.

Visualização e modificação de configurações para sondagem do Active Directory

Para visualizar e modificar as configurações para a sondagem de grupos do Active Directory:

1. Na árvore do console, expanda a pasta **Descoberta de dispositivos**, e selecione a subpasta **Active Directory**.

   Como alternativa, você pode prosseguir da pasta **Dispositivos não atribuídos** para a pasta **Descoberta de dispositivos** clicando no botão **Sondar agora**.

2. Clique em **Configurar a sondagem**.

   A janela Propriedades do Active Directory é aberta. Se quiser, modifique as configurações de sondagem do grupo do Active Directory:

   - Ativar sondagem do Active Directory

     Esta opção está marcada por padrão. Contudo, se você não usar o Active Directory, a sondagem não recuperará nenhum resultado. Neste caso, você pode desmarcar esta opção.

   - Definir agendamento da sondagem

O período padrão é de uma hora.

As seguintes opções de agendamento da sondagem estão disponíveis:

- **A cada N dias**

  A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

  Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

- **A cada N minutos**

  A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

  Por padrão, a sondagem é executada a cada cinco minutos, iniciando na hora atual do sistema.

- **Por dias da semana**

  A sondagem é executada regularmente, nos dias da semana e na hora especificados.

  Por padrão, a sondagem é executada todas as sextas-feiras às 18h.

- **Todo mês em dias especificados de semanas selecionadas**

  A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- **Executar tarefas ignoradas**

  Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

  Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

  Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

  Por padrão, esta opção está ativada.

- **Avançado**

Você pode selecionar quais domínios do Active Directory amostrar:

- Domínio do Active Directory ao qual o Kaspersky Security Center pertence.
- A floresta de domínio à qual o Kaspersky Security Center pertence.
- Lista especificada de domínios do Active Directory.

  Se você selecionar esta opção, poderá adicionar domínios ao escopo de sondagem:

  - Clique no botão **Adicionar**.
  - Nos campos correspondentes, especifique o endereço do controlador de domínio, o nome e a senha da conta para acessá-lo.
  - Clique em **OK** para salvar as alterações.

  Você pode selecionar o endereço do controlador de domínio na lista e clicar no botão **Modificar** ou **Remover** para modificá-lo ou removê-lo.
- Clique em **OK** para salvar as alterações.

Se quiser executar a sondagem imediatamente, clique no botão **Sondar agora**.

No Servidor de Administração virtual, você pode exibir e editar as configurações de sondagem de grupos do Active Directory na janela Propriedades do ponto de distribuição, na seção **Descoberta de dispositivos**.

Sondagem do conjunto de IPs

O Servidor de Administração fará a sondagem dos conjuntos de IPs especificados usando pacotes ICMP ou o protocolo NBNS e compilará um conjunto de dados completo nos dispositivos dentro dos conjuntos de IPs. Por padrão, esse tipo de sondagem está desativado.

Para todos os hosts baseados em Linux dentro de um controlador de domínio Microsoft Active Directory ou Samba, especifique o `netbios name` e os parâmetros do `workgroup` no arquivo `/etc/samba/smb.conf`. Caso contrário, os resultados da pesquisa podem conter hosts duplicados.

Antes de iniciar a sondagem da rede, verifique e confirme se o protocolo SMB está ativado. Caso contrário, o Kaspersky Security Center não poderá descobrir dispositivos na rede submetida a sondagem. Para ativar o protocolo SMB, siga as instruções para o seu sistema operacional.

Visualização e modificação de configurações para amostragem de faixas IP

Para visualizar e modificar as configurações para a amostragem de grupos de conjuntos de IPs:

1. Na árvore do console, expanda a pasta **Descoberta de dispositivos**, e selecione a subpasta **Intervalos de IPs**.

   Você pode prosseguir a partir da pasta **Dispositivos não atribuídos** para a pasta **Descoberta de dispositivos** clicando em **Sondar agora**.

2. Se desejar, na subpasta **Intervalos de IPs**, clique em **Adicionar sub-rede** para adicionar um conjunto de IPs para sondagem e, a seguir, clique em **OK**.

3. Clique em **Configurar a sondagem**.

   A janela de propriedades de conjuntos de IPs se abre. Se quiser, você pode modificar as configurações de sondagem de conjuntos de IPs:

   - **Ativar a sondagem de intervalos IP**

     Esta opção não está marcada por padrão. Não se recomenda usar esse tipo de sondagem se você usar a sondagem da rede do Windows e/ou a sondagem do Active Directory.

   - **Definir agendamento da sondagem**

O período padrão é de 420 minutos. Os dados recebidos na próxima sondagem substituem completamente os dados antigos.

As seguintes opções de agendamento da sondagem estão disponíveis:

- **A cada N dias**

  A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

  Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

- **A cada N minutos**

  A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

  Por padrão, a sondagem é executada a cada cinco minutos, iniciando na hora atual do sistema.

- **Por dias da semana**

  A sondagem é executada regularmente, nos dias da semana e na hora especificados.

  Por padrão, a sondagem é executada todas as sextas-feiras às 18h.

- **Todo mês em dias especificados de semanas selecionadas**

  A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- **Executar tarefas ignoradas**

  Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

  Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

  Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

  Por padrão, esta opção está ativada.

Se quiser executar a sondagem imediatamente, clique em **Sondar agora**. Este botão somente estará disponível se você tiver selecionado **Ativar a sondagem de intervalos IP**.

No Servidor de Administração virtual, você pode exibir e editar as configurações da sondagem de conjuntos de IPs na janela Propriedades do ponto de distribuição, na seção **Descoberta de dispositivos**. Os dispositivos cliente encontrados durante a sondagem de conjuntos de IPs são exibidos na pasta **Domínios** do Servidor de Administração virtual.

Sondagem Zeroconf

Este tipo de pesquisa é compatível apenas com pontos de distribuição baseados em Linux.

Um ponto de distribuição pode pesquisar redes que possuem dispositivos com endereços IPv6. Nesse caso, os intervalos IP não são especificados e o ponto de distribuição controla toda a rede usando a rede zero configuração (referida como *Zeroconf*). Para começar a usar o Zeroconf, você deve instalar o utilitário avahi-browse no ponto de distribuição.

Para habilitar a sondagem do Zeroconf:

1. Na árvore do console, expanda a pasta **Descoberta de dispositivos**, e selecione a subpasta **Intervalos de IPs**.

   Você pode prosseguir a partir da pasta **Dispositivos não atribuídos** para a pasta **Descoberta de dispositivos** clicando em **Sondar agora**.

2. Clique em **Configurar a sondagem**.

3. Na janela aberta de propriedades de intervalos IP, selecione **Ativar sondagem com tecnologia Zeroconf**.

Em seguida, o ponto de distribuição começa a sondar a rede. Nesse caso, os intervalos IP especificados são ignorados.

Trabalhar com domínios do Windows. Visualização e alteração das configurações de domínio

Para modificar as configurações de domínio:

1. Na árvore do console, expanda a pasta **Descoberta de dispositivos**, e selecione a subpasta **Domínios**.

2. Selecione um domínio e abra sua janela de propriedades numa das seguintes formas:

   - Selecionando **Propriedades** no menu de contexto do domínio.

   - Ao clicar no link **Mostrar propriedades de grupo**.

   A janela **Propriedades: <Nome do domínio>** será aberta, onde você poderá configurar o domínio selecionado.

Configuração de regras de retenção para dispositivos não atribuídos

Após a conclusão da sondagem de rede do Windows, os dispositivos encontrados são colocados em subgrupos do grupo de administração de Dispositivos não atribuídos. Este grupo de administração pode ser encontrado em **Avançado** → **Descoberta de dispositivos** → **Domínios**. A pasta **Domínios** é o grupo principal. Ele contém grupos denominados segundo os domínios e grupos de trabalho correspondentes encontrados durante a sondagem de rede. O grupo principal também pode conter o grupo de administração de dispositivos móveis. Você pode configurar as regras de retenção dos dispositivos não atribuídos do grupo principal e de cada um dos grupos secundários. As regras de retenção não dependem das configurações de sondagem de rede e funcionam mesmo se a sondagem de rede estiver desativada.

Para configurar as regras de retenção para dispositivos não atribuídos:

1. Na árvore do console, na pasta **Descoberta de dispositivos**, realize uma das seguintes ações:

   - Para definir configurações do grupo principal, clique com o botão direito na subpasta **Domínios** e selecione **Propriedades**.

     A janela Propriedades do grupo principal é aberta.

   - Para definir configurações de um grupo secundário, clique com o botão direito no nome do grupo e selecione **Propriedades**.

     A janela Propriedades do grupo secundário é aberta.

2. Na seção **Dispositivos**, especifique as seguintes configurações:

   - Remover o dispositivo do grupo se estiver inativo por mais de (dias)

     Se esta opção estiver selecionada, você poderá especificar o intervalo de tempo após o qual o dispositivo será automaticamente removido do grupo. Por padrão, esta opção também é distribuída aos grupos secundários. O intervalo de tempo predefinido é de 7 dias.

     Por padrão, esta opção está ativada.

   - Herdar do grupo principal

     Se esta opção estiver ativada, o período de retenção para os dispositivos no grupo atual é herdado do grupo principal e não pode ser alterado.

     Esta opção está disponível somente para grupos secundários.

     Por padrão, esta opção está ativada.

   - Forçar herança em grupos secundários

     Os valores de configuração serão distribuídos aos grupos secundários, mas essas configurações são bloqueadas nas propriedades dos grupos secundários.

     Por padrão, esta opção está desativada.

As suas alterações serão salvas e aplicadas.

Trabalhar com conjuntos de IPs

Você pode personalizar os conjuntos de IPs existentes e criar novos.

Criação de um conjunto de IPs

Para criar um conjunto de IPs:

1. Na árvore do console, expanda a pasta **Descoberta de dispositivos**, e selecione a subpasta **Intervalos de IPs**.
2. No menu de contexto da pasta, selecione **Nova → Intervalo de IP**.
3. Na janela **Novo intervalo de IPs** que se abre, defina o novo conjunto de IPs.

O novo conjunto de IPs aparece na pasta **Intervalos de IPs**.

Visualização e alteração de configurações de conjuntos de IPs

Para modificar as configurações de conjuntos de IPs:

1. Na árvore do console, na pasta **Descoberta de dispositivos** selecione a subpasta **Intervalos de IPs**.
2. Selecione um conjunto de IPs e abra sua janela de propriedades numa das seguintes formas:
   - Selecionando **Propriedades** no menu de contexto do conjunto de IPs.
   - Ao clicar no link **Mostrar propriedades de grupo**.

A janela **Propriedades: <Nome do conjunto de IPs>** será aberta, onde você poderá configurar as propriedades do conjunto de IPs selecionado.

Trabalhar com os grupos do Active Directory. Visualização e modificação de configurações de grupo

Para modificar as configurações para o grupo do Active Directory:

1. Na árvore do console, expanda a pasta **Descoberta de dispositivos**, e selecione a subpasta **Active Directory**.
2. Selecione um grupo do Active Directory e abra sua janela de propriedades numa das seguintes formas:
   - Selecionando **Propriedades** no menu de contexto do conjunto de IPs.
   - Ao clicar no link **Mostrar propriedades de grupo**.

A janela **Propriedades: <Nome do grupo Active Directory>** será aberta, onde você poderá configurar o grupo Active Directory selecionado.

Criar regras para migrar dispositivos automaticamente para grupos de administração

É possível configurar os dispositivos que serão movidos automaticamente para os grupos de administração após serem descobertos durante uma sondagem em uma rede corporativa.

Para configurar regras para mover automaticamente os dispositivos para grupos de administração:

1. Na árvore do console, selecione a pasta **Dispositivos não atribuídos**.
2. No espaço de trabalho desta pasta, clique em **Configurar regras**.

   Isso abre a janela **Propriedades: Dispositivos não atribuídos**. Na seção **Migrar dispositivos**, configure as regras para migrar dispositivos automaticamente para os grupos de administração.

A primeira regra aplicável na lista (de cima para baixo) será aplicada a um dispositivo.

Usar o modo dinâmico VDI nos dispositivos cliente

Uma infraestrutura virtual pode ser implementada em uma rede corporativa usando máquinas virtuais temporárias. O Kaspersky Security Center detecta máquinas virtuais temporárias e adiciona as informações sobre elas no banco de dados do Servidor de Administração. Após um usuário terminar de usar uma máquina virtual temporária, a máquina é removida da infraestrutura virtual. No entanto, um registro sobre a máquina virtual removida poderá ser salvo no banco de dados do Servidor de Administração. Além disso, máquinas virtuais não existentes podem ser exibidas no Console de Administração.

Para impedir que informações sobre máquinas virtuais não existentes sejam salvas, o Kaspersky Security Center oferece suporte ao modo dinâmico para o Virtual Desktop Infrastructure (VDI). O administrador pode ativar o suporte do modo dinâmico para VDI nas propriedades do pacote de instalação do Agente de Rede para que seja instalado na máquina virtual temporária.

Quando uma máquina virtual temporária é desativada, o Agente de Rede notifica o Servidor de Administração de que a máquina foi desativada. Após uma máquina virtual ter sido desativada com êxito, ela é removida da lista de dispositivos conectados com o Servidor de Administração. Se a máquina virtual for desativada com erros e o Agente de Rede não enviar uma notificação sobre a máquina virtual desativada para o Servidor de Administração, é usado um cenário de backup. Sob esse cenário, a máquina virtual é removida da lista de dispositivos conectados com o Servidor de Administração após três tentativas sem êxito de sincronização com o Servidor de Administração.

Ativar o modo dinâmico VDI nas propriedades de um pacote de instalação para o Agente de Rede

Para ativar o modo dinâmico VDI:

1. Na pasta **Instalação remota** na árvore do console, selecione a subpasta **Pacotes de instalação**.
2. No menu de contexto do pacote de instalação do Agente de Rede, selecione **Propriedades**.

   A janela **Propriedades: Agente de Rede do Kaspersky Security Center** é aberta.
3. Na janela **Propriedades: Agente de Rede do Kaspersky Security Center**, selecione a seção **Avançado**.
4. Na seção **Avançado**, selecione a opção **Ativar modo dinâmico para VDI**.

O dispositivo em que o Agente de Rede será instalado fará parte da VDI.

Pesquisar por dispositivos que fazem parte da VDI

Para encontrar dispositivos não atribuídos que fazem parte da VDI:

1. Selecione **Pesquisar** no menu de contexto da pasta **Dispositivos não atribuídos**.

   Para visualizar uma lista de todos os dispositivos que fazem parte da Virtual Desktop Infrastructure, selecione **Pesquisar** no menu de contexto da pasta **Servidor de Administração**.
2. Na janela **Pesquisar**, na guia **Máquinas virtuais**, selecione **Sim** no grupo de configurações **Parte da Virtual Desktop Infrastructure**.
3. Clique no botão **Localizar agora**.

A lista de dispositivos não atribuídos que fazem parte da Virtual Desktop Infrastructure é exibida.

Mover os dispositivos da VDI para um grupo de administração

Para migrar dispositivos que fazem parte da VDI para um grupo de administração:

1. No espaço de trabalho da pasta **Dispositivos não atribuídos**, clique em **Configurar regras**.

   Isso abre a janela Propriedades da pasta **Dispositivos não atribuídos**.
2. Na janela Propriedades da pasta **Dispositivos não atribuídos**, na seção **Migrar dispositivos**, clique no botão **Adicionar**.

   A janela **Nova regra** se abre.
3. Na janela **Nova regra**, selecione a seção **Máquinas virtuais**.
4. Na lista suspensa **Esta é uma máquina virtual**, selecione **Sim**.

Uma regra será criada para a realocação do dispositivo em um grupo de administração.

Inventário de equipamentos

A lista de hardware (**Repositórios** → **Hardware**) usada para inventariar equipamentos é preenchida de duas maneiras: automática e manualmente. Após cada sondagem de rede, todos os dispositivos detectados serão automaticamente adicionados na lista. No entanto, você também pode adicionar dispositivos manualmente se não quiser fazer a sondagem da rede. Você pode adicionar outros dispositivos na lista manualmente, por exemplo, roteadores, impressoras ou hardware de dispositivos.

Nas propriedades de um dispositivo, é possível ver e editar informações detalhadas sobre esse dispositivo.

A lista de hardware pode conter os seguintes tipos de dispositivos:

- Computadores
- Dispositivos móveis
- Dispositivos de rede
- Dispositivos virtuais
- Componentes OEM
- Periféricos do computador
- Dispositivos conectados
- Telefones VoIP
- Repositórios da rede

O administrador pode atribuir o atributo *Equipamento corporativo* aos dispositivos detectados. Este atributo pode ser atribuído manualmente nas propriedades de um dispositivo, ou o administrador pode especificar critérios para o atributo a atribuir automaticamente. Neste caso, o atributo *Equipamento corporativo* é atribuído pelo tipo de dispositivo.

O Kaspersky Security Center permite cancelar equipamento. Para isso, selecione a opção **Dispositivo com baixa efetuada** nas propriedades de um dispositivo. O dispositivo não é exibido na lista de equipamentos.

Um administrador pode gerenciar a lista de controladores lógicos programáveis (PLC) na pasta **Hardware**. As informações detalhadas sobre como gerenciar a lista PLC são fornecidas no *Guia do Usuário do Kaspersky Industrial CyberSecurity for Nodes*.

Adição de informações dobre novos dispositivos

Para adicionar informações sobre novos dispositivos na rede:

1. Na pasta **Repositórios** na árvore do console, selecione a subpasta **Hardware**.
2. No espaço de trabalho da pasta **Hardware**, clique no botão **Adicionar dispositivo** para abrir a janela **Novo dispositivo**.

   A janela **Novo dispositivo** se abre.

3. Na janela **Novo dispositivo**, na lista suspensa **Tipo**, selecione um tipo de dispositivo que pretende adicionar.

4. Clique em **OK**.

   A janela Propriedades do dispositivo é aberta na seção **Geral**.

5. Na seção **Geral**, preencha os campos de entrada com os dados do dispositivo. A seção **Geral** lista as seguintes configurações:

   - **Dispositivo corporativo**. Selecione a caixa de seleção se você quiser atribuir o atributo *Corporativo* ao dispositivo. Usando este atributo, você poderá procurar por dispositivos na pasta **Hardware**.

   - **Dispositivo com baixa efetuada**. Selecione a caixa de seleção se você não quiser que o dispositivo seja exibido na lista de dispositivos na pasta **Hardware**.

6. Clique em **Aplicar**.

O novo dispositivo será exibido no espaço de trabalho da pasta **Hardware**.

Configuração de critérios usados para definir dispositivos corporativos

Para configurar os critérios de detecção para dispositivos corporativos:

1. Na pasta **Repositórios** na árvore do console, selecione a subpasta **Hardware**.

2. No espaço de trabalho da pasta **Hardware**, clique no botão **Ações adicionais** e selecione **Configurar as regras para dispositivos corporativos** na lista suspensa.

   A janela de propriedades de hardware é aberta.

3. Na janela de propriedades de hardware, na seção **Dispositivos corporativos**, selecione um modo de atribuir o atributo *Corporativo* ao dispositivo:

   - **Configurar o atributo Dispositivo corporativo manualmente para o dispositivo**. O atributo *Hardware corporativo* é atribuído ao dispositivo manualmente na janela Propriedades do dispositivo, na seção **Geral**.

   - **Configurar o atributo Dispositivo corporativo automaticamente para o dispositivo**. No bloco de configurações **Por tipo de dispositivo**, especifique os tipos de dispositivo para os quais o aplicativo atribuirá automaticamente o atributo *Corporativo*.

     Essa opção afeta apenas os dispositivos adicionados por meio de sondagem de rede. Para os dispositivos adicionados manualmente, defina o atributo *Corporativo* manualmente.

4. Clique em **OK**.

Os critérios de detecção para dispositivos corporativos são configurados.

Configurar campos personalizados

Para configurar campos personalizados de dispositivos:

1. Na pasta **Repositórios** na árvore do console, selecione a subpasta **Hardware**.
2. No espaço de trabalho da pasta **Hardware**, clique no botão **Ações adicionais** e selecione **Configurar campos de dados personalizados** na lista suspensa.

   A janela de propriedades de hardware é aberta.
3. Na janela de propriedades do hardware, selecione a seção **Campos personalizados** e clique no botão **Adicionar**.

   A janela **Adicionar campo** se abre.
4. Na janela **Adicionar campo**, especifique o nome do campo personalizado que será exibido nas propriedades do hardware.

   Você pode criar múltiplos campos personalizados com nomes exclusivos para cada um.
5. Clique em **OK**.

Os campos personalizados que foram adicionados são exibidos na seção **Campos personalizados** das propriedades do hardware. Você pode usar campos personalizados para fornecer informações específicas sobre os dispositivos. Por exemplo, isto pode ser o número da ordem interna para uma compra de hardware.

Licenciamento

Esta seção fornece informações sobre os termos gerais relacionados à licença do Kaspersky Security Center 14.2.

Eventos do limite do licenciamento excedidos

O Kaspersky Security Center lhe permite obter informações sobre eventos quando alguns limites de licenciamento são excedidos pelos aplicativos Kaspersky instalados nos dispositivos cliente.

O nível de importância desses eventos, quando um limite de licenciamento é excedido, é definido de acordo com as seguintes regras:

- Se o número de unidades atualmente usadas cobertas por uma única licença estiver entre 90% e 100% do número total de unidades cobertas pela licença, o evento é publicado com o nível de importância **Informação**.
- Se o número de unidades atualmente usadas cobertas por uma única licença estiver entre 100% e 110% do número total de unidades cobertas pela licença, o evento é publicado com o nível de importância **Aviso**.
- Se o número de unidades atualmente usadas cobertas por uma licença exceder 110% do número total de unidades cobertas pela mesma licença, o evento será publicado com o nível de importância de **Evento crítico**.

Sobre o licenciamento

Esta seção contém informações sobre o licenciamento de aplicativos Kaspersky gerenciados pelo Kaspersky Security Center.

Sobre a licença

Uma *licença* é um direito com período de validade limitado para uso do Kaspersky Security Center, concedido nos termos do Contrato de Licença (Contrato de Licença de Usuário Final).

O escopo dos serviços e o período de validade dependem da licença sob a qual o aplicativo é utilizado.

São fornecidos os seguintes tipos de licença:

- *Avaliação*

  Uma licença gratuita concebida para experimentar o aplicativo. Uma licença de avaliação normalmente tem um prazo de validade curto.

  Quando a licença de avaliação expira, todos os recursos do Kaspersky Security Center são desativados. Para continuar usando o aplicativo, é necessário comprar a licença comercial.

  Você pode usar o aplicativo com uma licença de avaliação por apenas um período de avaliação.

- *Comercial*

  Uma licença paga.

  Quando uma licença comercial expira, os principais recursos do aplicativo são desativados. Para continuar usando o Kaspersky Security Center, é necessário renovar sua licença. Após a expiração de uma licença comercial, não é possível continuar usando o aplicativo e ele deve ser removido do dispositivo.

  Recomendamos a renovação da sua licença antes que ela expire para garantir a máxima proteção contra todas as ameaças à segurança.

Sobre o Contrato de Licença do Usuário Final

O Contrato de Licença do Usuário Final (Contrato de Licença ou EULA) é um contrato vinculativo entre você e a AO Kaspersky Lab que estipula os termos nos quais você pode usar o aplicativo.

Leia com atenção o seguinte Contrato de Licença antes de começar a usar o aplicativo.

O Kaspersky Security Center e seus componentes, por exemplo, Agente de Rede, têm seu próprio EULA.

Você pode visualizar os termos do Contrato de Licença do Usuário Final para o Kaspersky Security Center usando os seguintes métodos:

- Durante a instalação do Kaspersky Security Center.
- Lendo o documento license.txt incluído no kit de distribuição do Kaspersky Security Center.

- Lendo o documento license.txt presente na pasta de instalação do Kaspersky Security Center.
- Ao baixar o arquivo license.txt do site da Kaspersky.

É possível visualizar os termos do Contrato de Licença de Usuário Final para o Agente de Rede para Windows, Agente de Rede para Mac, Agente de Rede para Linux usando os seguintes métodos:

- Durante o download do pacote de distribuição do Agente de Rede a partir dos servidores web da Kaspersky.
- Durante a instalação do Agente de Rede para Windows, Agente de Rede para Mac ou Agente de Rede para Linux.
- Lendo o documento license.txt incluído no pacote de distribuição do Agente de Rede para Windows, Agente de Rede para Mac ou Agente de Rede para Linux.
- Lendo o documento license.txt na pasta de instalação do Agente de Rede para Windows, Agente de Rede para Mac ou Agente de Rede para Linux.
- Ao baixar o arquivo license.txt do site da Kaspersky.

Você aceita os termos do Contrato de Licença do Usuário Final confirmando que concorda com o Contrato de Licença do Usuário Final ao instalar o aplicativo. Se você não aceitar os termos do Contrato de Licença, cancele instalação do aplicativo e não o utilize.

Sobre o certificado de licença

O *Certificado de licença* é um documento que você recebe juntamente com um arquivo de chave ou um código de ativação.

Um certificado de licença contém as seguintes informações sobre a licença fornecida:

- ID da licença ou número do pedido
- Informações sobre o usuário ao qual foi concedida a licença
- Informações sobre o aplicativo que pode ser ativado com a licença fornecida
- Limite do número de unidades de licenciamento (por exemplo, dispositivos nos quais o aplicativo pode ser usado com uma licença fornecida)
- Data de início da validade da licença
- Data de expiração da licença ou período da licença
- Tipo de licença

Sobre a chave de licença

Chave de licença é a sequência de bits que você pode aplicar para ativar e usar o aplicativo de acordo com os termos do Contrato de Licença do Usuário Final. As chaves de licença são geradas pelos especialistas da Kaspersky.

Você pode adicionar uma chave de licença ao aplicativo usando um dos seguintes métodos: aplicando um *arquivo de chave* ou inserindo um *código de ativação*. A chave de licença é exibida na interface do aplicativo como uma sequência alfanumérica única após você a adicionar ao aplicativo.

A chave de licença pode estar bloqueada pela Kaspersky caso os termos do Contrato de Licença tenham sido violados. Se a chave de licença tiver sido bloqueada, você deve adicionar outra se desejar usar o aplicativo.

Uma chave de licença pode ser ativa ou adicional (ou reserva).

Uma *chave de licença ativa* é uma chave de licença que é atualmente usada pelo aplicativo. Uma chave de licença ativa pode ser adicionada para uma licença de avaliação ou comercial. O aplicativo não pode ter mais de uma chave de licença ativa.

Uma *chave de licença adicional (ou reserva)* é uma chave de licença que permite ao usuário utilizar o aplicativo, mas que não se encontra atualmente em uso. A chave de licença adicional torna-se automaticamente ativa quando a licença associada à chave atual expira. Uma chave de licença adicional pode ser adicionada somente se uma chave de licença atual tiver sido adicionada.

Uma chave de licença para uma licença de avaliação pode ser adicionada somente como um chave de licença atual. Uma chave de licença para uma licença de avaliação não pode ser adicionada como uma chave de licença adicional.

Sobre o arquivo de chave

Um *arquivo de chave* é um arquivo com a extensão .key fornecido a você pela Kaspersky. Os arquivos de chave se destinam a ativar o aplicativo adicionando uma chave de licença.

Você recebe o arquivo de chave pelo endereço de e-mail que especificou após comprar o Kaspersky Security Center, ou que utilizou para solicitar a versão de avaliação do Kaspersky Security Center.

Você não precisa se conectar aos servidores de ativação da Kaspersky para ativar o aplicativo com um arquivo de chave.

Você pode recuperar um arquivo de chave se ele tiver sido acidentalmente excluído. Você poderá precisar de um arquivo de chave para se registrar no Kaspersky CompanyAccount, por exemplo.

Para restaurar seu arquivo de chave, realize uma das seguintes ações:

- Entre em contato com o vendedor da licença.
- Receba um arquivo de chave através do site da Kaspersky usando o código de ativação.
- Exporte um arquivo de chave de licença de outro Servidor de Administração.

Sobre a assinatura

A *Assinatura para o Kaspersky Security Center* é um pedido para uso do aplicativo sob as configurações selecionadas (data de expiração da assinatura, número de dispositivos protegidos). Você pode registrar sua assinatura do Kaspersky Security Center com seu provedor de serviços (por exemplo, seu provedor de Internet). Uma assinatura pode ser renovada manualmente ou no modo automático; você também pode cancelá-la.

Uma assinatura pode ser limitada (por exemplo, um ano) ou ilimitada (sem uma data de expiração). Para continuar a usar o Kaspersky Security Center após uma assinatura limitada expirar, você precisa renová-la. Uma assinatura ilimitada é automaticamente renovada, caso tenha sido pré-paga ao provedor de serviços nas datas devidas.

Quando uma assinatura limitada expirar, um período adicional poderá lhe ser fornecido para efetuar a renovação durante o qual o aplicativo continua a funcionar. A disponibilidade e a duração do período de carência é definida pelo provedor de serviços.

Para usar o Kaspersky Security Center sob a assinatura, você precisa aplicar o código de ativação recebido do provedor de serviços.

Você pode aplicar um código de ativação diferente para o Kaspersky Security Center somente após sua assinatura expirar ou quando a cancelar.

Dependendo do provedor de serviços, o conjunto de ações possíveis para o gerenciamento da assinatura pode variar. O Provedor de Serviços não pode conceder nenhum período de carência para a renovação da assinatura, portanto o aplicativo perde sua funcionalidade.

Os códigos de ativação comprados sob a assinatura não podem ser usados para ativar versões anteriores do Kaspersky Security Center.

Ao usar o aplicativo sob a assinatura, o Kaspersky Security Center automaticamente tenta acessar o servidor de ativação em intervalos de tempo especificados até que a assinatura expire. Isso garante que as informações sobre a assinatura sejam sincronizadas com o servidor de ativação. Caso não seja possível acessar o servidor usando o DNS do sistema, o aplicativo usará os servidores DNS públicos. Você pode renovar sua assinatura no site do provedor de serviços.

É possível atualizar manualmente as informações sobre a assinatura, sem haver a necessidade de espera do Kaspersky Security Center acessar o servidor de ativação. Por exemplo, isso pode ser útil quando as configurações de assinatura forem alteradas.

Para atualizar manualmente as informações sobre a assinatura:

1. Na árvore do console, selecione a pasta **Licenças da Kaspersky**.
2. Clique em **Ações adicionais** e, na lista suspensa, selecione **Sincronizar configurações de assinatura com o servidor de licenciamento**.

As informações sobre a assinatura são atualizadas no servidor de ativação.

Sobre o código de ativação

Código de ativação é uma sequência única de 20 caracteres alfanuméricos. Você insere um código de ativação para adicionar uma chave de licença que ativa o Kaspersky Security Center. Você recebe o código de ativação através do endereço de e-mail que você especificou, após comprar o Kaspersky Security Center ou após fazer o pedido da versão de avaliação do Kaspersky Security Center.

Para ativar o aplicativo com um código de ativação, é necessário acesso à Internet para estabelecer a conexão com os servidores de ativação da Kaspersky. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos.

Se o aplicativo foi ativado com um código de ativação, o aplicativo em alguns casos envia solicitações regulares aos servidores de ativação da Kaspersky para verificar o status atual da chave de licença. Você precisa de fornecer o acesso à Internet ao aplicativo para ser possível enviar solicitações.

Se você perdeu seu código de ativação após instalar o aplicativo, entre em contato com o parceiro da Kaspersky do qual você comprou a licença.

Não é possível usar arquivos de chave para ativar aplicativos gerenciados; somente códigos de ativação são aceitos.

Revogando o consentimento com um Contrato de Licença do Usuário Final

Se decidir interromper a proteção dos dispositivos clientes, poderá desinstalar os aplicativos Kaspersky gerenciados e revogar o EULA (Contrato de Licença do Usuário Final) para esses aplicativos.

Para revogar o EULA dos aplicativos gerenciados da Kaspersky:

1. Na árvore do console, selecione **Administration Server** → **Advanced** → **Accepted EULAs**.

   É exibida uma lista de EULAs, aceitos ao criar pacotes de instalação, durante a instalação contínua de atualizações ou mediante implementação do Kaspersky Security for Mobile.

2. Na lista, selecione o EULA que deseja revogar.

   Você pode visualizar as seguintes propriedades da EULA:

   - Data em que o EULA foi aceito.
   - Nome do usuário que aceitou os termos da EULA.
   - Link para os termos da EULA.
   - Lista dos objetos conectados ao EULA: nomes de pacotes de instalação, nomes de atualizações contínuas, nomes de aplicativos móveis.

3. Clique no botão **Revoke EULA**.

   A janela aberta informa que você deve desinstalar o aplicativo Kaspersky que corresponde o EULA.

4. Clique no botão para confirmar a revogação.

   O Kaspersky Security Center verifica se os pacotes de instalação (que corresponde ao aplicativo da Kaspersky gerenciado à qual o EULA foi revogado) foram excluídos.

   Você pode revogar apenas o EULA de um aplicativo Kaspersky gerenciado, cujos pacotes de instalação foram excluídos.

A EULA foi revogada. Não está disponível na lista de EULAs na seção **Administration Server** → **Advanced** → **Accepted EULAs**. Você não pode proteger dispositivos cliente usando o aplicativo Kaspersky para o qual o EULA foi revogado.

Sobre a coleta de dados

Transferência de dados de terceiros

Ao usar a funcionalidade de Gerenciamento de Dispositivos Móveis do Software, com o objetivo de fornecer em tempo hábil os comandos para dispositivos que executam o sistema operacional Android por meio do sistema de notificação push, o serviço Google Firebase Cloud Messaging será usado. Se o Usuário configurou o uso do serviço Google Firebase Cloud Messaging, significa que aceita fornecer as seguintes informações ao serviço Google Firebase Cloud Messaging no modo automático: IDs de instalação dos aplicativos Kaspersky Endpoint Security for Android para os quais as notificações push devem ser enviadas.

Para bloquear a troca de informações com o serviço Google Firebase Cloud Messaging, o Usuário deve reverter as configurações de uso do serviço Google Firebase Cloud Messaging para seus valores de fábrica.

Ao usar a funcionalidade de Gerenciamento de Dispositivos Móveis do Software, com o objetivo de fornecer em tempo hábil os comandos para dispositivos que executam o sistema operacional iOS por meio do mecanismo de notificação push, o Apple Push Notification Service (APNs) será usado. Se o Usuário instalou um certificado de APNs em um servidor de MDM do iOS, criou um perfil de MDM do iOS com um conjunto de configurações para conexão dos dispositivos móveis iOS para o Software, e instalou este nos dispositivos móveis, o Usuário concorda em fornecer as seguintes informações para as APNs no modo automático:

- Token – Push token do dispositivo. O servidor usa este token quando está mandando notificações de push para o dispositivo.
- PushMagic – Um string que precisa ser incluído quando mandar notificações. O valor do string é gerado pelo dispositivo.

Dados processados localmente

O Kaspersky Security Center foi concebido para a execução centralizada de tarefas de administração e manutenção básicas na rede de uma organização. O Kaspersky Security Center fornece ao administrador o acesso a informações detalhadas sobre o nível de segurança da rede corporativa. A solução permite que o administrador configure todos os componentes de proteção criados com base nos aplicativos Kaspersky. O Kaspersky Security Center executa as seguintes funções principais:

- Detecção de dispositivos e seus usuários na rede da organização
- Criação de uma hierarquia de grupos administrativos para gerenciamento de dispositivos
- Instalação de aplicativos do Kaspersky nos dispositivos
- Gerenciamento de configurações e tarefas dos aplicativos instalados
- Gerenciamento de atualizações do Kaspersky e aplicativos de terceiros, busca e correções de vulnerabilidades
- Ativação de aplicativos Kaspersky nos dispositivos
- Como gerenciar contas de usuário

- Visualizando informações sobre a operação dos aplicativos do Kaspersky nos dispositivos
- Visualização de relatórios

Para desempenhar sua função principal, o Kaspersky Security Center pode receber, armazenar e processar as seguintes informações:

- Informações sobre os dispositivos na rede da organização recebidas como resultado da descoberta de dispositivos na rede do Active Directory ou na rede do Windows, ou por verificação de intervalos de IP. O Servidor de Administração obtém dados de forma independente ou recebe dados do Agente de Rede.
- Informações sobre as unidades organizacionais, domínios, usuários e grupos do Active Directory recebidos como resultado de uma descoberta de dispositivos na rede do Active Directory. O Servidor de Administração obtém dados de forma independente ou recebe dados do Agente de Rede.
- Detalhes dos dispositivos gerenciados. O Agente de Rede transfere os dados listados abaixo do dispositivo para o Servidor de Administração. O usuário digita o nome de exibição e a descrição do dispositivo na interface do Console de Administração ou na interface do Kaspersky Security Center Web Console:
    - Especificações técnicas dos dispositivos gerenciados e os componentes requeridos para identificação do dispositivo: nome e descrição do dispositivo, nome e tipo do domínio do Windows, nome do dispositivo no ambiente de Windows, o DNS, domínio e nome do DNS, endereço IPv4, endereço IPv6, local da rede, endereço de MAC, tipo de sistema operacional, se o sistema é virtual com tipo de hipervisor, e se o dispositivo e um sistema virtual dinâmico e parte de um VDI.
    - Outras especificações de dispositivos gerenciados e os componentes necessários para auditoria de dispositivos gerenciados e para tomar decisões especificas sobre atualizações e patches aplicáveis: status do Windows Update Agent (WUA), arquitetura do sistema operacional, fornecedor do sistema operacional, número da compilação do sistema operacional, ID da versão do sistema operacional, pasta de localização do sistema operacional, se o dispositivo for uma máquina virtual - o tipo de máquina virtual - o tipo de máquina virtual, o nome do Servidor de Administração virtual que gerencia o dispositivo, dados do dispositivo na nuvem (região da nuvem, VPC, zona de disponibilidade da nuvem, sub-rede da nuvem, zona de posicionamento da nuvem).
    - Detalhes de ações em dispositivos gerenciados: data e hora da ultima atualização, hora em que o dispositivo esteve visível na rede pela última vez, status de espera de reinício e hora em que o dispositivo foi ligado.
    - Detalhes das contas de usuário do dispositivo e as suas sessões.
- Estatísticas de operação do ponto de distribuição se o dispositivo for um ponto de distribuição. O Agente de Rede transfere os dados do dispositivo para o Servidor de Administração.
- Configurações do ponto de distribuição inseridas pelo usuário no Console de Administração ou no Kaspersky Security Center Web Console.
- Dados necessários para a conexão de dispositivos móveis ao Servidor de Administração: certificado, porta de conexão móvel, endereço de conexão do Servidor de Administração. O usuário insere os dados no Console de Administração ou no Kaspersky Security Center Web Console.

- Detalhes dos dispositivos móveis transferidos usando o protocolo de Exchange ActiveSync. Os dados listados abaixo são transferidos do dispositivo móvel para o Servidor de Administração:

  - Especificações técnicas do dispositivo móvel e seus componentes necessárias para identificação do dispositivo: nome do dispositivo, modelo, nome do sistema operacional, número do IMEI e número de telefone.

  - Especificações do dispositivo móvel e seus componentes: status de gerenciamento do dispositivo, suporte a SMS, permissão para enviar mensagens SMS, suporte a FCM, suporte a comandos do usuário, pasta de armazenamento do sistema operacional e nome do dispositivo.

  - Detalhes das atividades de dispositivos móveis: localização do dispositivo (através do comando Localizar), hora da última sincronização, hora da última conexão com o Servidor de Administração e detalhes de suporte a sincronização.

- Detalhes dos dispositivos móveis transferidos usando o protocolo MDM do iOS. Os dados listados abaixo são transferidos do dispositivo móvel para o Servidor de Administração:

  - Especificações técnicas do dispositivo móvel e seus componentes necessárias para identificação: nome do dispositivo, modelo, nome e número de compilação do sistema operacional, número do modelo do dispositivo, IMEI, UDID, MEID, número de série, quantidade de memória, versão do firmware do modem, endereço MAC do Bluetooth, endereço MAC da Wi-Fi e detalhes do cartão SIM (ICCID como parte do ID do cartão SIM).

  - Detalhes da rede móvel usada pelo dispositivo gerenciado: tipo de rede móvel, nome da rede móvel utilizada atualmente, nome da rede móvel doméstica, versão das configurações da operadora de rede móvel, status de roaming de voz, status de roaming de dados, código do país da rede doméstica, código do país de residência, código da rede atualmente em uso e nível de criptografia.

  - Configurações de segurança do dispositivo móvel: o uso de senha e respectiva conformidade com as configurações da política, lista de perfis de configuração e perfis de provisionamento usados para instalação de aplicativos de terceiros.

  - Data da última sincronização com o Servidor de Administração e status de gerenciamento de dispositivos.

- Detalhes dos aplicativos da Kaspersky instalados no dispositivo. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede:

  - Configurações dos aplicativos instalados no dispositivo gerenciado: nome e versão do aplicativo do Kaspersky, status, proteção em tempo real, data e hora de escaneamento do ultimo dispositivo, numero de ameaças detectadas, numero de objetos que falharam na detecção, disponibilidade e status dos componentes do aplicativo, hora do ultima atualização e versão do banco de dados de antivírus, detalhes das configurações e tarefas do aplicativo do Kaspersky, informações sobre as chaves de licença ativa e da reserva, a data e hora da instalação e o ID.

  - Estatística da operação de aplicativo: eventos relacionados a alterações no status dos componentes do aplicativo da Kaspersky no dispositivo gerenciado e desempenho de tarefas iniciadas pelos componentes de software.

  - Status do dispositivo definido pelo aplicativo do Kaspersky.

  - Marcações feitas por o aplicativo do Kaspersky.

  - Conjunto de atualizações instaladas pare o aplicativo do Kaspersky.

- Dados contidos em eventos dos componentes do Kaspersky Security Center e aplicativos gerenciados Kaspersky. O Agente de Rede transfere os dados do dispositivo para o Servidor de Administração.

- Dados necessários para a integração do Kaspersky Security Center com um sistema SIEM para exportação de eventos. O usuário insere os dados no Console de Administração ou no Kaspersky Security Center Web Console.

- Configurações dos componentes do Kaspersky Security Center e aplicativos gerenciados do Kaspersky estão nas politicas e nos perfis das politicas. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Configurações de tarefas dos componentes do Kaspersky Security Center e aplicativos gerenciados do Kaspersky. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Dados processados pelo recurso de Gerenciamento de patches e vulnerabilidades. O Agente de Rede transfere os dados listados abaixo do dispositivo para o Servidor de Administração:

  - Detalhes sobre aplicativos e patches instalados nos dispositivos gerenciados (Registro de aplicativos).

  - Informações sobre hardware detectado em dispositivos gerenciados (Registro de Aplicativos).

  - Detalhes sobre vulnerabilidades em aplicativos de terceiros nos dispositivos gerenciados.

  - Detalhes sobre atualizações de aplicativos de terceiros instalados em dispositivos gerenciados.

  - Detalhes sobre atualizações da Microsoft e detectados por a função WSUS.

  - Lista de atualizações da Microsoft encontradas pelo recurso WSUS que devem ser instaladas no dispositivo.

- Dados necessários para baixar atualizações no Servidor de Administração isolado para corrigir vulnerabilidades de softwares de terceiros em dispositivos gerenciados. O usuário insere e transmite dados usando o utilitário klscflag do Servidor de Administração.

- Dados necessários para o trabalho do Kaspersky Security Center com os ambientes de nuvem (Amazon Web Services, Microsoft Azure, Google Cloud, Yandex Cloud). O usuário insere os dados no Console de Administração ou no Kaspersky Security Center Web Console.

- Categorias de usuários de aplicativos. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Detalhes de arquivos executáveis detectados em dispositivos gerenciados pelo recurso de Controle de Aplicativos. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Detalhes sobre arquivos colocados em Backup. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Detalhes sobre arquivos colocados em quarentena. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Detalhes sobre arquivos requisitados por os especialistas da Kaspersky para análise detalhadas. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Detalhes sobre status e ativação de Controle de regras das Anomalias Adaptivas. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Detalhes sobre dispositivos externos (unidades de memória, ferramentas de transferência de informações, ferramentas cópia impressa de informações e conexões de buses) instalados ou conectados ao dispositivo gerenciado e detectados pelo recurso de Controle de Dispositivos. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Informações sobre dispositivos criptografados e o status da criptografia. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede.

- Detalhes sobre erros de dados criptografia feitos em dispositivos usando a função Criptografia de Dados dos aplicativos do Kaspersky. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Lista de controladores lógicos programáveis (PLCs) gerenciados. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Dados necessários para a criação de uma cadeia de desenvolvimento de ameaças. O aplicativo gerenciado transfere dados do dispositivo para o Servidor de Administração através do Agente de Rede. A lista completa de dados e providenciado nos arquivos de Ajuda do aplicativo correspondente.

- Dados necessários para a integração do Kaspersky Security Center ao serviço Kaspersky Managed Detection and Response (o plugin dedicado deve ser instalado para o Kaspersky Security Center Web Console): token de iniciação de integração, token de integração e token de sessão do usuário. O Usuário insere os dados na interface do Kaspersky Security Center Web Console. O serviço Kaspersky MDR transfere o token de integração e o token de sessão do usuário por meio do plugin dedicado.

- Detalhes dos códigos de ativação inseridos ou arquivos de chave especificados. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Contas de usuário: nome, descrição, nome completo, endereço de e-mail, número de telefone principal, senha, chave secreta gerada pelo Servidor de Administração e senha única para verificação em duas etapas. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Dados que o Gerenciador de Identidade e Acesso precisa para a autenticação centralizada e para fornecer login único (SSO) entre os aplicativos da Kaspersky integrados ao Kaspersky Security Center: definições de instalação e configuração do Gerenciador de Identidade e Acesso, sessão de usuário do Gerenciador de Identidade e Acesso, tokens do Gerenciador de Identidade e Acesso, status do aplicativo cliente e status do servidor de recursos. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Revisão de histórico de objetos gerenciados excluídos. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Registro de objetos gerenciados excluídos. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Pacotes de instalação criados dos arquivos e configurações de instalações. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Dados necessários para a exibição de informativos da Kaspersky no Kaspersky Security Center Web Console. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Dados necessários para o funcionamento de plugins de aplicativos gerenciados no Kaspersky Security Center Web Console e salvos pelos plugins no banco de dados do Servidor de Administração durante sua operação de rotina. A descrição e formas de fornecer os dados são fornecidas nos arquivos de Ajuda do aplicativo correspondente.

- Configurações de usuário do Kaspersky Security Center Web Console: idioma de localização e tema da interface, configurações de exibição do painel de monitoramento, informações sobre o status das notificações (Já lidas/Ainda não lidas), status das colunas nas planilhas (Mostrar/Ocultar), Modo de treinamento progresso. O usuário insere dados na interface do Kaspersky Security Center Web Console.

- Log de Eventos Kaspersky para os componentes do Kaspersky Security Center e aplicativos gerenciados Kaspersky. O Log de eventos Kaspersky é armazenado em cada dispositivo e nunca é transferido para o Servidor de Administração.

- Certificados de comunicação segura com dispositivos gerenciados e componentes do Kaspersky Security Center. O usuário insere dados na interface do Console de Administração ou do Kaspersky Security Center Web Console.

- Dados necessários para a operação do Kaspersky Security Center em ambientes de nuvem, como Amazon Web Services (AWS), Microsoft Azure, Google Cloud e Yandex.Cloud. O Servidor de Administração recebe os dados da máquina virtual na qual é executado.

- Informações sobre a aceitação do Usuário dos termos e condições dos acordos legais com a Kaspersky.

- Os dados do Servidor de Administração que o usuário insere nos seguintes componentes:

  - Console de Administração

  - Kaspersky Security Center Web Console

  - Terminal de linha de comando ao usar o utilitário klscflag

  - Componentes que interagem com o Servidor de Administração por meio de objetos de automação klakaut e Kaspersky Security Center OpenAPI

- Qualquer dado que o usuário inserir no Console de Administração ou na interface do Kaspersky Security Center Web Console.

Os dados listados acima podem estar presentes no Kaspersky Security Center se um dos seguintes métodos é aplicado:

- O usuário insere os dados na interface dos seguintes componentes:
  - Console de Administração
  - Kaspersky Security Center Web Console
  - Terminal de linha de comando ao usar o utilitário klscflag
  - Componentes que interagem com o Servidor de Administração por meio de objetos de automação klakaut e Kaspersky Security Center OpenAPI
- O Agente de Rede automaticamente recebe dados do dispositivo e os transfere para o Servidor de Administração.
- O Agente de Rede recebe extração de dados por o aplicativo gerenciado do Kaspersky e transfere para o Servidor de Administração. A lista de dados processados por aplicativos gerenciados do Kaspersky são providenciados nos arquivos de Ajuda para os aplicativos correspondentes.
- O servidor de administração obtém informações sobre dispositivos em rede de forma independente ou recebe informações de um Agente de Rede que atua como um ponto de distribuição.
- Os dados são transferidos do dispositivo móvel para o Servidor de Administração usando o protocolo Exchange ActiveSync ou MDM do iOS.

Os dados são armazenados no banco de dados do Servidor de Administração. Os nomes de usuários e as senhas são armazenados em formato criptografado.

Todos os dados listados acima podem ser transferidos para a Kaspersky apenas através de arquivos de dumping, arquivos de rastreamento ou arquivos de log dos componentes do Kaspersky Security Center, inclusive arquivos de log criados por instaladores e utilitários.

Arquivos de dumping, arquivos de rastreamento e arquivos de log dos componentes do Kaspersky Security Center contêm dados aleatórios do Servidor de Administração, Agente de Rede, Console de Administração, Servidor de MDM do iOS, Servidor de dispositivos móveis e Kaspersky Security Center Web Console. Esses arquivos podem conter dados pessoais e confidenciais. Arquivos de dumping, arquivos de rastreamento e arquivos de log são armazenados no dispositivo em forma não criptografada. Os arquivos de dumping e de rastreamento não são transferidos para a Kaspersky automaticamente; contudo, o administrador pode transferir dados para a Kaspersky manualmente mediante solicitação do Suporte Técnico para resolver problemas na operação do Kaspersky Security Center.

Seguindo os links no Console de Administração ou Kaspersky Security Center Web Console, o usuário concorda com a transferência automática dos seguintes dados:

- Código do Kaspersky Security Center
- Versão do Kaspersky Security Center
- Localização do Kaspersky Security Center
- ID da licença

- Tipo de licença
- Se a licença foi adquirida por meio de um parceiro

A lista de dados fornecida via cada link depende da finalidade e da localização do link.

A Kaspersky usa a informação recebida de forma anônima e somente como estatística geral. O resumo das estatísticas é gerado automaticamente através da informação original recebida e não contem qualquer dado pessoal ou confidencial. Assim que os dados novos são acumulados, os dados anteriores são excluídos (uma vez por ano). As estatísticas sumarizadas são armazenadas por tempo indeterminado.

A Kaspersky protege todas as informações recebidas, seguindo as leis e regras aplicáveis da Kaspersky. Os dados são transmitidos através de um canal seguro.

Opções de licença do Kaspersky Security Center

O Kaspersky Security Center pode funcionar nos seguintes modos:

- **Sem licença (funcionalidade básica)**

  O Kaspersky Security Center funciona nesse modo antes que o aplicativo seja ativado ou após a licença comercial expirar. O Kaspersky Security Center com suporte para a funcionalidade básica do Console de Administração é fornecido como parte dos aplicativos da Kaspersky para proteção de redes corporativas. Também pode baixá-lo pelo site da Kaspersky.

- **Licença comercial**

  Caso necessite de uma funcionalidade adicional não incluída na funcionalidade básica do Console de Administração, será necessário comprar uma licença comercial.

  Ao adicionar uma chave de licença na janela de propriedades do Servidor de Administração, certifique-se de adicionar uma chave de licença que permite usar o Kaspersky Security Center. Você pode encontrar essas informações no site da Kaspersky. Cada página da web da solução contém a lista de aplicativos incluídos nela. O Servidor de Administração pode aceitar chaves de licença não compatíveis, por exemplo, uma chave de licença do Kaspersky Endpoint Security Cloud, mas essas chaves de licença não fornecem novos recursos além da funcionalidade básica do Console de Administração.

Recurso ou propriedade	Mode de operação do Kaspersky Security Center	
	Sem licença	Licença comercial
Funcionalidade básica do Console de Administração As seguintes funções estão disponíveis: • Criação de Servidores de Administração virtuais para gerenciar uma rede de escritórios remotos ou organizações clientes • Criação de uma hierarquia de grupos de administração para gerenciar dispositivos específicos como uma entidade única • Instalação remota de aplicativos • Configuração centralizada de aplicativos instalados em dispositivos cliente • Controle do status de segurança antivírus de uma organização • Gerenciamento de funções do usuário • Estatísticas e relatórios sobre a operação do aplicativo assim como notificações sobre eventos críticos • Operações centralizadas com arquivos que foram movidos para a Quarentena e Backup e arquivos cujo processamento foi adiado • Criptografia e gerenciamento de proteção de dados • Exibir e editar grupos de aplicativos licenciados existentes • Visualização e edição manual da lista de componentes de hardware detectados pela sondagem da rede • Visualização da lista de imagens do sistema operacional disponíveis para instalação remota	✓	✓
Gerenciamento de patches e vulnerabilidades: funcionalidade básica	✓	✓

Recurso ou propriedade	Mode de operação do Kaspersky Security Center	
	Sem licença	Licença comercial
As seguintes tarefas não exigem uma licença comercial: • A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* Através dessa tarefa, o Kaspersky Security Center recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para o software de terceiros instalado nos dispositivos gerenciados. • A tarefa *Instalar as atualizações do Windows Update* Esta tarefa é usada para instalar apenas atualizações do Windows Update. Para usar essa tarefa, é necessário especificar manualmente as atualizações requeridas nas configurações da tarefa. • A tarefa *Corrigir vulnerabilidades* A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para softwares de terceiros. Para usar essa tarefa, é necessário especificar manualmente as correções do usuário para vulnerabilidades nas configurações da tarefa.		
Gerenciamento de patches e vulnerabilidades: funcionalidade avançada As seguintes funções estão disponíveis: • Instalação remota de atualizações de software e correção de vulnerabilidades automaticamente, de acordo com as regras definidas. • Uso do Servidor de Administração como o servidor Windows Server Update Services (WSUS) para fornecer atualizações para os serviços Windows Update em dispositivos no modo centralizado e com a frequência definida.	–	✓

Recurso ou propriedade	Mode de operação do Kaspersky Security Center	
	Sem licença	Licença comercial
Recurso de Gerenciamento de Dispositivos Móveis no Console de Administração baseado em MMC O recurso de Gerenciamento de Dispositivos Móveis é usado gerenciar dispositivos móveis Exchange ActiveSync (EAS) e MDM do iOS. As seguintes funções estão disponíveis para dispositivos móveis Exchange ActiveSync: • Adicionando novos dispositivos sob o gerenciamento do Kaspersky Security Center. • Criação e edição de perfis de gerenciamento de dispositivos móveis, atribuição de perfis a caixas de correio de usuários. • A configuração de dispositivos móveis (sincronização de e-mail, utilização de aplicativos, senha do usuário, criptografia de dados, conexão de unidades removíveis). • Instalação de certificados em dispositivos móveis. As seguintes funções estão disponíveis para dispositivos MDM do iOS: • Adicionando novos dispositivos sob o gerenciamento do Kaspersky Security Center. • Criar e editar de perfis de configuração, e instalar perfis de configuração em dispositivos móveis. • Instalar aplicativos em dispositivos móveis através da App Store® ou usando arquivos manifest (.plist). • Bloquear de dispositivos móveis, redefinir a senha do dispositivo móvel e excluir todos os dados do dispositivo móvel. As seguintes funções estão disponíveis para dispositivos Android: • Adicionando novos dispositivos sob o gerenciamento do Kaspersky Security Center. • Gerenciando o Kaspersky Endpoint Security for Android por meio da política. Além disso, o Gerenciamento de Dispositivos Móveis permite executar comandos fornecidos por protocolos relevantes. A unidade de gerenciamento da funcionalidade de gerenciamento de dispositivos móveis é o dispositivo móvel. Um dispositivo móvel é considerado gerenciado, uma vez que conecta a um servidor de dispositivos móveis.	–	✓ (Uma chave de licença deve ser adicionada nas propriedades do Servidor de Administração.)

Recurso ou propriedade	Mode de operação do Kaspersky Security Center	
	Sem licença	Licença comercial
Proteção de dispositivo móvel no Kaspersky Security Center Web Console O Kaspersky Security Center Web Console fornece os seguintes recursos para gerenciar dispositivos móveis Android e iOS: • Adicionando novos dispositivos sob o gerenciamento do Kaspersky Security Center. • Gerenciando o Kaspersky Endpoint Security for Android e Kaspersky Security for iOS por meio da política. • Enviando comandos para os dispositivos móveis por meio dos protocolos pertinentes e executando os comandos.	–	✓ (Uma chave de licença deve ser adicionada em cada dispositivo móvel.)
Gerenciamento do sistema As seguintes funções estão disponíveis: • Instalação de sistemas operacionais e aplicativos. O Kaspersky Security Center permite criar imagens de sistemas operacionais e implementá-los em dispositivos cliente na rede, assim como executar a instalação remota de aplicativos Kaspersky ou de outros fornecedores. Você pode capturar imagens de sistemas operacionais de dispositivos e transferi-las para o Servidor de Administração. Essas imagens de sistemas operacionais são armazenadas no Servidor de Administração em uma pasta dedicada. A imagem do sistema operacional de um dispositivo de referência é capturada e então criada através de uma tarefa de criação de pacote de instalação. Você pode usar as imagens recebidas para implementar em novos dispositivos na rede nos quais ainda não foi instalado nenhuma sistema operacional. Nesse caso, é usada uma tecnologia denominada Preboot eXecution Environment (PXE). • Gerenciamento do grupo de aplicativos licenciados. • Permissão remota de conexão aos dispositivos cliente através de um componente do Microsoft® Windows® denominado Remote Desktop Connection. • Conexão remota aos dispositivos cliente através do Windows Desktop Sharing. • Conexão remota por meio do **Visualizador da sessão do Kaspersky Remote Desktop**.	–	✓

Recurso ou propriedade	Mode de operação do Kaspersky Security Center	
	Sem licença	Licença comercial
Integração com ambientes em nuvem O Kaspersky Security Center trabalha com dispositivos locais e ainda oferece recursos especiais para trabalhar em um ambiente de nuvem, como o Assistente de Configuração de Ambiente em Nuvem. O Kaspersky Security Center funciona nas seguintes maquinas: • Instâncias do Amazon EC2 • Maquinas virtuais do Microsoft Azure • Instâncias das maquinas virtuas do Google Cloud • Máquinas virtuais Yandex.Cloud	–	✓
Exportando eventos para sistemas SIEM: uso do protocolo Syslog Usando o protocolo Syslog, você pode encaminhar qualquer evento que ocorre no Servidor de Administração do Kaspersky Security Center e em aplicativos Kaspersky que são instalados em dispositivos gerenciados. O protocolo Syslog é um protocolo de registro de mensagem padrão. É possível usá-lo para exportar os eventos para qualquer sistema SIEM.	✓	✓

Recursos de Licenças do Kaspersky Security Center e aplicativos gerenciados

As Licenças do Servidor de Administração e aplicativos gerenciados envolvem o seguinte:

- Você pode adicionar uma arquivo de chave licença ou um código de ativação válido a um Servidor de Administração para ativar o Gerenciamento de patches e vulnerabilidades, o Gerenciamento de Dispositivo Móveis ou a Integração com sistemas SIEM. Alguns recursos do Kaspersky Security Center só podem ser acessados dependendo dos arquivos de chave ativa ou códigos de ativação válidos adicionados ao Servidor de Administração.
- Você pode adicionar múltiplos códigos de ativação e arquivos de chave para aplicativos gerenciados ao repositório do Servidor de Administração.

Sobre o licenciamento do Kaspersky Security Center

Se você ativou um dos recursos gerenciados (por exemplo, o Gerenciamento de Dispositivos Móveis) usando um arquivo de chave, mas também quer usar outro recurso gerenciado (por exemplo, o Gerenciamento de patches e vulnerabilidades), deverá comprar do seu provedor de serviços um arquivo de chave para ativar ambos esses recursos e deverá ativar o Servidor de Administração usando este arquivo de chave.

Recursos de licenciamento de aplicativos gerenciados

Para o licenciamento de aplicativos gerenciados, um código de ativação ou um arquivo de chave pode ser implementado automaticamente ou de qualquer outro modo conveniente. Os seguintes métodos podem ser aplicados para implementar um código de ativação ou um arquivo de chave:

- Implementação automática

  > Se você usar aplicativos gerenciados diferentes e precisa implementar um arquivo de chave ou código de ativação específico para dispositivos, opte por outras formas de implementar aquele código de ativação ou arquivo de chave.

  O Kaspersky Security Center lhe permite implementar automaticamente as chaves de licença disponíveis nos dispositivos. Por exemplo, três chaves de licença são armazenadas no repositório do Servidor de Administração. Se você selecionou a caixa de seleção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados** para todas as três chaves de licença. Um aplicativo de segurança da Kaspersky – por exemplo, Kaspersky Endpoint Security for Windows – é instalado nos dispositivos da organização. Um novo dispositivo é descoberto, no qual uma chave de licença deve ser implementada. O aplicativo determina, por exemplo, que duas das chaves de licença do repositório podem ser aplicadas ao dispositivo: a chave de licença denominada *Key_1* e chave de licença denominada *Key_2*. Uma destas chaves de licença é implementada no dispositivo. Neste caso, não pode ser previsto qual das duas chaves de licença será implementada no dispositivo, porque a implementação automática de chaves de licença não é fornecida para nenhuma atividade do administrador.

  Quando uma chave de licença é implementada, os dispositivos são recontados para aquela chave de licença. Você deve assegurar-se de que o número de dispositivos nos quais a chave de licença foi implementada não excede o limite da licença. Se o número de dispositivos exceder o limite de licença, todos os dispositivos que não foram cobertos pela licença serão terão o status *Crítico* atribuído.

- Adicionando um arquivo de chave ou código de ativação ao pacote de instalação de um aplicativo gerenciado

  Se você instalar um aplicativo gerenciado usando um pacote de instalação, poderá especificar um código de ativação ou um arquivo de chave neste pacote de instalação ou na política do aplicativo. A chave de licença será implementada nos dispositivos gerenciados no momento da próxima sincronização do dispositivo com o Servidor de Administração.

- Implementação através da tarefa de adicionar uma chave de licença para um aplicativo gerenciado

  Se você optar por usar a tarefa de Adicionar chave de licença para um aplicativo gerenciado, poderá selecionar a chave de licença que deve ser implementada nos dispositivos e selecionar os dispositivos de qualquer forma conveniente – por exemplo, selecionando um grupo de administração ou uma seleção de dispositivos.

- Adicionar um código de ativação ou um arquivo de chave manualmente nos dispositivos

Aplicativos da Kaspersky. Implementação centralizada

Esta seção descreve os métodos para a instalação remota de aplicativos Kaspersky e a sua remoção dos dispositivos em rede.

> Antes de implementar aplicativos em dispositivos cliente, certifique-se de que o hardware e o software destes dispositivos cliente atendem aos requisitos aplicáveis.

O Agente de Rede é um componente que fornece a conexão do Servidor de Administração com dispositivos de cliente. Portanto, o Agente de Rede deve ser instalado em cada dispositivo cliente para ser conectado ao sistema de controle centralizado remoto. O dispositivo no qual o Servidor de Administração está instalado somente pode usar a versão de servidor do Agente de Rede. Esta versão está incluída no Servidor de Administração como uma parte que é instalada e removida junto com ele. Você não precisa instalar o Agente de Rede naquele dispositivo.

O Agente de Rede pode ser instalado remotamente ou localmente, como qualquer outro aplicativo. Durante a implementação centralizada de aplicativos de segurança através do Console de Administração, você pode instalar o Agente de Rede junto com esses aplicativos de segurança.

Os Agentes de Rede podem diferir dependendo dos aplicativos Kaspersky com os quais eles funcionam. Em alguns casos, o Agente de Rede pode ser instalado somente localmente (para obter os detalhes consulte a documentação para os aplicativos correspondentes). É preciso somente instalar o Agente de Rede em um dispositivo cliente uma vez.

Os aplicativos da Kaspersky são gerenciados através do Console de Administração usando plug-ins de gerenciamento. Portanto, para acessar a interface de gerenciamento de aplicativos através do Kaspersky Security Center, o plugin de gerenciamento correspondente deve ser instalado na estação de trabalho do administrador.

Você pode executar uma instalação remota de aplicativos a partir da estação de trabalho do administrador na janela principal do Kaspersky Security Center.

Para instalar software remotamente, você deve criar uma tarefa de instalação remota.

A tarefa criada para a instalação remota começará de acordo com seu agendamento. Você pode interromper o procedimento de instalação ao parar a tarefa manualmente.

Caso ocorra um erro na instalação remota de um aplicativo, certifique-se de que foi realizada a preparação necessária do dispositivo.

Você pode acompanhar o andamento da instalação remota de aplicativos Kaspersky em uma rede usando o relatório de implementação.

Para obter os detalhes sobre o gerenciamento dos aplicativos listados no Kaspersky Security Center, consulte a documentação para os aplicativos correspondentes.

Substituição de aplicativos de segurança de terceiros

A Instalação de aplicativos de segurança da Kaspersky através do Kaspersky Security Center pode necessitar a remoção de software de terceiros incompatível com o aplicativo sendo instalado. O Kaspersky Security Center fornece vários modos de remover os aplicativos de terceiros.

Remoção de aplicativos incompatíveis usando o instalador

Esta opção está disponível no Console de Administração com base no Console de Gerenciamento Microsoft.

O método do instalador de remoção de aplicativos incompatíveis tem suporte em vários tipos de instalação. Antes da instalação do aplicativo de segurança, todos os aplicativos incompatíveis são removidos automaticamente se a janela de propriedades do pacote de instalação deste aplicativo de segurança (seção **Aplicativos incompatíveis**) tiver a opção **Desinstalar automaticamente aplicativos incompatíveis** selecionada.

Remoção de aplicativos incompatíveis ao configurar a instalação remota de um aplicativo

Você pode ativar a opção **Desinstalar automaticamente aplicativos incompatíveis** ao configurar a instalação remota de um aplicativo de segurança. No Console de Administração com base no Console de Gerenciamento Microsoft (MMC), esta opção está disponível no Assistente de instalação remota. No Kaspersky Security Center Web Console, você pode encontrar essa opção no Assistente de implementação da proteção. Quando esta opção está ativada, o Kaspersky Security Center remove aplicativos incompatíveis antes de instalar um aplicativo de segurança em um dispositivo gerenciado.

Instruções de como proceder:

- Console de Administração: Remoção de aplicativos com o uso do Assistente de Instalação Remota
- Kaspersky Security Center Web Console: Remover aplicativos incompatíveis antes da instalação

Remover aplicativos incompatíveis através de uma tarefa dedicada

Para remover aplicativos incompatíveis, use a tarefa **Desinstalar o aplicativo remotamente**. Esta tarefa deve ser executada nos dispositivos antes da execução da tarefa de instalação do aplicativo de segurança. Por exemplo, na tarefa de instalação, você pode selecionar o tipo de agendamento **Na conclusão de outra tarefa** onde a outra tarefa for **Desinstalar o aplicativo remotamente**.

Este método da desinstalação é útil quando o instalador do aplicativo de segurança não puder remover apropriadamente um aplicativo incompatível.

Instruções do Console de Administração: Criando uma tarefa.

Instalação de aplicativos usando a tarefa de instalação remota

O Kaspersky Security Center permite instalar aplicativos em dispositivos remotamente, usando tarefas de instalação remotas. Essas tarefas são criadas e atribuídas aos dispositivos por um assistente dedicado. Para atribuir uma tarefa com mais rapidez e facilidade, é possível especificar dispositivos (até mil) na janela do assistente de uma das seguintes formas:

- **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**. Neste caso, a tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.
- **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**. Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

- **Atribuir a tarefa a uma seleção de dispositivos**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em uma seleção anteriormente criada. É possível especificar a seleção predefinida ou uma personalizada criada por você.

- **Atribuir tarefa a um grupo de administração**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em um grupo de administração anteriormente criado.

Para evitar problemas que possam ocorrer durante a instalação do aplicativo em um dispositivo cliente sem o Agente de Rede instalado, é necessário agir conforme o descrito no procedimento de implementação forçada por meio da tarefa de instalação remota do Kaspersky Security Center.

Instalar um aplicativo nos dispositivos selecionados

Para instalar um aplicativo nos dispositivos selecionados:

1. Na árvore do console, selecione a pasta **Tarefas**.

2. Execute a criação da tarefa, clicando no botão **Criar uma tarefa**.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

   Na janela **Selecionar o tipo de tarefa** do assistente para novas tarefas, no nó **Servidor de Administração do Kaspersky Security Center**, selecione **Instalar o aplicativo remotamente** como o tipo de tarefa.

   O Assistente para novas tarefas cria uma tarefa de instalação remota do aplicativo selecionado para dispositivos específicos. A tarefa recém criada é exibida no espaço de trabalho da pasta **Tarefas**.

3. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação especificada nas configurações da tarefa.

Após a conclusão da tarefa de instalação remota, o aplicativo selecionado será instalado nos dispositivos selecionados.

Instalação de um aplicativo em dispositivos cliente em um grupo de administração

Para instalar um aplicativo nos dispositivos cliente em um grupo de administração:

1. Estabeleça uma conexão ao Servidor de Administração que controla o grupo de administração relevante.

2. Selecione um grupo de administração na árvore do console.

3. No espaço de trabalho do grupo, selecione a guia **Tarefas**.

4. Execute a criação da tarefa, clicando no botão **Criar uma tarefa**.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

   Na janela **Selecionar o tipo de tarefa** do assistente para novas tarefas, no nó **Servidor de Administração do Kaspersky Security Center**, selecione **Instalar o aplicativo remotamente** como o tipo de tarefa.

   O Assistente para novas tarefas cria uma tarefa de grupo de instalação remota do aplicativo selecionado. A nova tarefa é exibida no espaço de trabalho do grupo de administração na guia **Tarefas**.

5. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação especificada nas configurações da tarefa.

Após a conclusão da tarefa de instalação remota, o aplicativo selecionado será instalado nos dispositivos cliente no grupo de administração.

Instalar um aplicativo usando as políticas de grupo do Active Directory

O Kaspersky Security Center permite instalar os aplicativos Kaspersky em dispositivo gerenciados, usando as políticas de grupo do Active Directory.

Você pode instalar aplicativos usando as políticas de grupo do Active Directory apenas dos pacotes de instalação que incluam Agente de Rede.

Para instalar um aplicativo usando as políticas de grupo do Active Directory:

1. Comece a configurar a instalação do aplicativo usando o Assistente de instalação remota.
2. Na janela **Definir configurações da tarefa de instalação remota** do Assistente de instalação remota, marque a opção **Atribuir a instalação do pacote em políticas de grupo do Active Directory**.
3. Na janela **Selecionar contas para acessar os dispositivos** do Assistente de instalação remota, selecione a opção **Conta necessária (Agente de Rede não é usado)**.
4. Adicionar a conta com privilégios de administrador no dispositivo onde o Kaspersky Security Center é instalado ou na conta incluída no grupo de domínio Proprietários do criador de política de grupo.

5. Conceda as permissões para a conta selecionada:

    a. Acesse **Painel de Controle** → **Ferramentas Administrativas** e abra **Gerenciamento de Política de Grupo**.

    b. Clique no nó com o domínio desejado.

    c. Clique na seção **Delegação**.

    d. Na lista suspensa de **Permissão**, selecione **Vincular GPOs**.

    e. Clique em **Adicionar**.

    f. Na janela aberta **Selecionar usuário, computador ou grupo**, selecione a conta desejada.

    g. Clique em **OK** para fechar a janela **Selecionar usuário, computador ou grupo**.

    h. Na lista **Grupos e usuários**, selecione a conta recém-adicionada, depois clique em **Avançado** → **Avançado**.

    i. Na lista **Entradas de permissão**, clique duas vezes na conta recém-adicionada.

    j. Conceda as seguintes permissões:

    - **Criar objetos de grupo**
    - **Excluir objetos de grupo**
    - **Criar objetos de contêiner de política de grupo**
    - **Excluir objetos de contêiner de política de grupo**

    k. Clique em **OK** para salvar as alterações.

6. Defina outras configurações seguindo as instruções do assistente.

7. Execute manualmente a tarefa de instalação remota criada ou aguarde pelo seu início programado.

Isto inicia a seguinte sequência de instalação remota:

1. Quando a tarefa estiver em execução, os seguintes objetos são criados em cada domínio que inclui os quaisquer dispositivos cliente do conjunto especificado:

    - Objeto da política de grupo (GPO) sob o nome **Kaspersky_AK{GUID}**.
    - Um grupo de segurança que corresponde à GPO. Esse grupo de segurança inclui dispositivos cliente abrangidos pela tarefa. O conteúdo do grupo de segurança define o escopo da GPO.

2. O Kaspersky Security Center instala os aplicativos Kaspersky selecionados nos dispositivos cliente diretamente do KLSHARE, que é a pasta de rede compartilhada no aplicativo. Na pasta de instalação do Kaspersky Security Center, será criada uma subpasta auxiliar que contém o arquivo .msi para o aplicativo a ser instalado.

3. Quando novos dispositivos são adicionados ao escopo da tarefa, são adicionados ao grupo de segurança após o início da próxima tarefa. Se a opção **Executar tarefas ignoradas** estiver selecionada no agendamento da tarefa, os dispositivos são adicionados imediatamente ao grupo de segurança.

4. Quando dispositivos são excluídos do escopo da tarefa, são excluídos também do grupo de segurança após o início da próxima tarefa.

5. Quando uma tarefa for excluída do Active Directory, a GPO, o link para o GPO e o grupo de segurança correspondente serão excluídos também.

Se quiser aplicar outro esquema de instalação usando o Active Directory, você pode definir as configurações necessárias manualmente. Por exemplo, isso poderá ser necessário nos seguintes casos:

- Quando o administrador da proteção de antivírus não tem direitos para efetuar alterações ao Active Directory de determinados domínios;

- Quando o pacote de instalação original tiver que ser armazenado em um recurso de rede separado;

- Quando é necessário vincular uma GPO a unidades específicas do Active Directory.

Estão disponíveis as opções que se seguem para usar um esquema de instalação alternativo através do Active Directory:

- Se a instalação tiver que ser realizada diretamente da pasta compartilhada do Kaspersky Security Center, nas propriedades da GPO do Active Directory especifique o arquivo .msi localizado na subpasta de execução da pasta do pacote de instalação para obter o aplicativo desejado.

- Se o pacote de instalação tiver de ser localizado em outro recurso de rede, é necessário copiar a totalidade do conteúdo da pasta exec, já que além do arquivo com a extensão, a pasta contém arquivos de configuração gerados quando o pacote foi criado. Para instalar a chave de licença com o aplicativo, copie também o arquivo de chave para essa pasta.

Instalando aplicativos nos Servidores de Administração secundários

Para instalar um aplicativo em Servidores de Administração secundários:

1. Estabeleça uma conexão ao Servidor de Administração que controla os Servidores de Administração secundários relevantes.

2. Certifique-se de que o pacote de instalação corresponde ao aplicativo sendo instalado em cada um dos Servidores de Administração secundários selecionados. Se o pacote de instalação não puder ser encontrado em nenhum dos Servidores secundários, distribua-o usando a tarefa de distribuição de pacote de distribuição.

3. Crie a tarefa de instalação do aplicativo nos Servidores de Administração secundários em uma das seguintes formas:

   - Se você desejar criar uma tarefa para Servidores de Administração secundários no grupo de administração selecionado, crie uma tarefa de grupo para a instalação remota para esse grupo.
   - Se você desejar criar uma tarefa para Servidores de Administração secundários específicos, crie uma tarefa de instalação remota para dispositivos específicos.

   O Assistente de criação da tarefa de implementação inicia para guiá-lo na criação da tarefa de instalação remota. Siga as instruções do Assistente.

   Na janela **Selecionar o tipo de tarefa** do assistente para novas tarefas, na seção **Servidor de Administração do Kaspersky Security Center**, abra a pasta **Avançado** e selecione **instalar o aplicativo remotamente nos Servidores de Administração secundários** como o tipo de tarefa.

   O Assistente para novas tarefas criará uma tarefa de instalação remota do aplicativo selecionado em Servidores de Administração secundários específicos.

4. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação especificada nas configurações da tarefa.

Após a conclusão da tarefa de instalação remota, o aplicativo selecionado será instalado nos Servidores de Administração secundários.

Instalação de aplicativos usando o Assistente de instalação remota

Para instalar os aplicativos Kaspersky, você pode usar o Assistente de instalação remota. O Assistente de instalação remota permite a instalação remota de aplicativos por meio de pacotes de instalação especialmente criados ou diretamente a partir de um pacote de distribuição.

Para a operação apropriada da tarefa de instalação remota em um dispositivo cliente que não tem o Agente de Rede instalado, as seguintes portas devem estar abertas: TCP 139 e 445; UDP 137 e 138. Por padrão, essas portas são abertas para todos os dispositivos incluídos no domínio. No caso de erros de rede, confira a Base de conhecimento do Kaspersky Security Center.

Para instalar um aplicativo nos dispositivos selecionados usando o Assistente de instalação remota:

1. Na árvore do console, localize a pasta **Instalação remota** e selecione a subpasta **Pacotes de instalação**.
2. No espaço de trabalho da pasta, selecione o pacote de instalação do aplicativo que você precisa instalar.
3. No menu de contexto do pacote de instalação, selecione **Instalar o aplicativo**.

   O Assistente de instalação remota é iniciado.

4. Na janela **Selecionar dispositivos para a instalação**, é possível criar uma lista de dispositivos nos quais o aplicativo será instalado:

   - **Instalar em um grupo de dispositivos gerenciados**

     Se esta opção estiver selecionada, a tarefa de instalação remota para um grupo de dispositivos será criada.

   - **Selecionar dispositivos para a instalação**

     Se esta opção estiver selecionada, a tarefa de instalação remota para dispositivos específicos será criada. Estes dispositivos específicos podem incluir tanto gerenciados como não atribuídos.

5. Na janela **Definir as configurações da tarefa de instalação remota**, especifique as configurações para a instalação remota do aplicativo.

   No grupo de configurações **Forçar download do pacote de instalação**, especifique como os arquivos que são necessários para instalar um aplicativo são distribuídos nos dispositivos clientes:

   - Usando o Agente de Rede

     Se esta opção de seleção estiver ativada, os pacotes de instalação são entregues aos dispositivos clientes pelo Agente de Rede instalado neles.

     Caso esta opção estiver desativada, os pacotes de instalação serão entregues usando as ferramentas do sistema operacional dos dispositivos clientes.

     Recomendamos que você ative esta opção se a tarefa tiver sido atribuída a dispositivos com o Agente de Rede instalado.

     Por padrão, esta opção está ativada.

   - Usando recursos do sistema operacional através do Servidor de Administração

     Caso esta opção esteja ativada, os arquivos serão transmitidos para os dispositivos clientes usando as ferramentas do sistema operacional pelo Servidor de Administração. Você pode ativar esta opção se nenhum Agente de Rede estiver instalado no dispositivo cliente, mas esse está na mesma rede que o Servidor de Administração.

     Por padrão, esta opção está ativada.

   - Usando recursos do sistema operacional através de pontos de distribuição

     Se esta opção estiver ativada, os pacotes de instalação serão transmitidos para os dispositivos clientes usando as ferramentas do sistema operacional, através dos pontos de distribuição. Você pode selecionar esta opção se houver, no mínimo, um ponto de distribuição na rede.

     Se opção **Uso do Agente de Rede** estiver ativada, os arquivos serão entregues pelas ferramentas do sistema operacional, apenas se os recursos do Agente de Rede estiverem indisponíveis.

     Por padrão, esta opção está ativada para as tarefas de instalação remotas que são criadas em um Servidor de Administração virtual.

   - Número de tentativas de instalação

Se, ao executar a tarefa de instalação remota, o Kaspersky Security Center falhar em instalar um aplicativo em um dispositivo gerenciado dentro do número e execuções do instalador especificado pelo parâmetro, o Kaspersky Security Center para a entrega do pacote de instalação para este dispositivo gerenciado e não mais inicia o instalador no dispositivo.

A opção `Número de tentativas de instalação` permite que você salve os recursos do dispositivo gerenciado, assim como reduzir o tráfego (desinstalação, execução do arquivo MSI e mensagens de erro).

As tentativas da tarefa recorrente pode indicar um problema no dispositivo que impede a instalação. O administrador deveria solucionar o problema dentro do número especificado de tentativas de instalação (por exemplo, ao alocar espaço em disco suficiente, remover aplicativos incompatíveis ou modificar as configurações de outros aplicativos que impedem a instalação) e para reiniciar a tarefa (manualmente ou por um agendamento).

Se a instalação não for realizada eventualmente, o problema é considerado não solucionável e quaisquer tarefas adicionais são consideradas como custosas em temos de consumo desnecessário de recursos e tráfego.

Quando a tarefa for criada, o contador de tentativas é definido como `0`. Cada execução do instalador retorna um erro no dispositivo e incrementa a leitura do contador.

Caso o número de tentativas especificado no parâmetro tenha sido excedido e o dispositivo esteja pronto para a instalação do aplicativo, é possível aumentar o valor do parâmetro `Número de tentativas de instalação` e iniciar a tarefa para instalar o aplicativo. Alternativamente, você pode criar uma nova tarefa de instalação remota.

Definir o que fazer com dispositivos cliente gerenciados por outro Servidor de Administração:

- **Instalar em todos os dispositivos**

  O aplicativo será instalado até mesmo nos dispositivos gerenciados por outros Servidores de Administração.

  Esta opção está marcada por padrão. Não é preciso alterar essa configuração se houver somente um Servidor de Administração na rede.

- **Instalar somente em dispositivos gerenciados por este Servidor de Administração**

  O aplicativo será instalado somente nos dispositivos gerenciados por este Servidor de Administração. Selecione esta opção se você tiver mais de um Servidor de Administração na rede e deseja evitar conflitos entre eles.

Defina as configurações adicionais:

- **Não reinstalar o aplicativo se ele já estiver instalado**

  Se esta opção estiver ativada, o aplicativo selecionado não será reinstalado se já estiver instalado neste dispositivo cliente.

  Se esta opção não estiver ativada, o aplicativo será instalado de qualquer forma.

  Por padrão, esta opção está ativada.

- **Atribuir a instalação do pacote em politicas de grupo do Active Directory (Diretório Ativo)**

  Se esta opção estiver ativada, é instalado um pacote de instalação, usando as políticas de grupo do Active Directory.

  Essa opção fica disponível se o pacote de instalação do Agente de Rede estiver selecionado.

  Por padrão, esta opção está desativada.

6. Na janela **Selecionando uma chave de licença**, selecione uma chave de licença e método para sua distribuição:

- **Não colocar uma chave de licença no pacote de instalação (recomendado)**

  A chave será automaticamente distribuída a todos os dispositivos com os quais ela for compatível:

  - Se a distribuição automática foi ativada nas propriedades da chave.
  - Se a tarefa **Adicionar chave** foi criada.

- **Colocar a chave de licença no pacote de instalação**

  A chave é distribuída aos dispositivos em conjunto com o pacote de instalação.

  Não recomendamos que distribua a chave usando este método, porque os direitos de acesso de Leitura são ativados para o repositório de pacotes de instalação.

A janela **Selecionando uma chave de licença** é exibida se o pacote de instalação não inclui uma chave de licença.

Se o pacote de instalação incluir uma chave de licença, a janela **Propriedades da chave de licença** é exibida, contendo os detalhes da chave de licença.

7. Na janela **Selecionando uma opção de reinício do sistema operacional**, especifique se os dispositivos devem ser reiniciados se o sistema operacional tiver que ser reiniciado durante a instalação de aplicativos nos mesmos:

- **Não reiniciar o dispositivo**

  Se esta opção for selecionada, o dispositivo não será reiniciado após a instalação do aplicativo de segurança.

- **Reiniciar o dispositivo**

  Se esta opção for selecionada, o dispositivo será reiniciado após a instalação do aplicativo de segurança.

- **Perguntar ao usuário o que fazer**

  Se esta opção for selecionada, após a instalação de um aplicativo de segurança, é exibida uma notificação ao usuário, informando que o dispositivo precisa ser reiniciado. Usando o link **Modificar**, você poderá modificar o texto da mensagem, o período de exibição de mensagem e o tempo da reinicialização automática.

  Por padrão, esta opção está selecionada.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

  Se esta opção estiver ativada, os aplicativos nos dispositivos bloqueados serão forçados a fechar antes do reinício.

  Por padrão, esta opção está desativada.

8. Na janela **Selecionar contas para acessar os dispositivos**, você pode adicionar as contas que serão usadas para iniciar a tarefa de instalação remota:

   - **Nenhuma conta necessária (Agente de Rede instalado)**

     Se essa caixa de seleção estiver selecionada, você não precisará especificar uma conta sob a qual o instalador do aplicativo será executado. A tarefa será executada sob a conta sob a qual o serviço do Servidor de Administração está sendo executado.

     Caso o Agente de Rede não tenha sido instalado em dispositivos cliente, a opção não estará disponível.

   - **Conta necessária (Agente de Rede não é usado)**

     Selecione esta opção se o Agente de Rede não estiver instalado nos dispositivos aos quais você atribui a tarefa de instalação remota. Neste caso, é possível especificar uma conta de usuário ou um certificado SSH para instalar o aplicativo.

     - **Conta local**. Se essa opção estiver selecionada, especifique a conta de usuário sob a qual o instalador do aplicativo será executado. Clique no botão **Adicionar**, selecione **Conta local** e, então, especifique as credenciais da conta do usuário.

       É possível especificar várias contas de usuário se, por exemplo, nenhuma delas tiver todos os direitos necessários em todos os dispositivos para os quais você atribui a tarefa. Nesse caso, todas as contas adicionadas são usadas para executar a tarefa, em ordem consecutiva, de cima para baixo.

     - **Certificado SSH**. Se quiser instalar um aplicativo em um dispositivo cliente baseado em Linux, poderá especificar um certificado SSH em vez de uma conta de usuário. Clique no botão **Adicionar**, selecione **Certificado SSH** e, então, especifique as chaves privada e pública do certificado.

       Para gerar uma chave privada, você pode usar o utilitário ssh-keygen. Observe que o Kaspersky Security Center é compatível com o formato PEM de chaves privadas, mas o utilitário ssh-keygen gera chaves SSH no formato OPENSSH por padrão. O formato OPENSSH não é compatível com o Kaspersky Security Center. Para criar uma chave privada no formato PEM compatível, adicione a opção -m PEM no comando ssh-keygen. Por exemplo:

       ```
       ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail do usuário>"
       ```

9. Na janela **Iniciar a instalação**, clique no botão **Avançar** para criar e iniciar uma tarefa de instalação remota nos dispositivos selecionados.

   Se a janela **Iniciar a instalação** tiver a opção **Não executar a tarefa após a conclusão do Assistente de instalação remota** selecionada, a tarefa de instalação remota não será iniciada. Você pode iniciar essa tarefa manualmente mais tarde. O nome de tarefa corresponde ao nome do pacote de instalação para o aplicativo: **Instalação de <nome do pacote de instalação>**.

Para instalar o aplicativo nos dispositivos em um grupo de administração usando o Assistente de instalação remota:

1. Estabeleça uma conexão ao Servidor de Administração que controla o grupo de administração relevante.

2. Selecione um grupo de administração na árvore do console.

3. No espaço de trabalho do grupo, clique no botão **Executar a ação** e selecione **Instalar o aplicativo** na lista suspensa.

   Isto iniciará o Assistente de instalação remota. Siga as instruções do Assistente.

4. Na etapa final do assistente, clique em **Avançar** para criar e executar a tarefa de instalação remota nos dispositivos selecionados.

Quando o Assistente de instalação remota for concluído, o Kaspersky Security Center executa as seguintes ações:

- Crie um pacote de instalação para implementação do aplicativo (se não foi criado anteriormente). O pacote de instalação é localizado na pasta **Instalação remota**, na subpasta **Pacotes de instalação**, com um nome que corresponde ao nome e à versão do aplicativo. Você pode usar esse pacote de instalação para instalação do aplicativo no futuro.

- Cria e executa uma tarefa de instalação remota para dispositivos específicos ou para um grupo de administração. A nova tarefa de instalação remota criada será armazenada na pasta **Tarefas** ou será adicionada às tarefas do grupo de administração para o qual ela foi criada. Você pode iniciar essa tarefa manualmente mais tarde. O nome de tarefa corresponde ao nome do pacote de instalação para o aplicativo: **Instalação de <nome do pacote de instalação>**.

Exibir um relatório de implementação da proteção

Você pode usar o relatório de implementação da proteção para monitorar o progresso da implementação de proteção da rede.

Para visualizar um relatório de implementação da proteção:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.

2. No espaço de trabalho do nó, selecione a guia **Relatórios**.

3. No espaço de trabalho da pasta **Relatórios** selecione o modelo de relatório com o nome **Relatório de implementação de proteção**.

O espaço de trabalho exibirá um relatório contendo informações sobre a implementação da proteção em todos os dispositivos na rede.

Você pode gerar um novo relatório de implementação da proteção e especificar o tipo de dados que deve incluir:

- Para um grupo de administração
- Para dispositivos específicos
- Para uma seleção de dispositivos
- Para todos os dispositivos

O Kaspersky Security Center assume que a proteção está implementada em um dispositivo se um aplicativo de segurança estiver instalado e a proteção em tempo real está ativada.

Como trabalhar com os plug-ins de gerenciamento

Os aplicativos da Kaspersky são gerenciados no Console de Administração usando os plug-ins de gerenciamento. Cada aplicativo da Kaspersky que pode ser gerenciado pelo Kaspersky Security Center inclui um plugin de gerenciamento. Usando o plug-in de gerenciamento de aplicativos, é possível executar as seguintes ações no Console de Administração:

- Crie e edite as políticas e configurações de aplicativos, assim como configurações das tarefas de aplicativo.
- Obtenha informações sobre as tarefas de aplicativo, os eventos que ocorrem em sua operação e as estatísticas da operação de aplicativo recebidas dos dispositivos clientes.

Para verificar a lista de plug-ins instalados e suas versões:

1. Na árvore do Console de Administração, clique com o botão direito do mouse em **Servidor de Administração <nome_do_servidor>** e selecione **Propriedades**.
2. Clique **Avançado → Detalhes dos plug-ins de gerenciamento de aplicativos instalados**.

A lista de plug-ins de gerenciamento instalados e suas versões aparecem no painel direito.

É possível instalar os plug-ins para aplicativos gerenciados ao executar o assistente de início rápido do Servidor de Administração durante a configuração inicial do Kaspersky Security Center. Além disso, é possível instalar os plug-ins de gerenciamento manualmente.

Para instalar um plug-in de gerenciamento manualmente:

1. Baixe o plug-in de gerenciamento para o aplicativo da Kaspersky e a versão necessária (por exemplo, Kaspersky Endpoint Security for Windows 12.3) na página de Suporte técnico da Kaspersky.
2. Se o Console de Administração estiver em execução, feche-o.
3. Descompacte o arquivo do plug-in baixado e execute o arquivo klcfginst.msi ou klcfginst.exe. Siga as instruções de instalação do assistente.
4. Quando a instalação estiver concluída, execute o Console de Administração e assegure-se de que o plug-in seja apresentado na lista de plug-ins instalados, conforme descrito no procedimento anterior.

Ao executar o Console de Administração após a instalação de um plug-in de gerenciamento compatível com o assistente de Início rápido de aplicativos gerenciados, esse assistente é iniciado automaticamente. É possível seguir as etapas do assistente de início rápido de aplicativos gerenciados para criar políticas e tarefas padrão do aplicativo da Kaspersky. O assistente inicia automaticamente apenas quando o Console de Administração for executado após a instalação inicial do plug-in ou após a atualização do plug-in de gerenciamento para uma versão compatível com outra versão do aplicativo da Kaspersky para a qual as tarefas e políticas ainda não foram criadas. Também é possível iniciar o assistente de início rápido de aplicativos gerenciados manualmente.

Para iniciar o assistente de início rápido de aplicativos gerenciados manualmente:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No menu de contexto do nó Servidor de Administração, selecione **Todas as tarefas → Assistente de Início Rápido de Aplicativos Gerenciados**.
3. O assistente de início rápido de aplicativos gerenciados é iniciado. Siga as etapas do assistente para criar políticas e tarefas padrão para o aplicativo do Kaspersky.

Para remover um plug-in de gerenciamento:

1. Se o Console de Administração estiver em execução, feche-o.
2. Abra o editor de Registro do Windows.
3. Encontre a seguinte chave de licença:
   - `HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\28\Plugins` em sistemas 32 bits.
   - `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\28\Plugins` em sistemas 64 bits.

   A chave contém plug-ins de gerenciamento instalados. Para cada plug-in, o valor `DisplayName` contém o nome do plug-in e o valor `UninstallString` contém o comando para desinstalar o plug-in.
4. Encontre a chave do plug-in que deseja desinstalar e copie seu valor `UninstallString` na área de transferência.
5. Cole o valor na string de comando e execute-o com direitos de administrador do sistema.

A versão do plug-in de gerenciamento não deve ser anterior à versão do aplicativo gerenciado da Kaspersky. Se você atualizar o aplicativo Kaspersky nos dispositivos, instale o plug-in de gerenciamento da mesma versão.

Ao abrir a política criada em uma versão anterior do plug-in, você será solicitado a aceitar a Declaração da Kaspersky Security Network.

Ao desinstalar o Kaspersky Security Center Web Console, todos os plug-ins de gerenciamento também são desinstalados.

Se você abrir e salvar a política na versão do plug-in posterior à versão do aplicativo gerenciado, a política será atualizada e não será possível abri-la no plug-in da versão anterior.

Remoção remota de aplicativos

O Kaspersky Security Center permite desinstalar aplicativos de dispositivos remotamente através de tarefas de desinstalação remotas. Essas tarefas são criadas e atribuídas aos dispositivos por um assistente dedicado. Para atribuir uma tarefa aos dispositivos mais rapidamente e facilmente, você pode especificar os dispositivos na janela assistente em uma das seguintes formas:

- **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**. Neste caso, a tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

- **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**. Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

- **Atribuir a tarefa a uma seleção de dispositivos**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em uma seleção anteriormente criada. É possível especificar a seleção predefinida ou uma personalizada criada por você.

- **Atribuir tarefa a um grupo de administração**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em um grupo de administração anteriormente criado.

Problemas de remoção remota

Ao executar a remoção remota de aplicativos de terceiros, os administradores podem encontrar uma advertência informando: "A desinstalação remota foi concluída neste dispositivo com advertências: o aplicativo para remoção não está instalado". Esse problema geralmente surge quando o aplicativo a ser removido é instalado apenas para o usuário que está conectado no momento. Se o usuário não estiver conectado, o aplicativo ficará invisível e não poderá ser removido remotamente.

Esse comportamento é diferente com aplicativos destinados ao uso por vários usuários no mesmo dispositivo, situação em que os aplicativos ficam globalmente visíveis e acessíveis a todos os usuários do dispositivo.

No Kaspersky Security Center, o algoritmo de registro de aplicativos maneja aplicativos para usuários individuais e aplicativos para vários usuários de forma diferente:

- Os aplicativos para vários usuários são mantidos em uma lista de aplicativos instalados atualizada em tempo real.

- Os aplicativos para usuários individuais são monitorados por um mecanismo de cache.

  Se um usuário estiver conectado no momento da detecção do aplicativo, o Kaspersky Security Center armazenará em cache informações sobre os aplicativos desse usuário. Mesmo que o usuário fizer logout posteriormente, o Kaspersky Security Center continuará exibindo esses aplicativos como instalados com base nos dados armazenados em cache, embora eles não estejam mais visíveis ou acessíveis no dispositivo.

Essa discrepância pode resultar em situações em que o Kaspersky Security Center identifica um aplicativo como instalado com base em dados armazenados em cache, mas a tarefa de remoção falha porque o aplicativo não fica acessível quando o usuário está desconectado.

Por padrão, o tempo de vida útil dos dados do aplicativo armazenados em cache é definido como 30 dias. Os administradores podem modificar essa configuração para reduzir a duração do cache, minimizando assim as discrepâncias entre os dados exibidos e a visibilidade real do aplicativo nos dispositivos.

Para ajustar o tempo de vida do cache para 1 hora (3.600 segundos), execute o seguinte comando no Servidor de Administração:

```
klscflag -fset -pv klserver -n KLNAG_INV_PERUSER_APPS_CACHE_NONACTIVE_SIDS_LIFETIME_SEC
-t d -v 3600
```

Após executar esse comando, reinicie o Servidor de Administração para que as alterações entrem em vigor.

Fonte de informação sobre os aplicativos instalados

O Agente de Rede recupera informações sobre software instalado em dispositivos Windows das seguintes chaves de registro:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para todos os usuários.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para todos os usuários.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para o usuário atual.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para usuários específicos.

Remoção remota de um aplicativo de um dispositivo cliente do grupo de administração

Para remover um aplicativo remotamente de dispositivos cliente do grupo de administração:

1. Estabeleça uma conexão ao Servidor de Administração que controla o grupo de administração relevante.
2. Selecione um grupo de administração na árvore do console.
3. No espaço de trabalho do grupo, selecione a guia **Tarefas**.
4. Execute a criação da tarefa, clicando no botão **Nova tarefa**.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

   Na janela **Selecionar o tipo de tarefa** do assistente para novas tarefas, no nó do **Servidor de Administração do Kaspersky Security Center**, na pasta **Avançado**, selecione **Desinstalar o aplicativo remotamente** como o tipo de tarefa.

   O Assistente para novas tarefas cria uma tarefa de grupo de remoção remota do aplicativo selecionado. A nova tarefa é exibida no espaço de trabalho do grupo de administração na guia **Tarefas**.
5. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação especificada nas configurações da tarefa.

Após a conclusão da tarefa de remoção remota, o aplicativo selecionado será removido dos dispositivos cliente no grupo de administração.

Remoção remota de um aplicativo de dispositivos selecionados

Para remover um aplicativo remotamente de dispositivos selecionados:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Execute a criação da tarefa clicando em **Nova tarefa**.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

   Na janela **Selecionar o tipo de tarefa** do assistente para novas tarefas, no nó do **Servidor de Administração do Kaspersky Security Center**, na pasta **Avançado**, selecione **Desinstalar o aplicativo remotamente** como o tipo de tarefa.

   O Assistente para novas tarefas cria uma tarefa de uma instalação remota do aplicativo selecionado nos dispositivos específicos. A tarefa recém criada é exibida no espaço de trabalho da pasta **Tarefas**.
3. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação especificada nas configurações da tarefa.

Após a conclusão da tarefa de remoção remota, o aplicativo selecionado será removido dos dispositivos cliente selecionados.

Trabalho com pacotes de instalação

Durante criação de tarefas de implementação, o sistema utiliza pacotes de instalação contendo conjuntos de parâmetros necessários para a instalação de software.

Os pacotes de instalação podem conter um arquivo de chave. Recomendamos que você evite compartilhar o acesso aos pacotes de instalação que contêm um arquivo de chave.

Você pode usar um único pacote de instalação várias vezes.

Os pacotes de instalação criados pelo Servidor de Administração são movidos para a árvore do console e localizados na pasta **Instalação remota**, na subpasta **Pacotes de instalação**. Os pacotes de instalação são armazenados no Servidor de Administração na subpasta de serviço de Pacotes dentro da pasta compartilhada especificada.

Caso necessário, será possível excluir um pacote de instalação da subpasta **Pacotes de instalação** seguindo as instruções no artigo Excluir um objeto.

Não faça a alteração manual do conteúdo dos pacotes de instalação em uma pasta compartilhada. Caso necessário, será possível criar uma cópia de um pacote de instalação, fazer as alterações necessárias e criar novas tarefas de instalação.

Criação de um pacote de instalação

Este artigo descreve o procedimento de criação dos seguintes tipos de pacotes de instalação:

- Pacote de instalação para um aplicativo da Kaspersky
- Pacote de instalação para um arquivo executável especificado
- Pacote de instalação para um aplicativo do banco de dados da Kaspersky

Não é necessário criar manualmente um pacote de instalação para a instalação remota do Agente de Rede. Ele é criado automaticamente durante a instalação do Kaspersky Security Center e armazenado na pasta **Pacotes de instalação**. Caso o pacote de instalação remota do Agente de Rede tenha sido excluído, será possível recriá-lo ao selecionar o arquivo nagent.kud na pasta NetAgent do pacote de distribuição do Kaspersky Security Center.

Para criar um pacote de instalação:

1. Conecte ao Servidor de Administração necessário.
2. Na árvore do console, selecione **Avançado** → **Instalação remota** → **Pacotes de instalação**.
3. Inicie a criação de um novo pacote de instalação de uma das seguintes maneiras:
   - Clique com o botão direito do mouse na pasta **Pacotes de instalação** e selecione **Novo** → **Pacote de instalação** no menu de contexto.
   - Clique com o botão direito do mouse na área vazia da lista de pacotes de instalação e selecione **Criar** → **Pacote de instalação** no menu de contexto.
   - Clique em **Criar pacote de instalação** na seção de gerenciamento da lista de pacotes de instalação.

   O Assistente de novo pacote inicia.
4. Selecione um dos seguintes tipos de pacote de instalação ao clicar no ícone correspondente:
   - Pacote de instalação para um aplicativo da Kaspersky.
   - Pacote de instalação para um arquivo executável especificado.
   - Pacote de instalação para um aplicativo do banco de dados da Kaspersky.
5. Especifique o nome do pacote de instalação a ser criado.

   É possível especificar qualquer nome.

6. Selecione o aplicativo ou arquivo executável para o qual o pacote de instalação deve ser criado, de uma das seguintes formas:

   - Clique no botão **Procurar** e, na janela padrão **Abrir** do Windows, selecione o pacote de distribuição do aplicativo necessário localizado nos discos disponíveis.

     Esta opção será aplicável se você optar por criar um pacote de instalação para um aplicativo Kaspersky ou para um arquivo executável especificado.

   - Clique no botão **Procurar** e, na janela **Selecionar aplicativo**, selecione o pacote de distribuição do aplicativo necessário.

     Essa opção será aplicável se você optar pela criação de um pacote de instalação para um aplicativo do banco de dados da Kaspersky.

   Caso esteja criando um pacote de instalação para o Servidor de Administração, selecione o arquivo sc.kud. O arquivo sc.kud está localizado na pasta raiz do pacote de distribuição do Kaspersky Security Center.

   Não especifique nenhum detalhe de contas privilegiadas nos parâmetros dos pacotes de instalação.

7. Leia o Contrato de Licença de Usuário Final e a Política de Privacidade.

   Ao criar um pacote de instalação para um aplicativo, uma solicitação de visualização e aceitação de um Contrato de Licença de Usuário Final e uma Política de Privacidade poderá ser emitida para esse aplicativo.

   Leia ambos os documentos. Caso concorde com todos os termos do Contrato de Licença e da Política de Privacidade, basta aceitá-los ao marcar as caixas de seleção correspondentes.

   A instalação do aplicativo no seu dispositivo continua e a criação do pacote de instalação é retomada.

   Caso esteja criando um pacote de instalação para o Kaspersky Endpoint Security for Mac, será possível escolher o idioma do Contrato de Licença e da Política de Privacidade.

8. Caso necessário, ative a instalação automática dos componentes do sistema.

   Caso esteja criando um pacote de instalação para um aplicativo do banco de dados da Kaspersky, será possível ativar a instalação automática dos componentes necessários do sistema. O Assistente de novo pacote contém uma lista de todos os componentes do sistema disponíveis para o aplicativo selecionado. É possível acessar a lista a qualquer momento nas propriedades do pacote de instalação.

   Se você estiver criando um pacote de instalação de patch, a lista incluirá todos os componentes do sistema necessários para a implementação deste patch.

9. Clique no botão **Concluir** para concluir o processo de criação do pacote.

Quando o Assistente de novo pacote for concluído, o novo pacote de instalação aparecerá no espaço de trabalho da pasta **Pacotes de instalação** na árvore do console.

Criar pacote de instalação autônomo

Você e os usuários de dispositivos na sua organização podem usar pacotes de instalação independente para instalar os aplicativos no dispositivo manualmente.

Um pacote de instalação independente é um arquivo executável (installer.exe) que você pode armazenar no Servidor da Web ou na pasta compartilhada, ou transferir para um dispositivo cliente usando outro método. Você também pode enviar o link para o pacote de instalação independente por e-mail. No dispositivo cliente, o usuário pode executar o arquivo recebido localmente para instalar um aplicativo sem envolver o Kaspersky Security Center.

Certifique-se de que o pacote de instalação independente não está disponível para pessoas não autorizadas.

Você pode criar pacotes de instalação independentes para aplicativos Kaspersky e de terceiros, para as plataformas Windows, macOS e Linux. Para criar um pacote de instalação independente para um aplicativo de terceiros, você deve primeiro criar um pacote de instalação personalizada.

A fonte para criar pacotes de instalação independentes são os pacotes de instalação na lista criada no Servidor de Administração.

Para criar um pacote de instalação independente:

1. Na árvore do console, selecione o **Servidor de Administração** → **Avançado** → **Instalação remota** → **Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Na lista de pacotes de instalação, selecione um pacote de instalação para o qual você deseja criar um pacote independente.

3. No menu de contexto, selecione **Criar pacote de instalação independente**.

   O Assistente de criação de pacote de instalação independente é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

4. Na primeira página do assistente, se você selecionou um pacote de instalação para o aplicativo Kaspersky e deseja instalar o Agente de Rede junto com o aplicativo selecionado, certifique-se de que a opção **Instalar o Agente de Rede junto com este aplicativo** está ativada.

   Por padrão, esta opção está ativada. Recomendamos ativar esta opção se você não tiver certeza se o Agente de Rede está instalado no dispositivo. Se o Agente de Rede já estiver instalado no dispositivo, após a instalação do pacote de instalação independente com o Agente de Rede, esse será atualizado para a versão mais recente.

   Se você desativar esta opção, o Agente de Rede não será instalado no dispositivo e esse não será gerenciado.

   Se já existir um pacote de instalação independente para o aplicativo selecionado no Servidor de Administração, o assistente informará a respeito. Nesse caso, você deve selecionar uma das seguintes ações:

   - **Criar pacote de instalação independente**. Selecione esta opção, por exemplo, se deseja criar um pacote de instalação independente para uma nova versão do aplicativo e também deseja manter um pacote de instalação independente criado para uma versão anterior do aplicativo. O novo pacote de instalação independente é colocado em outra pasta.

   - **Usar pacote de instalação independente existente**. Selecione esta opção se desejar usar um pacote de instalação independente existente. O processo de criação do pacote não será iniciado.

   - **Recriar pacote de instalação independente existente**. Selecione esta opção se desejar criar um pacote de instalação independente para o mesmo aplicativo novamente. O pacote de instalação independente é colocado na mesma pasta.

5. Na próxima página do assistente, selecione a opção **Migrar dispositivos não atribuídos para este grupo** e especifique um grupo de administração para o qual deseja mover o dispositivo cliente após a instalação do Agente de Rede.

   Por padrão, o dispositivo é movido para o grupo **Dispositivos gerenciados**.

   Se não deseja mover o dispositivo cliente para um grupo de administração após a instalação do Agente de Rede, selecione a opção **Não migrar dispositivos**.

6. Na próxima página do assistente, quando o processo de criação do pacote de instalação independente for concluído, um resultado da criação do pacote independente e um caminho para o pacote independente serão exibidos.

   Você pode clicar nos links e executar um dos seguintes procedimentos:

   - Abra a pasta com o pacote de instalação independente.
   - Envie o link por e-mail para o pacote de instalação independente criado. Para executar esta ação, você deve ter um aplicativo de e-mail ativado.
   - Código HTML de amostra para a publicação de link em um site. Um arquivo TXT é criado e aberto em um aplicativo associado a um formato TXT. No arquivo, a tag <a> HTML com atributos é exibida.

7. Na próxima página do assistente, se você deseja abrir a lista de pacotes de instalação autônomos, ative a opção **Abrir a lista de pacotes independentes**.

8. Clique no botão **CONCLUIR**.

   O Assistente de criação de pacote de instalação independente é fechado.

O pacote de instalação independente é criado e colocado na subpasta PkgInst da pasta compartilhada do Servidor de Administração. Você pode visualizar a lista de pacotes independentes, clicando no botão **Exibir a lista de pacotes independentes** acima da lista de pacotes de instalação.

Criar pacotes de instalação personalizados

Você pode usar os pacotes de instalação personalizada para fazer o seguinte:

- Instalar qualquer aplicativo (como um editor de texto) em um dispositivo cliente, por exemplo, através de uma tarefa.
- Para criar um pacote de instalação independente.

Um pacote de instalação personalizada é uma pasta com um conjunto de arquivos. Uma fonte para criar um pacote de instalação personalizado é um *arquivo morto*. O arquivo de compactação contém um ou mais arquivos que devem ser incluídos no pacote de instalação personalizada. Criando um pacote de instalação personalizado, é possível especificar parâmetros da linha de comandos, por exemplo, para instalar o aplicativo em um modo silencioso.

Para criar um pacote de instalação personalizado:

1. Na árvore do console, selecione o **Servidor de Administração** → **Avançado** → **Instalação remota** → **Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Acima da lista de pacotes de instalação, clique no botão **Criar pacote de instalação**.

   O Assistente de novo pacote inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na primeira página do assistente, selecione **Criar um pacote de instalação para o arquivo executável especificado**.

4. Na próxima página do assistente, especifique o nome do pacote de instalação personalizada.

5. Na próxima página do assistente, clique no botão **Procurar** e, em uma janela padrão do Windows **Abrir**, escolha um arquivo comprimido localizado nos discos disponíveis para criar um pacote de instalação personalizada.

   É possível carregar um arquivo ZIP, CAB, TAR ou TAR.GZ. Não é possível criar um pacote de instalação a partir do arquivo SFX (arquivo de extração automática).

   Os arquivos são baixados no Servidor de Administração do Kaspersky Security Center.

6. Na próxima página do assistente, especifique os parâmetros da linha de comando de um arquivo executável.

   Você pode especificar parâmetros da linha de comando, para instalar o aplicativo a partir do pacote de instalação em um modo silencioso. A especificação de parâmetros da linha de comando é opcional.

   Se desejar, configure as seguintes opções:

   - **Copiar pastas inteira para o pacote de instalação**

     Selecione esta opção se o arquivo executável está acompanhado por arquivos adicionais necessários para a instalação do aplicativo. Antes de você ativar esta opção, assegure-se de que todos os arquivos necessários estão armazenados na mesma pasta. Se esta opção estiver ativada, o aplicativo adiciona todo o conteúdo da pasta, incluindo o arquivo executável, no pacote de instalação.

   - **Converter configurações nos valores recomendados para aplicativos reconhecidos pelo Kaspersky Security Center**

     O aplicativo será instalado com as configurações recomendadas, se as informações sobre o aplicativo especificado estiverem contidas no banco de dados da Kaspersky.

     Se você inseriu parâmetros no campo **Linha de comando de arquivo executável**, ela é reescrita com as configurações recomendadas.

     Por padrão, esta opção está ativada.

     O banco de dados da Kaspersky é criado e mantido pelos analistas da Kaspersky. Para cada aplicativo que for adicionado no banco de dados, os analistas da Kaspersky definem as configurações ótimas de instalação. As configurações são definidas para assegurar a instalação remota com êxito de um aplicativo em um dispositivo cliente. O banco de dados é atualizado no Servidor de Administração quando a tarefa Baixar as atualizações no repositório do Servidor de Administração for executada.

   O processo para criação do pacote de instalação personalizado é iniciado.

   O assistente informa quando o processo é concluído.

   Se o pacote de instalação personalizada não for criado, uma mensagem apropriada será exibida.

7. Clique no botão **Concluir** para fechar o assistente.

O pacote de instalação que você criou é baixado na subpasta Packages da pasta compartilhada do Servidor de Administração. Após o download, o pacote de instalação personalizada aparece na lista de pacotes de instalação.

Na lista de pacotes de instalação no Servidor de Administração, você pode visualizar e editar as propriedades personalizadas do pacote de instalação.

Exibir e editar as propriedades de pacotes de instalação personalizada

Após criar um pacote de instalação personalizada, é possível visualizar as informações gerais sobre o pacote de instalação e especificar as configurações de instalação na janela Propriedades.

Para visualizar e editar propriedades de um pacote de instalação personalizada:

1. Na árvore do console, selecione o **Servidor de Administração** → **Avançado** → **Instalação remota** → **Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. No menu de contexto do pacote de instalação, selecione **Propriedades**.

   A janela Propriedades do pacote de instalação selecionado é aberta.

3. Veja as seguintes informações:

   - Nome do pacote de instalação
   - Nome do aplicativo compactado no pacote de instalação personalizada
   - Versão do aplicativo
   - Data de criação do pacote de instalação
   - Caminho para o pacote de instalação personalizada no Servidor de Administração
   - Executable file command line

4. Especificar as seguintes configurações:

   - Nome do pacote de instalação
   - Instalar os componentes gerais do sistema necessários

     Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional.

     Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

     Por padrão, esta opção está desativada.

     Esta opção está disponível apenas quando o aplicativo adicionado ao pacote de instalação é reconhecido pelo Kaspersky Security Center.
   - Linha de comando de arquivo executável

     Se o aplicativo requer parâmetros adicionais para uma instalação silenciosa, especifique-os neste campo. Consulte a documentação do fornecedor para obter detalhes.

     Você também pode inserir outros parâmetros.

     Este recurso está disponível apenas para pacotes que não são criados com base nos aplicativos Kaspersky.

5. Clique no botão **OK** ou **Aplicar** para salvar as alterações, se houver.

   As novas configurações são salvas.

Obtenção do pacote de instalação do agente de rede a partir do kit de distribuição do Kaspersky Security Center

É possível obter o pacote de instalação do Agente de Rede a partir do kit de distribuição do Kaspersky Security Center, sem a necessidade de instalar o Kaspersky Security Center. Em seguida, é possível usar o pacote de instalação para instalar o Agente de Rede nos dispositivos cliente.

Para obter o pacote de instalação a partir do agente de rede do kit de distribuição do Kaspersky Security Center:

1. Execute o arquivo executável ksc_<version number>.<build number>_full_<localization language>.exe a partir do kit de distribuição do Kaspersky Security Center.
2. Na janela que se abre, clique no link **Extrair pacotes de instalação**.
3. Na lista de pacotes de instalação, marque a caixa de seleção ao lado do pacote de instalação do agente de rede e clique no botão **Avançar**.
4. Caso seja necessário, clique no botão **Procurar** para alterar a pasta exibida e extrair o pacote de instalação.

5. Clique no botão **Extrair**.

   O aplicativo extrai o pacote de instalação do agente de rede.

6. Quando o processo for concluído, clique no botão **Fechar**.

O pacote de instalação do agente de rede é extraído para a pasta selecionada.

É possível usar o pacote de instalação para instalar o agente de rede por um dos seguintes métodos:

- Localmente executando o arquivo setup.exe a partir da pasta extraída
- Via instalação silenciosa
- Usando políticas de grupo do Microsoft Windows

Distribuindo pacotes de instalação para Servidores de Administração secundários

Para distribuir pacotes de instalação para Servidores de Administração secundários:

1. Estabeleça uma conexão ao Servidor de Administração que controla os Servidores de Administração secundários relevantes.
2. Crie uma tarefa de distribuição de pacotes de distribuição para Servidores de Administração secundários de uma das seguintes formas:

   - Se desejar criar uma tarefa para Servidores de Administração secundários no grupo de administração selecionado, inicie a criação de uma tarefa de grupo para esse grupo.
   - Caso deseje criar uma tarefa para Servidores de Administração secundários específicos, inicie a criação de uma tarefa para dispositivos específicos.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

   Na janela **Selecionar o tipo de tarefa** do assistente para novas tarefas, no nó **Servidor de Administração do Kaspersky Security Center**, na pasta **Avançado**, selecione **distribuir pacote de instalação** como o tipo de tarefa.

   O Assistente para novas tarefas criará uma tarefa de distribuição dos pacotes de instalação selecionados nos Servidores de Administração secundários específicos.

3. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que você especificou nas configurações da tarefa.

Os pacotes de instalação selecionados serão copiados para os Servidores de Administração secundários específicos.

Distribuir os pacotes de instalação através de pontos de distribuição

Você pode usar pontos de distribuição para distribuir pacotes de instalação dentro de um grupo de administração.

Após os pacotes de instalação serem recebidos do Servidor de Administração, os pontos de distribuição os distribuem automaticamente para os dispositivos cliente através de multicasting de IP. A multicasting de IP de novos pacotes de instalação dentro de um grupo de administração ocorre uma vez. Se um dispositivo cliente for desconectado da rede corporativa no momento da distribuição, o Agente de Rede (no dispositivo cliente) baixa automaticamente o pacote de instalação necessário de um ponto de distribuição quando a tarefa de instalação for iniciada.

Transferência de resultados da instalação do aplicativo para o Kaspersky Security Center

Após você ter criado o pacote de instalação do aplicativo, você pode configurá-lo para que todas as informações de diagnóstico sobre os resultados da instalação do aplicativo sejam transferidos para o Kaspersky Security Center. Para pacotes de instalação de aplicativos Kaspersky, a transferência de informações de diagnóstico sobre os resultados de instalação do aplicativo é configurada por padrão, e não é necessária qualquer configuração adicional.

Para configurar a transferência de informações de diagnóstico sobre os resultados da instalação do aplicativo no Kaspersky Security Center:

1. Navegue até à pasta do pacote de instalação criado usando o Kaspersky Security Center para o aplicativo selecionado. A pasta pode ser encontrada na pasta compartilhada especificada durante a instalação do Kaspersky Security Center.

2. Abra o arquivo com a extensão .kpd ou .kud para edição (por exemplo, no editor de Microsoft Windows Notepad).

   O arquivo possui o formato de um arquivo .ini de configuração regular.

3. Adicione as seguintes linhas ao arquivo:

   ```
   [SetupProcessResult]
   Wait=1
   ```

   Esse comando configura o Kaspersky Security Center para aguardar a conclusão da configuração para o aplicativo, para o qual o pacote de instalação é criado, e analisa o código de retorno do instalador. Se você precisar desativar a transferência de dados de diagnósticos, defina a chave Espera para 0.

4. Adicione a descrição dos códigos de retorno para uma instalação bem sucedida. Para fazer isso, adicione as seguintes linhas ao arquivo:

   ```
   [SetupProcessResult_SuccessCodes]
   <código de retorno>=[<descrição>]
   <código de retorno 1>=[<descrição>]
        …
   ```

   > Os colchetes contêm chaves opcionais.

   Sintaxe para as linhas:

   - `<código de retorno>`. Qualquer número correspondente ao código de retorno do instalador. O número de códigos de retorno pode ser arbitrário.

   - `<descrição>`. Descrição em texto do resultado da instalação. A descrição pode ser omitida.

5. Adicione a descrição de códigos de retorno para uma instalação com falha. Para fazer isso, adicione as seguintes linhas ao arquivo:

   ```
   [SetupProcessResult_ErrorCodes]
   <código de retorno>=[<descrição>]
   <código de retorno 1>=[<descrição>]
   ...
   ```

   A sintaxe dessas linhas é idêntica à sintaxe das linhas contendo os códigos de retorno de configuração bem-sucedida.

6. Feche o arquivo .kpd ou .kud ao salvar todas as alterações.

Finalmente, os resultados da instalação do aplicativo definido pelo usuário serão gravadas nos registros do Kaspersky Security Center, e aparecerão na lista de eventos e nos registros de relatórios e de execução de tarefas.

Definindo o endereço do servidor proxy da KSN para pacotes de instalação

Caso o endereço ou domínio do Servidor de Administração mude, você pode definir o endereço do servidor proxy da KSN para o pacote de instalação.

Para definir o endereço do servidor proxy da KSN para o pacote de instalação:

1. Na árvore do console, na pasta **Instalação remota** clique duas vezes na subpasta **Pacotes de instalação**.
2. No menu aberto, selecione **Propriedades**.
3. Na janela de propriedades aberta, selecione a subseção **Geral**.
4. Na subseção **Geral** da janela de propriedades, insira o endereço do servidor proxy da KSN.

Os pacotes de instalação usarão este endereço como padrão.

Obtenção de versões atualizadas de aplicativos

O Kaspersky Security Center permite obter versões atualizadas de aplicativos corporativos armazenados em servidores da Kaspersky.

Para receber versões atualizadas dos aplicativos corporativos da Kaspersky:

1. Execute uma das seguintes ações:

   - Na Console da árvore selecione o nó com o nome do Servidor de Administração requerido, verifique que a aba **Monitoramento** esta selecionado, e na secção **Implementação** clique o link **Existem novas versões de aplicativos Kaspersky disponíveis**.

     O link **Existem novas versões de aplicativos Kaspersky disponíveis** torna-se disponível quando o Servidor de Administração encontra uma nova versão de um aplicativo corporativo em um servidor da Kaspersky.

   - Na árvore do console, selecione **Avançado → Instalação remota → Pacotes de instalação** e, no espaço de trabalho, clique em **Ações adicionais**; e, na lista suspensa, selecione **Ver versões atuais dos aplicativos Kaspersky**.

   A lista da versão atual dos aplicativos Kaspersky é exibida.

2. Você pode filtrar a lista de aplicativos Kaspersky para simplificar a busca pelo aplicativo necessário.

   No topo da janela **Versões atuais do aplicativo**, clique no link **Filtro** para filtrar a lista de aplicativos pelos seguintes critérios:

   - **Componentes**. Use este critério para filtrar a lista de aplicativos Kaspersky pelas áreas de proteção que estão em uso em sua rede.
   - **Tipo de software baixado**. Use este critério para filtrar a lista de aplicativos Kaspersky pelo tipo de aplicativo.
   - **Produtos de software e atualizações a exibir**. Use este critério para exibir os aplicativos Kaspersky disponíveis por versões específicas.
   - **Idiomas exibidos para o software e atualizações**. Use este critério para exibir aplicativos Kaspersky com um idioma de localização específico.

   Clique no botão **Aplicar** para aplicar os filtros selecionados.

3. Selecione o aplicativo desejado a partir da lista.

4. Baixe o pacote de distribuição do aplicativo clicando no link na sequência de caracteres **Endereço da Web do pacote de distribuição**.

   As atualizações de aplicativos gerenciados podem exigir a instalação de uma versão mínima específica do Kaspersky Security Center. Se esta versão for posterior à versão atual, essas atualizações serão exibidas, mas não poderão ser aprovadas. Além disso, nenhum pacote de instalação pode ser criado a partir dessas atualizações até que você atualize o Kaspersky Security Center. Você receberá uma solicitação para atualizar sua instância do Kaspersky Security Center para a versão mínima necessária.

Se o botão **Baixar aplicativos e criar pacotes de instalação** for exibido para o aplicativo selecionado, clique nele para baixar o pacote de distribuição do aplicativo e criar um pacote de instalação automaticamente. O Kaspersky Security Center baixa o pacote de distribuição do aplicativo para o Servidor de Administração, para a pasta compartilhada especificada durante a instalação do Kaspersky Security Center. O pacote de instalação criado automaticamente é exibido na pasta **Instalação remota** na árvore do console, na subpasta **Pacotes de instalação**.

Depois de **Versões atuais do aplicativo** a janela está fechada, o **Existem novas versões de aplicativos Kaspersky disponíveis** o link desaparece do **Implementação** seção.

Você pode criar pacotes de instalação para novas versões de aplicativos e gerenciar pacotes de instalação recém criados na pasta **Instalação remota** na árvore do console, na subpasta **Pacotes de instalação**.

Você também pode abrir a janela **Versões atuais do aplicativo**, clicando no link **Ver versões atuais dos aplicativos Kaspersky** no espaço de trabalho para a pasta **Pacotes de instalação**.

Preparação de um dispositivo Windows para instalação remota

A instalação remota do aplicativo no dispositivo cliente poderá retornar um erro devido aos seguintes motivos:

- A tarefa já foi executada com êxito neste dispositivo.

  Nesse caso, a tarefa não tem de ser executada novamente.

- Quando a tarefa foi iniciada, o dispositivo foi desligado.

  Nesse caso, ligue o dispositivo, e em seguida, reinicie a tarefa.

- Não há conexão entre o Servidor de Administração e o Agente de Rede instalados no dispositivo cliente.

  Para determinar a causa do problema, use o utilitário projetado para o diagnóstico remoto nos dispositivos clientes (klactgui).

- Se o Agente de Rede não estiver instalado no dispositivo, podem ocorrer os seguintes problemas durante a instalação remota:

  - O dispositivo cliente possui **Desativar compartilhamento simples de arquivo** ativado.
  - O serviço do servidor não está sendo executado no dispositivo cliente.
  - As portas relevantes estão fechadas no dispositivo cliente.
  - A conta de usuário que é usada para executar a tarefa possui privilégios insuficientes.

  Para evitar problemas que possam ocorrer durante a instalação do aplicativo em um dispositivo cliente sem o Agente de Rede instalado, é necessário agir conforme o descrito no procedimento de implementação forçada por meio da tarefa de instalação remota do Kaspersky Security Center.

Anteriormente, o utilitário riprep foi usado para preparar um dispositivo para instalação remota. Agora, o procedimento é considerado um método desatualizado para configurar sistemas operacionais. O utilitário riprep não é recomendado para uso em sistemas operacionais mais recentes que Windows XP e Windows Server 2003 R2.

Preparar um dispositivo Linux e instalar o Agente de Rede em um dispositivo Linux remotamente

A instalação do Agente de Rede compreende duas etapas:

- Preparação de um dispositivo Linux
- Instalação remota do Agente de Rede

Preparação de um dispositivo Linux

Para preparar um dispositivo executando no Linux para a instalação remota do Agente de Rede:

1. Verifique e confirme se o dispositivo no qual deseja instalar o Agente de Rede para Linux está executando em uma das distribuições Linux compatíveis.
2. Baixe o pacote de instalação do Agente de Rede usando a interface do aplicativo ou no site da Kaspersky.
3. Certifique-se de que o software a seguir está instalado no dispositivo Linux de destino:
   - Sudo (para Ubuntu 10.04, a versão do Sudo é 1.7.2p1 ou posterior)
   - Intérprete de linguagem Perl versão 5.10 ou posterior

4. Testar a configuração do dispositivo:

   a. Verifique se você pode conectar-se ao dispositivo através de um cliente SSH (como PuTTY).

      Se não for possível se conectar ao dispositivo, abra o arquivo `/etc/ssh/sshd_config` e assegure-se de que as seguintes configurações têm os respectivos valores listados abaixo:

      ```
      PasswordAuthentication no
      ```

      ```
      ChallengeResponseAuthentication yes
      ```

      Não modifique o arquivo /etc/ssh/sshd_config caso possa se conectar ao dispositivo sem problemas. Caso contrário, poderá haver falha de autenticação SSH ao executar uma tarefa de instalação remota.

      Salve o arquivo (se necessário) e reinicie o serviço SSH usando o comando `sudo service ssh restart`.

   b. Desative a senha sudo para a conta do usuário sob a qual o dispositivo deve ser conectado.

   c. Use o comando `visudo` no sudo para abrir o arquivo de configuração sudoers.

      No arquivo aberto, adicione a seguinte linha ao final do arquivo: `<nome de usuário> ALL = (ALL) NOPASSWD: ALL`. Neste caso, o `< username >` é a conta de usuário que deve ser usada para a conexão de dispositivo usando o SSH. Caso esteja usando o sistema operacional Astra Linux, no arquivo /etc/sudoers, adicione a última linha com o seguinte texto: `%astra-admin ALL=(ALL:ALL) NOPASSWD: ALL`

   d. Salve o arquivo sudoers e, a seguir, feche-o.

   e. Conecte-se novamente ao dispositivo pelo SSH, verifique e confirme se o serviço Sudo não solicita a inserção de uma senha. Será possível fazer isso com o uso do comando `sudo whoami`.

5. Abra o arquivo `/etc/systemd/logind.conf` e proceda de uma das seguintes formas:

   - Especifique 'no' como valor para a configuração de KillUserProcesses: `KillUserProcesses=no`.
   - Para a configuração de KillExcludeUsers, digite o nome de usuário da conta sob a qual a instalação remota será executada, por exemplo `KillExcludeUsers=root`.

   Caso o dispositivo de destino esteja executando o Astra Linux, adicione a string `export PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin` no arquivo `/home/<nome de usuário>/.bashrc`, onde `< nome de usuário >` é a conta de usuário que deve ser usada para a conexão do dispositivo com o uso do SSH.

   Para aplicar a configuração alterada, reinicie o dispositivo Linux ou execute o comando a seguir:

   ```
   $ sudo systemctl restart systemd-logind.service
   ```

6. Caso queira instalar o agente de rede em dispositivos com o sistema operacional SUSE Linux Enterprise Server 15, instale o pacote insserv-compat primeiro para configurar o agente de rede.

7. Se você quiser instalar o Agente de Rede em dispositivos com o sistema operacional Astra Linux em execução no modo de ambiente de software fechado, execute as etapas adicionais para preparar os dispositivos Astra Linux.

8. Se você deseja instalar o Agente de Rede em dispositivos que usam o sistema operacional RED OS 7.3.4 ou posterior ou MSVSPHERE 9.2 ou posterior, instale o pacote libxcrypt-compat para a função correta do Agente de Rede.

Instalação remota do Agente de Rede

Para instalar o Agente de Rede em dispositivos Linux remotamente:

1. Baixar e criar um pacote de instalação:

   a. Antes da instalação no dispositivo, assegure-se que ele já tenha todas as dependências (programas e bibliotecas) instaladas para este pacote.

   Você pode exibir as dependências para cada pacote por si só, usando utilitários que são específicos para a distribuição Linux na qual o pacote deve ser instalado. Para obter mais detalhes sobre os utilitários, consulte a documentação de seu sistema operacional.

   b. Para criar um pacote de instalação remota, use os seguintes arquivos:

   - klnagent.kpd
   - akinstall.sh
   - Pacote .deb ou .rpm para Agente de Rede

2. Crie uma tarefa de instalação remota com as seguintes configurações:

   - Na página **Configurações** do Assistente para novas tarefas, marque a caixa de seleção **Uso dos recursos do sistema operacional por meio do Servidor de Administração**. Limpar todas as outras caixas de seleção.
   - Na página **Selecionar uma conta para executar a tarefa**, especifique as configurações da conta de usuário usadas para a conexão do dispositivo através de SSH.

3. Executar a tarefa de instalação remota. Use a opção para o comando `su` para preservar o ambiente: `-m, -p, --preserve-environment`.

Preparo de um dispositivo executando o SUSE Linux Enterprise Server 15 para instalação do agente de rede

Para instalar o agente de rede em um dispositivo com o sistema operacional SUSE Linux Enterprise Server 15,

Antes da instalação do agente de rede, execute o seguinte comando:

```
$ sudo zypper install insserv-compat
```

Isso permite a instalação do pacote insserv-compat e configure o agente de rede corretamente.

> Execute o comando `rpm -q insserv-compat` para verificar se o pacote já está instalado.

Caso a rede inclua muitos dispositivos executando o SUSE Linux Enterprise Server 15, será possível usar o software especial para configurar e gerenciar a infraestrutura da empresa. Ao usar o software, é possível instalar automaticamente o pacote insserv-compat em todos os dispositivos necessários de uma só vez. Por exemplo, é possível usar Puppet, Ansible, Chef ou, ainda, criar o próprio script – use qualquer método conveniente para você.

Se o dispositivo não tiver as chaves de assinatura GPG para o SUSE Linux Enterprise, o seguinte aviso poderá aparecer: `O cabeçalho do pacote não está assinado!` Selecione a opção `i` para ignorar a advertência.

Além da instalação do pacote insserv-compat, certifique-se de ter preparado os dispositivos Linux. Depois disso, implante e instale o agente de rede.

Preparar um dispositivo macOS para a instalação remota do Agente de Rede

Para preparar um dispositivo executando no macOS para a instalação remota do Agente de Rede:

1. Certifique-se de que o sudo esteja instalado no dispositivo macOS de destino.

2. Testar a configuração do dispositivo:

   a. Certifique-se de que a porta 22 esteja aberta no dispositivo cliente. Para fazer isso, nas **Preferências do Sistema**, abra o painel de **Compartilhamento** e, em seguida, verifique se a caixa de seleção **Login Remoto** está marcada.

      Você pode se conectar ao dispositivo cliente via Secure Shell (SSH) somente pela porta 22. Você não pode alterar o número da porta.

      Você pode usar o comando `ssh <nome_do_dispositivo>` para fazer login no dispositivo macOS remotamente. No painel **Compartilhamento**, você pode usar a opção **Permitir acesso para** definir o escopo dos usuários que têm acesso permitido ao dispositivo macOS.

   b. Desative a senha sudo para a conta do usuário sob a qual o dispositivo deve ser conectado.

      Use o comando `sudo visudo` no terminal para abrir o arquivo de configuração sudoers. No arquivo que você abriu, na entrada `User privilege specification`, especifique o seguinte: `username ALL = (ALL) NOPASSWD: ALL`. Neste caso, o campo `username` corresponde à conta de usuário, que deve ser usada para a conexão de dispositivo usando o SSH.

   c. Salve o arquivo sudoers e, a seguir, feche-o.

   d. Conecte-se novamente ao dispositivo por meio do SSH e assegure-se de que o serviço Sudo não solicita inserir uma senha. Você poderá fazer isso usando o comando `sudo whoami`.

3. Baixar e criar um pacote de instalação:

   a. Baixe o pacote de instalação do Agente de Rede usando um dos seguintes métodos:

      - Na árvore do console, abrindo o menu de contexto em **Instalação remota** → **Pacotes de instalação** e selecionando **Mostrar as versões atuais dos aplicativos** para escolher entre os pacotes disponíveis
      - Baixando a versão relevante do Agente de Rede no site de Suporte Técnico em https://support.kaspersky.com.br/
      - Solicitando o pacote de instalação aos especialistas do Suporte Técnico

   b. Para criar um pacote de instalação remota, use os seguintes arquivos:

      - klnagent.kud
      - install.sh
      - klnagentmac.dmg

4. Criar uma tarefa de instalação remota com as seguintes configurações:

   - Na página **Configurações** do Assistente para novas tarefas, marque a caixa de seleção **Usando recursos do sistema operacional através do Servidor de Administração**. Limpar todas as outras caixas de seleção.
   - Na página **Selecionar uma conta para executar a tarefa**, para executar a tarefa, especifique as configurações da conta de usuário que são usadas para a conexão do dispositivo por meio de SSH.

O dispositivo cliente está pronto para a instalação remota do Agente de Rede por meio da tarefa correspondente que foi criada.

Aplicativos Kaspersky: licenciamento e ativação

Esta seção descreve os recursos do Kaspersky Security Center relacionados ao trabalho com chaves de licença de aplicativos gerenciados da Kaspersky.

O Kaspersky Security Center lhe permite realizar a distribuição centralizada de chaves de licença para os aplicativos Kaspersky em dispositivos clientes, monitorar seu uso e renovar licenças.

Ao adicionar uma chave de licença usando o Kaspersky Security Center, as configurações da chave de licença são salvas no Servidor de Administração. Com base nestas informações, o aplicativo gera um relatório sobre o uso das chaves de licença e notifica o administrador sobre a expiração das licenças e sobre a violação das restrições de licença que estão definidas nas propriedades das chaves de licença. Você pode configurar as notificações do uso de chaves de licença dentro das configurações do Servidor de Administração.

Licenciamento de aplicativos gerenciados

Os aplicativos Kaspersky instalados em dispositivos gerenciados devem ser licenciados com a aplicação de um arquivo de chave ou um código de ativação à cada um dos aplicativos. Um arquivo de licença ou um código de ativação pode ser implementado nas seguintes formas:

- Implementação automática
- O pacote de instalação de um aplicativo gerenciado
- A tarefa de adicionar uma *chave de licença* para um aplicativo gerenciado
- Ativação manual de um aplicativo gerenciado

É possível adicionar uma nova chave de licença ativa ou reserva por qualquer um dos métodos listados acima. Um aplicativo da Kaspersky usa uma chave ativa no momento e armazena uma chave reserva para aplicar após a expiração da chave ativa. O aplicativo ao qual a chave de licença é adicionada define se a chave é ativa ou reserva. A definição da chave não depende do método usado para adicionar uma nova chave de licença.

Implementação automática

Se você usar aplicativos gerenciados diferentes e precisa implementar um arquivo de chave ou código de ativação específico para dispositivos, opte por outras formas de implementar aquele código de ativação ou arquivo de chave.

O Kaspersky Security Center lhe permite implementar automaticamente as chaves de licença disponíveis nos dispositivos. Por exemplo, três chaves de licença são armazenadas no repositório do Servidor de Administração. Se você selecionou a caixa de seleção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados** para todas as três chaves de licença. Um aplicativo de segurança da Kaspersky – por exemplo, Kaspersky Endpoint Security for Windows – é instalado nos dispositivos da organização. Um novo dispositivo é descoberto, no qual uma chave de licença deve ser implementada. O aplicativo determina, por exemplo, que duas das chaves de licença do repositório podem ser implementadas ao dispositivo: a chave de licença denominada *Key_1* e chave de licença denominada *Key_2*. Uma destas chaves de licença é implementada no dispositivo. Neste caso, não pode ser previsto qual das duas chaves de licença será implementada no dispositivo, porque a implementação automática de chaves de licença não é fornecida para nenhuma atividade do administrador.

Quando uma chave de licença é implementada, os dispositivos são recontados para aquela chave de licença. Você deve assegurar-se de que o número de dispositivos nos quais a chave de licença foi implementada não excede o limite da licença. Se o número de dispositivos exceder o limite de licença, todos os dispositivos que não foram cobertos pela licença serão terão o status *Crítico* atribuído.

Antes da implementação, o arquivo de chave ou o código de ativação deve ser adicionado ao repositório do Servidor de Administração.

Instruções de como proceder:

- Console de Administração:
  - Adição de uma chave de licença ao repositório do Servidor de Administração
  - Distribuição automática de uma chave de licença

  ou

- Kaspersky Security Center Web Console:
  - Adição de uma chave de licença ao repositório do Servidor de Administração
  - Distribuição automática de uma chave de licença

Observe que uma chave de licença distribuída automaticamente pode não ser exibida no repositório do Servidor de Administração virtual nos seguintes casos:

- A chave de licença não é válida para o aplicativo.
- O Servidor de Administração virtual não tem dispositivos gerenciados.
- A chave de licença já foi usada para dispositivos gerenciados por outro Servidor de Administração virtual e o limite no número de dispositivos foi atingido.

Adicionando um arquivo de chave ou código de ativação ao pacote de instalação de um aplicativo gerenciado

Por motivos de segurança, esta opção não é recomendada. Um arquivo de licença ou um código de ativação adicionado a um pacote de instalação pode se tornar comprometido.

Se você instalar um aplicativo gerenciado usando um pacote de instalação, poderá especificar um código de ativação ou um arquivo de chave neste pacote de instalação ou na política do aplicativo. A chave de licença será implementada nos dispositivos gerenciados no momento da próxima sincronização do dispositivo com o Servidor de Administração.

Instruções de como proceder:

- Console de Administração:
  - Criação de um pacote de instalação
  - Instalar aplicativos em dispositivos cliente

  ou

- Kaspersky Security Center Web Console: Adicionando uma chave de licença a um pacote de instalação

Implementação através da tarefa de adicionar uma chave de licença para um aplicativo gerenciado

Se você optar por usar a tarefa de *Adicionar chave de licença* para um aplicativo gerenciado, poderá selecionar a chave de licença que deve ser implementada nos dispositivos e selecionar os dispositivos de qualquer forma conveniente – por exemplo, selecionando um grupo de administração ou uma seleção de dispositivos.

Antes da implementação, o arquivo de chave ou o código de ativação deve ser adicionado ao repositório do Servidor de Administração.

Instruções de como proceder:

- Console de Administração:
  - Adição de uma chave de licença ao repositório do Servidor de Administração
  - Implementando uma chave de licença para dispositivos clientes

  ou
- Kaspersky Security Center Web Console:
  - Adição de uma chave de licença ao repositório do Servidor de Administração
  - Implementando uma chave de licença para dispositivos clientes

Adicionar um código de ativação ou um arquivo de chave manualmente nos dispositivos

Você pode ativar o aplicativo da Kaspersky instalado localmente usando as ferramentas fornecidas na interface do aplicativo. Consulte a documentação do aplicativo instalado.

Visualizando de informações sobre chaves de licença em uso

Para visualizar informações sobre chaves de licença em uso,

Na árvore do console, selecione a pasta **Licenças da Kaspersky**.

O espaço de trabalho da pasta exibe uma lista de chaves de licença usadas em dispositivos cliente.

Próximo a cada chave de licença, um ícone é exibido, correspondente ao tipo de uso:

-  – Informações sobre a chave de licença atual são recebidas de um dispositivo cliente conectado ao Servidor de Administração. O arquivo desta chave de licença é armazenado fora do Servidor de Administração.
-  – A chave de licença é armazenado no repositório do Servidor de Administração. A distribuição automática é desabilitada para esta chave de licença.
-  – A chave de licença é armazenado no repositório do Servidor de Administração. A distribuição automática é habilitada para esta chave de licença.

Você pode visualizar informações sobre as chaves de licença que são usadas para ativação do aplicativo em um dispositivo cliente, abrindo a janela de propriedades na seção **Aplicativos** da janela de propriedades do dispositivo cliente.

Para definir configurações atualizadas das chaves de licença do Servidor de Administração virtual, o Servidor de Administração envia uma solicitação para os servidores de ativação da Kaspersky ao menos uma vez por dia. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos.

Caso uma chave de licença seja recebida de um dispositivo cliente, não será possível exportá-la como um arquivo.

Adição de uma chave de licença ao repositório do Servidor de Administração

Adicionar uma chave de licença ao repositório do Servidor de Administração:

1. Na árvore do console, selecione a pasta **Licenças da Kaspersky**.
2. Inicie a tarefa de adição da chave de licença usando uma das seguintes formas:
   - Selecione **Adicionar código de ativação ou arquivo de chave** no menu de contexto da lista chaves de licença.
   - Ao clicar no link **Adicionar código de ativação ou arquivo de chave** no espaço de trabalho da lista de chaves de licença.
   - Clique no botão **Adicionar código de ativação ou arquivo de chave**.

   O Assistente para Adicionar chaves de licença é iniciado.
3. Selecione como deseja ativar o Servidor de Administração: usando um código de ativação ou um arquivo de chave.
4. Especifique o código de ativação ou um arquivo de chave.
5. Selecione a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados** caso queira distribuir uma chave de licença relevante na rede imediatamente. Caso esta opção não seja selecionada, será possível distribuir uma chave de licença manualmente mais tarde.

Como resultado, o arquivo de chave é baixado e o Assistente para Adicionar chaves de licença é finalizado. Agora, é possível visualizar a chave de licença adicionada na lista de licenças da Kaspersky.

Adição de uma chave de licença do Servidor de Administração

Para adicionar uma chave de licença do Servidor de Administração:

1. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
2. Na janela de propriedades do Servidor de Administração que é exibida, selecione a seção **Chaves de licença**.
3. Na seção **Chave de licença ativa**, clique no botão **Editar**.
4. Na janela exibida, adicione uma chave de licença clicando no botão **Adicionar**.

   O Assistente para Adicionar chaves de licença é iniciado.

Após a conclusão do assistente, será possível verificar se os recursos são exibidos no Console de Administração de acordo com a licença correspondente.

Remover uma chave de licença do Servidor de Administração

Para remover uma chave de licença do Servidor de Administração:

1. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
2. Na janela de propriedades do Servidor de Administração que é exibida, selecione a seção **Chaves de licença**.
3. Remova a chave de licença clicando no botão **Remover**.

   Isso remove a chave de licença.

Se uma chave reserva de licença tiver sido adicionada, ela se tornará automaticamente a chave de licença ativa após a remoção da anterior.

Após a chave de licença atual do Servidor de Administração ter sido removida, as funções Gerenciamento de patches e vulnerabilidades e Gerenciamento de dispositivos móveis se tornam indisponíveis. Você pode adicionar novamente uma chave de licença removida ou adicionar uma nova chave de licença.

Implementando uma chave de licença para dispositivos clientes

O Kaspersky Security Center permite distribuir uma chave de licença para dispositivos cliente usando a tarefa *Distribuição de chaves de licença*.

Antes da implementação, adicione uma chave de licença ao repositório do Servidor de Administração.

Para distribuir uma chave de licença aos dispositivos cliente:

1. Na árvore do console, selecione a pasta **Licenças da Kaspersky**.
2. No espaço de trabalho da lista de chaves de licença, clique no botão **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

   O **Assistente de criação de tarefa de ativação do aplicativo** é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
3. Na lista de aplicativos, selecione o aplicativo para o qual deseja criar uma tarefa.
4. Na etapa **Adicionar chave** do assistente, adicione a chave de licença com uma das seguintes opções:

   - Selecione a opção **Código de ativação** para adicionar um código de ativação do repositório do Kaspersky Security Center.

     Clique em **Selecionar**. Na janela aberta, selecione o código de ativação e clique em **OK**.

   - Selecione a opção **Arquivo de chave ou chave** e faça o seguinte:

     a. Clique em **Selecionar**.

     b. No menu de contexto, selecione uma das opções:

     - **Arquivo de chave de pasta**.

       Na janela que é aberta, selecione o arquivo de chave do dispositivo e clique em **Abrir**.

     - **Chave do repositório do Kaspersky Security Center**.

       Na janela exibida, selecione a chave no repositório do Kaspersky Security Center e clique em **OK**.
5. Se você quiser substituir a chave de licença ativa, desmarque a caixa de seleção padrão **Usar como chave reserva**.

   Por exemplo, isso é necessário quando a organização muda e a chave de outra organização é necessária no dispositivo; ou se a chave for emitida novamente e uma nova licença expirar antes da licença atual. Para evitar erros, é necessário desmarcar a caixa de seleção **Usar como chave reserva**.

   Caso queira mais informações sobre os problemas que podem ocorrer ao adicionar uma chave de licença ao Kaspersky Security Center Windows e como resolvê-los, consulte a base de conhecimento do Kaspersky Security Center.
6. Verifique as informações da chave de licença e clique em **Avançar**.

7. Nesta etapa do assistente, selecione os dispositivos aos quais deseja atribuir a tarefa de adicionar chave. É possível especificar dispositivos (até mil dispositivos) de uma das seguintes formas:

   - **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**. Neste caso, a tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

   - **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**. Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

   - **Atribuir a tarefa a uma seleção de dispositivos**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em uma seleção anteriormente criada. É possível especificar a seleção predefinida ou uma personalizada criada por você.

   - **Atribuir tarefa a um grupo de administração**. Neste caso, a tarefa é atribuída aos dispositivos incluídos no grupo de administração criado anteriormente.

8. Na etapa **Configurar agendamento da tarefa** do assistente, crie um agendamento para o início da tarefa:

- **Início agendado**:
  - Uma vez

    A tarefa é executada uma vez, na data e hora especificadas (por padrão, no dia em que a tarefa foi criada).

  - Manualmente

    A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

    Por padrão, esta opção está selecionada.

  - Quando novas atualizações são baixadas no repositório

    A tarefa é executada após as atualizações serem baixadas no repositório. Por exemplo, pode ser necessário usar esse agendamento para a tarefa Encontrar as vulnerabilidades e atualizações necessárias.

  - No surto de vírus

    A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

    - Antivírus para estações de trabalho e servidores de arquivo
    - Antivírus para defesa de perímetro
    - Antivírus para sistemas de correio

    Por padrão, todos os tipos de aplicativos estão selecionados.

    Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

  - Na conclusão de outra tarefa

    A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- Executar tarefas ignoradas

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

9. Na etapa **Definir o nome da tarefa** do assistente, especifique o nome para a tarefa. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

10. Na etapa **Concluir a criação da tarefa** do assistente, clique no botão **Concluir** para fechar o assistente.

    Se você desejar que tarefa inicie assim que o assistente for concluído, marque a caixa de seleção **Executar a tarefa após a conclusão do assistente**.

As tarefas criadas usando o **Assistente de criação de tarefa de ativação do aplicativo** são tarefas para dispositivos específicos armazenados na pasta **Tarefas** da árvore do console.

Você também pode criar um grupo ou uma tarefa de distribuição de chaves de licença usando o Assistente de criação de tarefa para um grupo de administração e para um dispositivo cliente.

Distribuição automática de uma chave de licença

O Kaspersky Security Center permite a distribuição automática de chaves de licença para os dispositivos gerenciados, se elas estiverem localizadas no repositório de chaves de licença do Servidor de Administração. A distribuição automática de chaves de licença não se aplica aos dispositivos na pasta **Dispositivos não atribuídos**.

Para distribuir automaticamente uma chave de licença para os dispositivos gerenciados:

1. Na árvore do console, selecione a pasta **Licenças da Kaspersky**.
2. No espaço de trabalho da pasta, selecione a chave de licença que você pretende distribuir automaticamente para os dispositivos.
3. Abra a janela Propriedades da chave de licença selecionada usando uma das seguintes formas:
   - Selecionando **Propriedades** no menu de contexto da chave de licença.
   - Ao clicar no link **Mostrar as propriedades da chave de licença** na caixa de informações para a chave de licença selecionada.
4. Na janela de propriedades da chave de licença que abrir, marque a caixa de seleção **Chave de licença automaticamente distribuída**. Feche a janela propriedades da chave de licença.

A chave de licença será distribuída automaticamente para todos os dispositivos compatíveis.

A distribuição de chaves de licença é realizada através do Agente de Rede. Não é criada nenhuma tarefa de distribuição de chaves de licença para o aplicativo.

Durante a distribuição automática de uma chave de licença, o limite de licenciamento no número de dispositivos é levado em consideração. (O limite de licenciamento é definido nas propriedades da chave de licença.) Se o limite de licenciamento for atingido, a distribuição dessa chave de licença nos dispositivos cessará automaticamente.

O Servidor de Administração virtual distribui automaticamente chaves de licença de seu repositório e do repositório do Servidor de Administração. Recomendamos que você:

- Use a tarefa *Adicionar chave de licença* para selecionar a chave de licença que deve ser implementada nos dispositivos.
- Evite desativar a opção **Permitir a implementação automática das chaves de licença deste Servidor de Administração virtual em seus dispositivos** nas configurações do Servidor de Administração virtual. Caso contrário, o Servidor de Administração virtual não distribuirá chaves de licença aos dispositivos, incluindo as chaves de licença do repositório do Servidor de Administração.

Caso a caixa de seleção **Chave de licença automaticamente distribuída** seja marcada na janela de propriedades da chave de licença, uma chave de licença será distribuída em sua rede imediatamente. Caso esta opção não seja selecionada, será possível distribuir uma chave de licença manualmente mais tarde.

Criação e visualização de um relatório de uso da chave de licença

Para criar um relatório sobre o uso de chaves de licença nos dispositivos cliente:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Selecione o modelo de relatório denominado **Relatório de uso da chave de licença** ou crie um novo modelo de relatório do mesmo tipo.

O espaço de trabalho do relatório sobre o uso das chaves de licença exibe informações sobre as chaves de licença ativas e de reserva usadas nos dispositivos cliente. O relatório também contém informações sobre dispositivos nos quais as chaves de licença são usadas e sobre as restrições especificadas nas propriedades dessas chaves de licença.

Visualizando informações sobre as chaves de licença do aplicativo

Para saber quais chaves de licença estão em uso para um aplicativo da Kaspersky:

1. Na árvore do console do Kaspersky Security Center, selecione o nó **Dispositivos gerenciados** e siga para a guia **Dispositivos**.
2. Clique com o botão direito do mouse para abrir o menu de contexto do dispositivo relevante e selecione **Propriedades**.
3. Na janela de propriedades do dispositivo que será aberta, selecione a seção **Aplicativos**.
4. Na lista de aplicativos que aparece, selecione o aplicativo cujas licenças você deseja visualizar e clique no botão **Propriedades**.
5. Na janela de propriedades do aplicativo que se abre, selecione a seção **Configurações**.

   As informações são exibidas no espaço de trabalho desta seção.

Exportação de um arquivo de chave de licença

Caso sua chave de licença seja excluída acidentalmente e houver o interesse de restaurá-la, é possível exportar um arquivo de chave de licença de outro Servidor de Administração.

Para exportar um arquivo de chave de licença, é necessário ter o direito **Exportar arquivo de chave** na área funcional **Funcionalidades gerais: Gerenciamento de chaves**.

Caso uma chave de licença seja recebida de um dispositivo cliente, não será possível exportá-la.

Para exportar uma chave de licença:

1. Na árvore do console, selecione a pasta **Licenças da Kaspersky**.
2. Na lista, selecione a chave de licença que você deseja exportar como um arquivo.
3. Na caixa de informações exibida, clique no link **Exportar arquivo de chave**.
4. Na janela exibida, especifique o caminho para a pasta onde deseja salvar um arquivo de chave de licença e especifique um nome de arquivo. Depois disso, clique em **Salvar**.

O arquivo de chave de licença no formato .key é exportado para a pasta selecionada.

Se a chave de licença exportada foi adicionada ao repositório do Servidor de Administração como um código de ativação e você quiser usá-la em outro Servidor de Administração, será necessário adicioná-la novamente como um código de ativação, não como um arquivo de chave. Caso contrário, ocorrerá um erro. Você precisa abrir o arquivo de chave de licença exportado em qualquer editor de texto conveniente e, em seguida, copiar o código de ativação.

Configuração da proteção da rede

Esta seção contém informações sobre a configuração manual de políticas e tarefas, funções de usuário, criação de uma estrutura de grupo de administração e hierarquia de tarefas.

Cenário: Configurar a proteção da rede

O Assistente de início rápido cria políticas e tarefas com as configurações padrão. Essas configurações podem ficar abaixo do ideal ou até mesmo não serem permitidas pela organização. Portanto, recomendamos que você ajuste essas políticas e tarefas e crie outras, se necessárias para a sua rede.

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- Servidor de Administração do Kaspersky Security Center instalado com êxito
- Kaspersky Security Center Web Console instalado com êxito (opcional)

- Cenário principal de instalação do Kaspersky Security Center concluído
- Concluiu o Assistente de início rápido ou criou manualmente as seguintes políticas e tarefas no grupo de administração **Dispositivos gerenciados**:
  - Política do Kaspersky Endpoint Security
  - Tarefa de grupo para atualizar o Kaspersky Endpoint Security
  - Política de Agente de Rede
  - Tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*

A configuração da proteção de rede continua em fases:

1. **Configuração e propagação de políticas e perfis da política de aplicativos Kaspersky**

   Para configurar e propagar as configurações dos aplicativos Kaspersky instalados nos dispositivos gerenciados, você pode usar duas abordagens de gerenciamento de segurança diferentes: centrado no dispositivo ou centrado no usuário. Essas duas abordagens também podem ser combinadas. Para implementar o gerenciamento de segurança centrado no dispositivo, você pode usar ferramentas fornecidas no Console de Administração baseado no Console de Gerenciamento Microsoft ou Kaspersky Security Center Web Console. O gerenciamento de segurança centrado no usuário pode ser implementado por meio do Kaspersky Security Center Web Console somente.

2. **Configuração de tarefas de gerenciamento remoto de aplicativos Kaspersky**

   Verifique as tarefas criadas com o Assistente de início rápido e faça o ajuste fino delas, se necessário.

   Instruções de como proceder:

   - Console de Administração:
     - Configurar a tarefa de grupo para atualizar o Kaspersky Endpoint Security
     - Agendar a tarefa Encontrar vulnerabilidades e atualizações necessárias
   - Kaspersky Security Center Web Console:
     - Configurar a tarefa de grupo para atualizar o Kaspersky Endpoint Security
     - As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias

   Se necessário, crie tarefas adicionais para gerenciar os aplicativos Kaspersky instalados nos dispositivos cliente.

3. **Avaliação e limitação da carga de eventos no banco de dados**

   As informações sobre eventos que ocorrem durante a operação de aplicativos gerenciados são transferidas de um dispositivo cliente e registradas no banco de dados do Servidor de Administração. Para reduzir a carga do Servidor de Administração, avalie e limite o número máximo de eventos que podem ser armazenados no banco de dados.

   Instruções de como proceder:

   - Console de Administração: Configuração do número máximo de eventos
   - Kaspersky Security Center Web Console: Configurar o número máximo de eventos

Resultados

Quando você concluir esse cenário, sua rede estará protegida pela configuração de aplicativos, tarefas e eventos da Kaspersky recebidos pelo Servidor de Administração:

- Os aplicativos Kaspersky são configurados de acordo com as políticas e perfis de política.
- Os aplicativos são gerenciados através de um conjunto de tarefas.
- O número máximo de eventos que podem ser armazenados no banco de dados está definido.

Quando a configuração da proteção de rede for concluída, você poderá prosseguir para configurar atualizações regulares para bancos de dados e aplicativos Kaspersky.

Para obter detalhes sobre como configurar respostas automáticas a ameaças detectadas pelo Kaspersky Sandbox, consulte a Ajuda Online do Kaspersky Sandbox 2.0.

Configuração e propagação de políticas: abordagem centrada no dispositivo

Quando você concluir este cenário, os aplicativos serão configurados em todos os dispositivos gerenciados em conformidade com as políticas de aplicativo e perfis da política definidos por você.

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha instalado o Servidor de Administração do Kaspersky Security Center e o Kaspersky Security Center Web Console (opcional). Se tiver instalado o Kaspersky Security Center Web Console, você também poderá considerar o gerenciamento de segurança centrado no usuário como uma alternativa ou opção adicional à abordagem centrada no dispositivo.

Fases

O cenário de gerenciamento centrado no dispositivo dos aplicativos Kaspersky consiste nas seguintes etapas:

1. **Configurar os políticas de aplicativo**

   Defina as configurações para aplicativos da Kaspersky instalados nos dispositivos gerenciados por meio da criação de uma política para cada aplicativo. Esse conjunto de políticas será propagado para os dispositivos clientes.

   Quando você configura a proteção da sua rede no Assistente de início rápido, o Kaspersky Security Center cria a política padrão para os seguintes aplicativos:

   - Kaspersky Endpoint Security for Windows – para dispositivos clientes baseados em Windows
   - Kaspersky Endpoint Security for Linux – para dispositivos clientes baseados em Linux

   Se tiver concluído o processo de configuração usando este assistente, você não precisará criar uma nova política para este aplicativo. Siga para a configuração manual da política do Kaspersky Endpoint Security.

Se você tiver uma estrutura hierárquica de vários Servidores de Administração e/ou grupos de administração, os Servidores de Administração secundários e os grupos de administração secundários herdarão as políticas do Servidor de Administração principal por padrão. Você pode forçar a herança pelos grupos secundários e Servidores de Administração secundários para proibir qualquer modificação das configurações definidas na política de fluxo acima. Se você quiser que somente uma parte das configurações seja herdada por imposição, poderá bloqueá-las na política de fluxo acima. O restante das configurações desbloqueadas ficarão disponíveis para modificação nas políticas de fluxo abaixo. A hierarquia de políticas criada permite que você gerencie dispositivos nos grupos de administração com mais eficiência.

Instruções de como proceder:

- Console de Administração: Criar uma política
- Kaspersky Security Center Web Console: Criar uma política

2 Criar os perfis da política (opcional)

Se você quiser que os dispositivos em um único grupo de administração seja executado sob diferentes configurações de política, crie perfis de políticas para esses dispositivos. Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos de destino em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo gerenciado.

Usando condições de ativação do perfil, você pode aplicar diferentes perfis de políticas, por exemplo, nos dispositivos localizados em uma unidade ou grupo de segurança específico do Active Directory, ter configuração de hardware específica ou marcada com tags específicas. Use tags para filtrar dispositivos que atendem a critérios específicos. Por exemplo, você pode criar um identificador denominado *Windows*, marcar todos os dispositivos executando o sistema operacional Windows com esse identificador e especificar esse identificador como uma condição de ativação para um perfil da política. Como resultado, os aplicativos Kaspersky instalados em todos os dispositivos executando o Windows serão gerenciados por seu próprio perfil da política.

Instruções de como proceder:

- Console de Administração:
  - Criar um perfil da política
  - Criar uma regra de ativação do perfil da política
- Kaspersky Security Center Web Console:
  - Criar um perfil da política
  - Criar uma regra de ativação do perfil da política

3 Propagar políticas e perfil da política para os dispositivos gerenciados

Por padrão, o Servidor de Administração sincroniza automaticamente com os dispositivos gerenciados a cada 15 minutos. Você pode ignorar a sincronização automática e executar a sincronização manualmente usando o comando Forçar a sincronização. Além disso, a sincronização é forçada depois que você cria ou altera a política ou um perfil da política. Durante a sincronização, as políticas novas ou alteradas e os perfis da política são propagados para os dispositivos gerenciados.

Se usar o Kaspersky Security Center Web Console, você poderá verificar se as políticas e os perfil da política foram entregues a um dispositivo. O Kaspersky Security Center especifica a data e hora de entrega nas propriedades do dispositivo.

Instruções de como proceder:

- Console de Administração: Sincronização forçada

- Kaspersky Security Center Web Console: Sincronização forçada

Resultados

Quando o cenário centrado no dispositivo for concluído, os aplicativos Kaspersky serão configurados segundo as configurações especificadas e propagadas por meio da hierarquia de políticas.

As políticas e perfis da política de aplicativo configuradas serão aplicadas automaticamente aos novos dispositivos adicionados aos grupos de administração.

Sobre as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário

Você pode gerenciar configurações de segurança do ponto de vista de recursos de dispositivo e do ponto de vista de funções de usuário. A primeira abordagem é chamada de *gerenciamento de segurança centrado no dispositivo*, e a segunda, *gerenciamento de segurança centrado no usuário*. Para aplicar configurações diferentes a dispositivos diferentes, é possível usar um dos tipos de gerenciamento ou ambos em conjunto. Para implementar o gerenciamento de segurança centrado no dispositivo, você pode usar ferramentas fornecidas no Console de Administração baseado no Console de Gerenciamento Microsoft ou Kaspersky Security Center Web Console. O gerenciamento de segurança centrado no usuário pode ser implementado por meio do Kaspersky Security Center Web Console somente.

O gerenciamento de segurança centralizado no dispositivo permite aplicar diferentes configurações de aplicativos de segurança aos dispositivos gerenciados, dependendo dos recursos específicos do dispositivo. Por exemplo, você pode aplicar configurações diferentes aos dispositivos alocados em diferentes grupos de administração. Você também pode diferenciar os dispositivos usando esses dispositivos no Active Directory ou suas especificações de hardware.

O gerenciamento de segurança centralizado no usuário permite aplicar diferentes configurações do aplicativo de segurança à diferentes funções do usuário. Você pode criar várias funções de usuário, atribuir uma função de usuário apropriada á cada usuário e definir configurações de aplicativos diferentes para os dispositivos pertencentes a usuários com funções diferentes. Por exemplo, convém aplicar configurações do aplicativo diferentes nos dispositivos de contadores e especialistas em recursos humanos (RH). Como resultado, quando o gerenciamento de segurança centrado no usuário é implementado, cada departamento, o departamento de contas e o departamento de RH, têm a sua própria configuração para os aplicativos Kaspersky. Uma configuração define qual configuração do aplicativo pode ser modificada pelos usuários e que são impostas e bloqueadas pelo administrador.

gerenciamento de segurança centrado no usuário, você pode aplicar configurações de aplicativo específicas a usuários individuais. Isso pode ser necessário quando um funcionário tem uma função única na empresa ou quando você quer controlar incidentes de segurança relacionados a dispositivos de uma pessoa específica. Dependendo da função desse funcionário na empresa, você pode expandir ou limitar os direitos dessa pessoa para alterar as configurações do aplicativo. Por exemplo, é possível expandir os direitos de um administrador do sistema que gerencia dispositivos clientes em um escritório local.

Você também pode combinar as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário. Por exemplo, você pode configurar uma política de aplicativo específica para cada grupo de administração e, adicionalmente, criar perfis de política para uma ou várias funções dos usuários da sua empresa. Nesse caso, as políticas e os perfis de política são aplicados na seguinte ordem:

1. As políticas criadas para o gerenciamento de segurança centrado no dispositivo são aplicadas.
2. Elas são modificadas pelos perfis de política segundo as prioridades de perfil de política.
3. As políticas são modificadas pelos perfis de política associados às funções de usuário.

Configuração manual da política do Kaspersky Endpoint Security

Esta seção fornece recomendações sobre como configurar a política do Kaspersky Endpoint Security, que é criada pelo Assistente de início rápido. Você pode executar a configuração na janela de propriedades da política.

Ao editar uma configuração, tenha em mente que é necessário clicar no ícone de cadeado acima da configuração pertinente para permitir usar o seu valor em uma estação de trabalho.

Configurar a política na seção Proteção Avançada Contra Ameaças

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Proteção Avançada Contra Ameaças**, é possível configurar o uso da Kaspersky Security Network para o Kaspersky Endpoint Security for Windows. Você também pode configurar os módulos do Kaspersky Endpoint Security for Windows, tal como a Detecção de Comportamento, Prevenção de Exploit, Prevenção de Intrusão do Host e Mecanismo de Correção.

Na subseção **a Kaspersky Security Network**, recomendamos a ativação da opção **Kaspersky Security Network**. Use esse recurso para redistribuir e otimizar o tráfego na rede. Se a opção **Kaspersky Security Network** estiver desativada, será possível ativar o uso direto de servidores KSN.

Configurar a política na seção Proteção Essencial Contra Ameaças

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Proteção Essencial Contra Ameaças** da janela de propriedades da política, recomendamos que especifique configurações adicionais nas subseções **Firewall** e **Proteção Contra Ameaças ao Arquivo**.

A subseção **Firewall** contém configurações que permitem controlar a atividade de rede dos aplicativos nos dispositivos cliente. Um dispositivo cliente usa uma rede à qual um dos seguintes status é atribuído: pública, local ou confiável. Dependendo do status da rede, o Kaspersky Endpoint Security pode permitir ou negar atividade de rede em um dispositivo. Ao adicionar uma nova rede à sua organização, você deve atribuir um status de rede apropriado a ela. Por exemplo, se o dispositivo cliente for um laptop, recomendamos que esse dispositivo use a rede pública ou confiável, porque o laptop nem sempre está conectado à rede local. Na subseção **Firewall**, é possível verificar se foram atribuídos corretamente os status às redes usadas na organização.

Para verificar a lista de redes:

1. Nas propriedades de política, acesse **Proteção Essencial Contra Ameaças → Firewall**.
2. Na seção **Redes disponíveis**, clique no botão **Configurações**.
3. Na janela **Firewall** que se abre, vá para a guia **Redes** para visualizar a lista de redes.

Na subseção **Proteção Contra Ameaças ao Arquivo**, é possível desativar a verificação de unidades de rede. A verificação das unidades de rede pode colocar uma carga significativa nas unidades de rede. É mais conveniente executar a verificação indireta em servidores de arquivos.

Para desativar a verificação de unidades de rede:

1. Nas propriedades de política, acesse **Proteção Essencial Contra Ameaças → Proteção Contra Ameaças ao Arquivo**.
2. Na seção **Nível de segurança**, clique no botão **Configurações**.
3. Na janela **Proteção Contra Ameaças ao Arquivo** que é aberta, na guia **Geral**, desmarque a caixa de seleção **Todas as unidades de rede**.

Configurar a política na seção Configurações Gerais

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Configurações gerais** da janela de propriedades da política, recomendamos que especifique configurações adicionais nas subseções **Relatórios e armazenamento** e **Interface**.

Na subseção **Relatórios e armazenamento**, vá para a seção **Transferência de dados para o Servidor de Administração**. A caixa de seleção **Sobre os aplicativos iniciados** especifica se o banco de dados do Servidor de Administração salvará as informações sobre todas as versões de todos os módulos do software nos dispositivos em rede. Se esta caixa de seleção for marcada, as informações salvas poderão necessitar de uma quantidade significativa do espaço disponível em disco para o banco de dados do Kaspersky Security Center (dúzias de gigabytes). Desmarque a caixa de seleção **Sobre os aplicativos iniciados** se estiver selecionada na política de nível superior.

Caso o Console de Administração gerencie a proteção contra ameaças na rede da organização no modo centralizado, desative a exibição da interface do usuário do Kaspersky Endpoint Security for Windows nas estações de trabalho. Para fazer isso, na subseção **Interface**, acesse a seção **Interação com o usuário** e, em seguida, marque a opção **Não exibir interface do usuário**.

Para ativar a proteção por senha nas estações de trabalho, na subseção **Interface**, acesse a seção **Proteção por senha**, clique no botão **Configurações** e, em seguida, marque a caixa de seleção **Ativar a proteção por senha**.

Configurando a política na seção Configuração de eventos

Na seção **Configuração de eventos**, é necessário desativar a função de salvar quaisquer eventos no Servidor de Administração, exceto os seguintes:

- Na guia **Crítico**:
  - *A execução automática do aplicativo está desativada*
  - *Acesso negado*
  - *Proibida a inicialização do aplicativo*
  - *Não é possível desinfectar*
  - *O Contrato de Licença do Usuário Final foi violado*
  - *Não foi possível carregar o módulo de criptografia*
  - *Não é possível iniciar duas tarefas simultaneamente*
  - *Ameaça ativa detectada. A Desinfecção avançada deve ser iniciada*
  - *Ataque de rede detectado*
  - *Nem todos os componentes foram atualizados*
  - *Erro de ativação*
  - *Erro ao ativar o modo portátil*
  - *Erro de interação com o Kaspersky Security Center*
  - *Erro ao desativar o modo portátil*
  - *Erro ao alterar componentes do aplicativo*
  - *Erro na aplicação das regras de criptografia/descriptografia do arquivo*
  - *A política não pode ser aplicada*
  - *Processo encerrado*
  - *Atividade de rede bloqueada*
- Na guia **Falha funcional**: *Configurações de tarefa inválidas. Configurações não aplicadas*

- Na guia **Advertência**:
  - *A Autodefesa está desativada*
  - *Chave de reserva inválido*
  - *O usuário optou por cancelar a política de criptografia*
- Na guia **Informações**: *Proibida a inicialização do aplicativo em modo de teste*

Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security

A opção de agendamento ideal e recomendada para o Kaspersky Endpoint Security versões 10 e posteriores é **Quando novas atualizações são baixadas no repositório** quando a caixa de seleção **Usar atraso aleatório automaticamente para início da tarefa** estiver marcada.

Configuração manual da tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security

O Assistente de início rápido cria uma tarefa de grupo para verificar um dispositivo. Por padrão, à tarefa é atribuído um agendamento **Executar às sextas-feiras as 19:00** com aleatorização automática e se a caixa de seleção **Executar tarefas ignoradas** estiver desmarcada.

Isto significa que se os dispositivos em uma organização são desligados às sextas-feiras, por exemplo, às 18:30, a tarefa de verificação de dispositivo nunca será executada. Você deve definir o agendamento mais conveniente para esta tarefa com base nas regras do local de trabalho adotadas na organização.

Agendar a tarefa Encontrar vulnerabilidades e atualizações necessárias

O Assistente de início rápido cria a tarefa *Encontrar vulnerabilidades e atualizações necessárias* para o Agente de Rede. Por padrão, à tarefa é atribuído um agendamento **Executar às terças-feiras as 19:00** com aleatorização automática e se a caixa de seleção **Executar tarefas ignoradas** estiver marcada.

Se as regras do local de trabalho da organização proverem o desligamento de todos os dispositivos nessa hora, a tarefa *Encontrar vulnerabilidades e atualizações necessárias* será executada após os dispositivos serem novamente ligados, ou seja, na quarta-feira pela manhã. Tal atividade pode ser indesejável porque uma verificação de vulnerabilidades pode aumentar a carga de subsistemas de disco e da CPU. Você deve definir o agendamento mais conveniente para a tarefa com base nas regras do local de trabalho adotadas na organização.

Configuração manual da tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades

O Assistente de início rápido cria uma tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades para o Agente de Rede. Por padrão, a tarefa é configurada para ser executada todos os dias à 1h, com randomização automática, e a opção **Executar tarefas perdidas** não está habilitada.

Se as regras do local de trabalho da organização proverem o desligamento dos dispositivos durante a noite, a instalação da atualização nunca será executada. Você deve definir o agendamento mais conveniente da tarefa de verificação de vulnerabilidades com base nas regras do local de trabalho adotadas na organização. Também é importante ter em mente que a instalação das atualizações pode necessitar o reinício do dispositivo.

Configuração do número máximo de eventos no repositório de eventos

Na seção **Repositório de eventos** da janela Propriedades do Servidor de Administração, você pode editar as configurações de armazenamento do evento no banco de dados do Servidor de Administração ao limitar o número de registros de evento ou o tempo de armazenamento do registro. Quando você especifica o número máximo de eventos, o aplicativo calcula um volume aproximado do espaço de armazenamento necessário para o número especificado. Você pode usar esse cálculo aproximado para avaliar se você tem espaço livre suficiente no disco para evitar sobrecarga do banco de dados. A capacidade padrão do banco de dados do Servidor de Administração é de 400.000 eventos. A capacidade máxima recomendada do banco de dados é de 45 milhões de eventos.

O aplicativo verifica o banco de dados a cada 10 minutos. Caso o número de eventos atinja o valor máximo especificado em mais de 10.000, o aplicativo exclui os eventos mais antigos para que apenas o número máximo de eventos especificado permaneça.

Quando o Servidor de Administração exclui eventos antigos, não pode salvar novos eventos no banco de dados. Durante esse período de tempo, as informações sobre eventos rejeitados são gravadas no Log de Eventos Kaspersky. Os novos eventos são colocados em fila e salvos no banco de dados depois que a operação de exclusão é concluída.

Para limitar o número de eventos que podem ser armazenados no repositório de eventos no Servidor de Administração:

1. Clique com o botão direito do mouse no Servidor de Administração e depois selecione **Propriedades**.

   A janela Propriedades do Servidor de Administração é aberta.

2. No espaço de trabalho da seção **Repositório de eventos**, especifique o número máximo de eventos armazenados no banco de dados.

3. Clique em **OK**.

Além disso, é possível alterar as configurações de qualquer tarefa para salvar eventos relacionados ao andamento da tarefa ou salvar apenas os resultados de execução da tarefa. Ao fazer isso, você reduzirá o número de eventos no banco de dados, aumentará a velocidade da execução dos cenários associados com a análise da tabela de eventos no banco de dados e abaixará o risco de que os eventos críticos sejam substituídos por um grande número de eventos.

Definindo o período máximo de armazenamento para as informações sobre vulnerabilidades corrigidas

Para definir o período máximo de armazenamento no banco de dados para as informações sobre as vulnerabilidades que já foram corrigidas em dispositivos gerenciados:

1. Clique com o botão direito do mouse no Servidor de Administração e depois selecione **Propriedades**.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na área de trabalho da seção **Repositório de eventos**, especifique o período máximo de armazenamento para as informações sobre as vulnerabilidades corrigidas no banco de dados.

   Por padrão, o período de armazenamento é de 90 dias.

3. Clique em **OK**.

O período máximo de armazenamento para as informações sobre as vulnerabilidades corrigidas é limitado ao número especificado de dias. Depois disso, a tarefa de manutenção do Servidor de Administração excluirá as informações desatualizadas do banco de dados.

Tarefas de gerenciamento

O Kaspersky Security Center gerencia os aplicativos instalados nos dispositivos cliente criando e executando diversas tarefas. As tarefas são necessárias para a instalação, inicialização e interrupção de aplicativos, verificação de arquivos, atualização de bancos de dados e módulos de software e para a realização de outras ações em aplicativos.

As tarefas estão subdivididas nos seguintes tipos:

- *Tarefas de grupo*. Tarefas que são executadas em dispositivos do grupo de administração selecionado.
- *Tarefas do Servidor de Administração*. Tarefas que são executadas no Servidor de Administração.
- *Tarefas para dispositivos específicos*. Tarefas que são executadas em dispositivos selecionados, independentemente se os mesmos estão incluídos em qualquer grupo de administração.
- *Tarefas locais*. Tarefas que são executadas em um dispositivo específico.

Uma tarefa de aplicativo pode ser criada somente se o plugin de gerenciamento daquele aplicativo estiver instalado na estação de trabalho do administrador.

É possível compilar uma lista de dispositivos (até mil dispositivos) para os quais uma tarefa será criada de uma das seguintes formas:

- Selecionando os dispositivos na rede descobertos pelo Servidor de Administração.
- Especificando uma lista de dispositivos manualmente. Você pode usar um endereço IP (ou uma faixa IP), nome NetBIOS ou nome DNS como o endereço do dispositivo.
- Importe uma lista de dispositivos de um arquivo txt com os endereços de dispositivos a adicionar (cada endereço deve ser colocado como uma linha individual).

  Se você importar uma lista de dispositivos a partir de um arquivo ou cria uma lista manualmente, e os dispositivos cliente estão identificados pelos seus nomes, a lista deve conter somente os dispositivos cuja informação já foi adicionada ao banco de dados do Servidor de Administração ao conectar estes dispositivos ou durante uma descoberta de dispositivos.

Para cada aplicativo, você pode criar qualquer número de tarefas de grupo, tarefas para dispositivos específicos ou tarefas locais.

A troca de informações sobre as tarefas entre um aplicativo instalado em um dispositivo cliente e o banco de dados do Kaspersky Security Center é realizada no momento em que o Agente de Rede for conectado ao Servidor de Administração.

Você pode efetuar alterações nas configurações de tarefas, exibir o andamento das tarefas, copiar, exportar, importar e excluir tarefas.

As tarefas somente são iniciadas em um dispositivo cliente se um aplicativo para o qual a tarefa foi criada estiver sendo executado. Se o aplicativo não estiver sendo executado, todas as tarefas em execução são canceladas.

Os resultados das tarefas concluídas são salvos nos registros de evento do Microsoft Windows e do Kaspersky Security Center, tanto centralmente no Servidor de Administração como localmente em cada dispositivo.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Detalhes de tarefas de gerenciamento para aplicativos com suporte a multiinquilinato

Uma tarefa de grupo para um aplicativo com o suporte a multiinquilinato é aplicada ao aplicativo, dependendo da hierarquia dos Servidores de Administração e dos dispositivos cliente. O Servidor de Administração virtual do qual a tarefa é criada deve estar no mesmo grupo ou em um grupo de administração de nível mais baixo do que o dispositivo cliente no qual o aplicativo está instalado.

Nos eventos que correspondem a resultados de execução de tarefas, as informações sobre o dispositivo no qual a tarefa foi executada são mostradas a um administrador do provedor de serviços. Por outro lado, em uma administração de locatários, é mostrado o **Nó multilocatário**.

Criar uma tarefa

No Console de Administração, você pode criar tarefas diretamente na pasta do grupo de administração para o qual a tarefa de grupo deve ser criada, ou no espaço de trabalho da pasta **Tarefas**.

Para criar uma tarefa de grupo na pasta de um grupo de administração:

1. Na árvore do console, selecione o grupo de administração para o qual você deseja criar uma tarefa.
2. No espaço de trabalho do grupo, selecione a guia **Tarefas**.
3. Execute a criação da tarefa, clicando no botão **Criar uma tarefa**.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

*Para criar uma tarefa no espaço de trabalho da pasta **Tarefas**:*

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Execute a criação da tarefa, clicando no botão **Finalizar**.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Criação de uma tarefa do Servidor de Administração

O Servidor de Administração realiza as seguintes tarefas:

- Entregar relatórios
- Baixar atualizações no repositório do Servidor de Administração
- Backup de dados do Servidor de Administração
- Manutenção do Servidor de Administração
- Executar a sincronização com o Windows Update
- Criar pacote de instalação com a imagem do SO do dispositivo de referência
- Instalar aplicativo remotamente
- Desinstalar aplicativo remotamente
- Distribuir pacote de instalação
- Instalar aplicativos nos Servidores de Administração secundários remotamente

Em um Servidor de Administração virtual, somente a tarefa de entrega de relatório automática e a tarefa de criação de pacote de instalação a partir da imagem do SO de um dispositivo referência estão disponíveis. O repositório do Servidor de Administração virtual exibe as atualizações baixadas para o Servidor de Administração principal. O backup de dados do Servidor de Administração virtual é realizado juntamente com o Backup de dados do Servidor de Administração principal.

Para criar uma tarefa do Servidor de Administração:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Inicie a criação da tarefa em uma das seguintes formas:
   - Selecionando **Nova → Tarefa** no menu de contexto da pasta **Tarefas** na árvore do console.
   - Clicando no botão **Criar uma tarefa** no espaço de trabalho da pasta **Tarefas**.

O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

As tarefas Baixar atualizações para o repositório do Servidor de Administração, Executar a sincronização com o Windows Update, Manutenção do Servidor de Administração e *Backup de dados do Servidor de Administração* podem ser criadas apenas uma vez. Caso as tarefas *Baixar atualizações para o repositório do Servidor de Administração*, *Manutenção do Servidor de Administração*, *Backup de dados do Servidor de Administração* e *Executar a sincronização com o Windows Update* já tenham sido criadas pelo Servidor de Administração, elas não serão exibidas na janela de seleção de tipo de tarefa do Assistente para novas tarefas.

Criar uma tarefa para dispositivos específicos

No Kaspersky Security Center, você poderá criar tarefas para dispositivos específicos. Os dispositivos que estejam em um conjunto podem ser incluídos em vários grupos de administração ou permanecerem fora de qualquer grupo de administração. O Kaspersky Security Center pode executar as seguintes tarefas principais para dispositivos específicos:

- Instalar um aplicativo remotamente
- Enviar mensagem a usuário
- Alterar o Servidor de Administração
- Dispositivos gerenciados
- Verificar atualizações
- Distribuir pacotes de instalação
- Instalar aplicativos nos Servidores de Administração secundários remotamente
- Desinstalar um aplicativo remotamente

Para criar uma tarefa para dispositivos específicos:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Inicie a criação da tarefa em uma das seguintes formas:
   - Selecionando **Novo → Tarefa** no menu de contexto da pasta **Tarefas** na árvore do console.
   - Clicando no botão **Criar uma tarefa** no espaço de trabalho da pasta **Tarefas**.

O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

Criação de uma tarefa local

Para criar uma tarefa local para um dispositivo:

1. Selecione a guia **Dispositivos** no espaço de trabalho do grupo que inclua o dispositivo.
2. Na lista de dispositivos na guia **Dispositivos**, selecione o dispositivo para o qual deve ser criada uma tarefa local.
3. Comece criando a tarefa para o dispositivo selecionado usando uma das seguintes formas:
   - Clique no botão **Executar a ação** e selecione **Criar uma tarefa** na lista suspensa.
   - Clique no link **Criar uma tarefa** no espaço de trabalho do dispositivo.
   - Use as propriedades do dispositivo como se segue:
     a. No menu de contexto do dispositivo, selecione **Propriedades**.
     b. Na janela de propriedades do dispositivo que será aberta, selecione a seção **Tarefas** e clique em **Adicionar**.

O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

São fornecidas instruções detalhadas sobre como criar e configurar tarefas locais nos Guias dos respectivos aplicativos Kaspersky.

Exibição de uma tarefa de grupo herdada no espaço de trabalho de um grupo hospedado

Para habilitar a exibição de tarefas herdadas de um grupo alojado no espaço de trabalho:

1. Selecione a guia **Tarefas** no espaço de trabalho de um grupo alojado.
2. No espaço de trabalho da pasta **Tarefas**, clique no botão **Exibir tarefas herdadas**.

As tarefas herdadas serão exibidas na lista de tarefas com um dos seguintes ícones:

-  – Se elas foram herdadas de um grupo criado no Servidor de Administração principal.
-  – Se elas foram herdadas de um grupo de nível superior.

Se o modo de herança estiver ativado, as tarefas herdadas só podem ser editadas no grupo em que as mesmas foram criadas. As tarefas herdadas não podem ser editadas no grupo que as herda.

Ativar automaticamente os dispositivos antes de iniciar uma tarefa

O Kaspersky Security Center não executa tarefas em dispositivos desligados. Você pode configurar o Kaspersky Security Center para ligar esses dispositivos automaticamente antes de iniciar uma tarefa, usando a função Wake-on-LAN.

Para configurar a ativação automática de dispositivos antes de iniciar uma tarefa:

1. Na janela de propriedades da tarefa, selecione a seção **Agendamento**.
2. Para configurar ações em dispositivos, clique no link **Avançado**.
3. Na janela **Avançado** que se abre, marque a caixa de seleção **Ligar dispositivos usando a função Wake-On-LAN antes de iniciar a tarefa (min.)** e especifique o intervalo de tempo em minutos.

Como resultado, durante o número de minutos especificado antes de iniciar a tarefa, o Kaspersky Security Center liga os dispositivos e carrega o sistema operacional neles usando a função Wake-on-LAN. Depois que a tarefa for concluída, os dispositivos serão desligados automaticamente se os usuários do dispositivo não fizerem login no sistema. Observe que o Kaspersky Security Center desliga automaticamente apenas os dispositivos que estão ligados usando a função Wake-on-LAN.

O Kaspersky Security Center pode iniciar sistemas operacionais automaticamente apenas nos dispositivos compatíveis com o padrão Wake-on-LAN (WoL).

Desativar automaticamente um dispositivo após a conclusão de uma tarefa

O Kaspersky Security Center permite definir as configurações de uma tarefa de tal modo que os dispositivos aos quais elas são distribuídos sejam automaticamente desligados após a conclusão da tarefa.

Para desligar automaticamente um dispositivo após a conclusão de uma tarefa:

1. Na janela de propriedades da tarefa, selecione a seção **Agendamento**.
2. Clique no link **Avançado** para abrir a janela para configurar ações em dispositivos.
3. Na janela **Avançado** que se abre, selecione a caixa de seleção **Desligar os dispositivos após concluir a tarefa**.

Limitação do tempo de execução de tarefas

Para limitar o tempo durante o qual uma tarefa é executada nos dispositivos:

1. Na janela de propriedades da tarefa, selecione a seção **Agendamento**.
2. Abra a janela elaborada para a configuração de ações em dispositivos cliente, clicando no link **Avançado**.
3. Na janela **Avançado** que se abre, selecione a caixa de seleção **Parar a tarefa se ela for executada por mais que (min.)** e especifique o intervalo de tempo em minutos.

Se a tarefa ainda não estiver concluída quando o intervalo de tempo especificado expirar, o Kaspersky Security Center interrompe a execução da tarefa automaticamente.

Exportação de tarefa

Você poderá exportar tarefas de grupo e tarefas para dispositivos específicos para um arquivo. As tarefas do Servidor de Administração não estão disponíveis para exportação.

Para exportar uma tarefa:

1. No menu de contexto da tarefa, selecione **Todas as tarefas** → **Exportar**.
2. Na janela **Salvar como** que for aberta, especifique o nome e o caminho do arquivo.
3. Clique no botão **Salvar**.

Os direitos dos usuários locais não são exportados.

Importação de uma tarefa

Você poderá importar tarefas de grupo e tarefas para dispositivos específicos. As tarefas do Servidor de Administração não estão disponíveis para importação.

Para importar uma tarefa:

1. Selecione a lista para a qual a tarefa deve ser importada:
   - Se você desejar importar a tarefa para a lista de tarefas de grupo, no espaço de trabalho do grupo de administração relevante selecione a guia **Tarefas**.
   - Se você desejar importar uma tarefa para a lista de tarefas para dispositivos específicos, selecione a pasta **Tarefas** na árvore do console.
2. Selecione uma das seguintes opções para importar a tarefa:
   - No menu de contexto da lista de tarefas, selecione **Todas as tarefas** → **Importar**.
   - Clique no link **Importar tarefa de um arquivo** no bloco de gerenciamento da lista de tarefas.
3. Na janela que se abre, especifique o caminho para o arquivo a partir do qual você deseja importar uma tarefa.
4. Clique no botão **Abrir**.

A tarefa é exibida na lista de tarefas.

Se a tarefa recém-importada tiver um nome idêntico a uma tarefa existente, o nome da tarefa importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Conversão de tarefas

Você pode usar o Kaspersky Security Center para converter tarefas de versões mais antigas dos aplicativos Kaspersky para as tarefas de versões atualizadas dos mesmos aplicativos.

A conversão está disponível para as tarefas dos seguintes aplicativos:

- Kaspersky Anti-Virus 6.0 for Windows Workstations MP4
- Kaspersky Endpoint Security 8 for Windows
- Kaspersky Endpoint Security 10 for Windows

Para converter tarefas:

1. Na árvore do console, selecione um Servidor de Administração para o qual você pretende converter tarefas.
2. No menu de contexto do Servidor de Administração, selecione **Todas as tarefas → Assistente de conversão de políticas e tarefas em lotes**.

O Assistente de conversão de políticas e tarefas em lotes é iniciado. Siga as instruções do Assistente.

Depois de o Assistente concluir sua operação, são criadas novas tarefas, que usam as configurações das tarefas de versões mais antigas dos aplicativos.

Início e interrupção manual de uma tarefa

Você pode iniciar e parar tarefas manualmente usando um dos seguintes métodos: a partir do menu de contexto da tarefa ou na janela Propriedades do dispositivo cliente para o qual esta tarefa foi atribuída.

O início de tarefas de grupo a partir do menu de contexto do dispositivo somente é permitido para usuários incluídos no **grupo** KL Admins.

Para iniciar ou parar uma tarefa no menu de contexto ou na janela de propriedades da tarefa:

1. Na lista de tarefas, selecione uma tarefa.
2. Inicie ou pare a tarefa numa das seguintes formas:
   - Ao selecionar **Iniciar** ou **Parar** no menu de contexto da tarefa.
   - Clicando **Iniciar** ou **Parar** na seção **Geral** da janela Propriedades da tarefa.

Para iniciar ou parar uma tarefa no menu de contexto ou na janela Propriedades do dispositivo cliente:

1. Na lista de dispositivos, selecione o dispositivo.
2. Inicie ou pare a tarefa numa das seguintes formas:
   - Selecionando **Todas as tarefas** → **Executar a tarefa** no menu de contexto do dispositivo. Selecione a tarefa relevante na lista de tarefas.

     A lista de dispositivos aos quais a tarefa é atribuída será substituída pelo dispositivo que você selecionou. A tarefa é iniciada.
   - Ao clicar no botão Iniciar () ou no botão Parar () na seção **Tarefas** da janela de propriedades do dispositivo.

Pausa e continuação manual de uma tarefa

Para pausar ou continuar o funcionando da tarefa manualmente:

1. Na lista de tarefas, selecione uma tarefa.
2. Para pausar ou retomar a tarefa em uma das seguintes formas:
   - Ao selecionar **Pausar** ou **Retomar** no menu de contexto da tarefa.
   - Selecionando a seção **Geral** na janela Propriedades de tarefa e clicando em **Pausar** ou **Retomar**.

Monitoramento de execução de tarefa

Para monitorar a execução de tarefa,

na janela de propriedades da tarefa, selecione a seção **Geral**.

Na parte central da seção **Geral**, é exibido o status da tarefa atual.

Visualização de resultados da execução de tarefas armazenados no Servidor de Administração

O Kaspersky Security Center lhe permite visualizar resultados de execução para tarefas de grupo, tarefas para dispositivos específicos e tarefas do Servidor de Administração. Não podem ser visualizados resultados de execução para tarefas locais.

Para visualizar os resultados da tarefa:

1. Na janela de propriedades da tarefa, selecione a seção **Geral**.
2. Clique no link **Resultados** para abrir a janela **Resultados da tarefa**.

Configuração da filtragem de informações sobre resultados da execução de tarefas

O Kaspersky Security Center lhe permite filtrar informações sobre resultados de execução para tarefas de grupo, tarefas para dispositivos específicos e tarefas do Servidor de Administração. A filtragem não está disponível para as tarefas locais.

Para configurar a filtragem de informações sobre os resultados da execução de tarefas:

1. Na janela de propriedades da tarefa, selecione a seção **Geral**.
2. Clique no link **Resultados** para abrir a janela **Resultados da tarefa**.

   A tabela na parte superior da janela contém todos os dispositivos para os quais a tarefa está atribuída. A tabela na parte inferior da janela exibe os resultados da tarefa executada no dispositivo selecionado.
3. Clique com o botão direito do mouse na tabela relevante para abrir o menu de contexto e selecione **Filtro**.
4. Na janela **Definir filtro** que se abre, defina as configurações do filtro nas seções **Eventos**, **Dispositivos** e **Hora**. Clique em **OK**.

A janela **Resultados da tarefa** exibe as informações que cumprem com as configurações especificadas no filtro.

Modificar uma tarefa. Reverter modificações

Para modificar uma tarefa:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Na área de trabalho da pasta **Tarefas**, selecione uma tarefa e prossiga à janela Propriedades da tarefa usando o menu de contexto.
3. Efetuar as alterações relevantes.

   Na seção **Exclusões do escopo da tarefa**, você poderá definir a lista de subgrupos aos quais a tarefa não será aplicada.
4. Clique em **Aplicar**.

As modificações feitas à tarefa serão salvas na janela de propriedades de tarefa, na seção **Histórico de revisões**.

Você poderá reverter as alterações feitas a uma tarefa, se necessário.

Para reverter as alterações feitas em uma tarefa:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Selecione a tarefa na qual as modificações devem ser revertidas, e siga para a janela Propriedades da tarefa usando o menu de contexto.

3. Na janela de propriedades da tarefa, selecione a seção **Histórico de revisões**.

4. Na lista de revisões de tarefa, selecione o número da revisão para a qual você precisa reverter as modificações.

5. Clique no botão **Avançado** e selecione o valor **Reverter** na lista suspensa.

Comparar tarefas

Você pode comparar tarefas do mesmo tipo: por exemplo, você pode comparar duas tarefas de verificação de malwares, mas não pode comparar uma tarefa de verificação de malwares com uma tarefa de instalação de atualização. Após a comparação, você tem um relatório que exibe quais configurações das tarefas coincidem e quais configurações se diferenciam. Você pode imprimir o relatório de comparação de tarefa ou salvá-lo como um arquivo. Você pode precisar da comparação de tarefa quando à diferentes unidades dentro de uma empresa são atribuídas diversas tarefas do mesmo tipo. Por exemplo, os funcionários no departamento de contabilidade têm uma tarefa da verificação de malware somente nos discos locais de seus dispositivos, enquanto os funcionários no departamento de vendas se comunicam com clientes, portanto, eles têm uma tarefa de verificação de discos locais e e-mails. Você não tem de exibir todas as configurações de tarefa para notar rapidamente tal a diferença; basta simplesmente comparar as tarefas.

Somente as tarefas do mesmo tipo podem ser comparadas.

As tarefas somente podem ser comparadas em pares.

Você pode comparar tarefas em uma de seguintes formas: selecionando uma tarefa e comparando-a com outra, ou comparando quaisquer de duas tarefa da lista de tarefas.

Para selecionar uma tarefa e compará-la com outra:

1. Na árvore do console, selecione a pasta **Tarefas**.

2. No espaço de trabalho da pasta **Tarefas**, selecione a tarefa que você deseja comparar com outra.

3. No menu de contexto da tarefa, selecione **Todas as tarefas → Comparar com outra tarefa**.

4. Na janela **Selecionar uma tarefa**, selecione a tarefa para comparação.

5. Clique em **OK**.

É exibido um relatório no formato de HTML que compara as duas tarefas.

Para comparar quaisquer de duas tarefa da lista de tarefas:

1. Na árvore do console, selecione a pasta **Tarefas**.

2. Na pasta **Tarefas**, na lista de tarefas, pressione a tecla **`Shift`** ou **`Ctrl`** para selecionar duas tarefas do mesmo tipo.

3. No menu de contexto, selecione **Comparar**.

É exibido um relatório no formato de HTML que compara as tarefas selecionadas.

Quando as tarefas são comparadas, se as senhas se diferenciarem, asteriscos (******) são exibidos no relatório de comparação de tarefa.

Se a senha tiver sido alterada nas propriedades da tarefa, asteriscos (******) são exibidos no relatório de comparação de revisão (******).

Contas para iniciar tarefas

Você pode especificar uma conta sob a qual a tarefa deve ser executada.

Por exemplo, para executar uma tarefa de verificação sob demanda, você precisará ter direitos de acesso ao objeto sendo verificado, e para executar uma tarefa de atualização, você precisará ter direitos de usuário autorizado do servidor proxy. A oportunidade para especificar uma conta para a execução da tarefa lhe permite evitar problemas com a verificação sob demanda e tarefas de atualização quando o usuário que executa a tarefa não possui os direitos de acesso necessários.

Durante a execução das tarefas de instalação/desinstalação remota, a conta especificada é usada para baixar para os dispositivos cliente os arquivos necessários para instalar ou desinstalar um aplicativo se o Agente de Rede não estiver instalado ou estiver indisponível. Se o Agente de Rede estiver instalado e disponível, a conta é usada se estiver de acordo com as configurações de tarefa, e a entrega de arquivos somente é executada usando os utilitários do Microsoft Windows a partir da pasta compartilhada. Neste caso, a conta deve ter os seguintes direitos no dispositivo:

- O direito de iniciar os aplicativos remotamente.
- O direito de usar o recurso Admin$.
- O direito de fazer *Login como serviço*.

Se os arquivos forem entregues aos dispositivos através do Agente de Rede, a conta não será usada. Todas as instalações de cópia e instalação de arquivos são então realizadas pelo **Agente de Rede** (**conta do LocalSystem**).

Exportar histórico de execução de tarefas

Se encontrar algum problema com uma tarefa, talvez seja necessário investigar os motivos subjacentes. Para fazer isso, é possível exportar e analisar melhor o histórico de execução de tarefas.

Para exportar o histórico de execução de tarefas:

1. Crie um arquivo TXT vazio em um diretório dentro do dispositivo.

   O histórico de execução de tarefas será exportado para esse arquivo.

2. Abra a janela de resultados da tarefa.

3. Na parte superior da janela de resultados da tarefa, selecione o dispositivo com problemas.

4. Na parte inferior da janela de resultados da tarefa, onde aparece o histórico de execução do dispositivo selecionado, escolha um ou mais eventos.

   Para selecionar vários eventos, use a tecla **`Shift`** ou **`Ctrl`**.

5. Clique com o botão direito do mouse no(s) evento(s) selecionado(s) para abrir o menu de contexto e selecione **Exportar**.

   O Assistente de exportação de eventos é iniciado.

6. Na etapa **Exportar arquivo** do assistente, clique no botão **Procurar** e selecione o arquivo TXT criado para exportar o histórico de execução da tarefa.

   Se deseja exportar apenas o(s) evento(s) selecionado(s), ative a opção **Exportar somente eventos selecionados**.

   Se deseja exportar todo o histórico de execução de tarefas (todos os eventos), a opção **Exportar somente eventos selecionados** deve ser desabilitada.

7. Clique no botão **Avançar**.

8. Na etapa **Formato de exportação** do assistente, ative uma das seguintes opções:

   - **Exportar como texto Unicode delimitado por tabulação**

     Habilite essa opção se os dados exportados incluírem caracteres especiais e símbolos de vários idiomas e for necessário garantir que todos os caracteres sejam preservados quando o arquivo TXT com os dados exportados for aberto em diferentes aplicativos.

   - **Exportar como texto delimitado por tabulação**

     Habilite essa opção se quiser manter a compatibilidade com sistemas ou aplicativos mais antigos que possam não ser compatíveis com Unicode.

9. Clique no botão **Avançar** para encerrar o assistente.

O histórico de execução da tarefa é exportado para o arquivo TXT selecionado.

Assistente para Alterar a Senha das Tarefas

Para uma tarefa não local, você pode especificar uma conta na qual a tarefa deve ser executada. Você pode especificar a conta durante a criação da tarefa ou nas propriedades de uma tarefa existente. Se a conta especificada for usada de acordo com as instruções de segurança da organização, essas instruções poderão exigir a alteração periódica da senha da conta. Quando a senha da conta expirar e você definir uma nova, as tarefas não serão iniciadas até que você especifique a nova senha válida nas propriedades da tarefa.

O Assistente para alterar a senha das tarefas permite substituir automaticamente a senha antiga pela nova em todas as tarefas em que a conta esteja especificada. Como alternativa, você pode fazer isso manualmente nas propriedades de cada tarefa.

Para iniciar o Assistente para alterar a senha das tarefas:

1. Na árvore do console, selecione o nó **Tarefas**.

2. No menu de contexto do nó selecione **Assistente para Alterar a Senha das Tarefas**.

Siga as instruções do Assistente.

Etapa 1. Especificar as credenciais

Nos campos **Conta** e **Senha**, especifique novas credenciais atualmente válidas no seu sistema (por exemplo, no Active Directory). Quando você passa para a próxima etapa do Assistente, o Kaspersky Security Center verifica se o nome da conta especificado corresponde ao nome da conta nas propriedades de cada tarefa não local. Se os nomes das contas corresponderem, a senha nas propriedades da tarefa será automaticamente substituída pela nova.

Se você preencher o campo **Senha antiga (opcional)**, o Kaspersky Security Center substitui a senha apenas para as tarefas nas quais o nome da conta e a senha antiga são encontrados. A substituição é realizada automaticamente. Em todos os outros casos, você precisa escolher uma ação a ser executada na próxima etapa do Assistente.

Etapa 2. Selecionar uma ação a ser executada

Se você não especificou a senha antiga na primeira etapa do Assistente ou a senha antiga especificada não correspondeu às senhas nas tarefas, será necessário escolher uma ação a ser executada para as tarefas encontradas.

Para cada tarefa que possui o status *Aprovação necessária*, decida se deseja remover a senha nas propriedades da tarefa ou substitui-la pela nova. Se você optar por remover a senha, a tarefa será alternada para executar sob a conta padrão.

Etapa 3. Visualizar os resultados

Na última etapa do Assistente, visualize os resultados para cada uma das tarefas encontradas. Para concluir o Assistente, pressione o botão **Concluir**.

Criar uma hierarquia de grupos de administração subordinados a um Servidor de Administração virtual

Após a criação do Servidor de Administração virtual, ele contém por padrão um grupo de administração nomeado **Dispositivos gerenciados**.

O procedimento de criação de uma hierarquia de grupos de administração subordinados ao Servidor de Administração virtual é igual ao procedimento de criação de uma hierarquia de grupos de administração subordinados ao Servidor de Administração físico.

Você não pode adicionar Servidores de Administração secundários e virtuais a grupos de administração subordinados a um Servidor de Administração virtual. Isto é devido a limitações dos Servidores de Administração virtuais.

Políticas e perfis da política

No Kaspersky Security Center Web Console, é possível criar políticas para aplicativos da Kaspersky. Esta seção descreve políticas e perfis da política e fornece instruções para criá-las e modificá-las.

Hierarquia de políticas, usando perfis de política

Essa seção fornece informações sobre como aplicar políticas aos dispositivos em grupos de administração. Esta seção também fornece informações sobre os perfis da política.

Hierarquia de políticas

No Kaspersky Security Center, você usa políticas para definir uma coleção única de configurações para múltiplos dispositivos. Por exemplo, o escopo do aplicativo P definido para o grupo de administração G inclui dispositivos gerenciados com o aplicativo P instalado o que foi implementado no grupo G e em todos dos seus subgrupos, exceto para os subgrupos onde a caixa de seleção **Herdar do grupo de origem** estiver desmarcada nas propriedades.

Uma política se diferencia de qualquer configuração local pelos ícones de cadeado (🔒) ao lado de suas configurações. Se uma configuração (ou um grupo de configurações) estiver bloqueada nas propriedades da política, será necessário, em primeiro lugar, usar essa configuração (ou o grupo de configurações) ao criar configurações efetivas e, em segundo lugar, salvar as configurações ou o grupo de configurações no fluxo abaixo da política.

A criação das configurações efetivas em um dispositivo pode ser descrita como se segue: os valores de todas as configurações que não foram bloqueadas são tiradas da política, então elas são sobregravadas com os valores das configurações locais, e então a coleção resultante é sobregravada com os valores de configurações bloqueadas tiradas da política.

As políticas do mesmo aplicativo se afetam entre si através da hierarquia de grupos de administração: as configurações bloqueadas da política de fluxo acima substituem as mesmas políticas do fluxo abaixo.

Há uma política especial para usuários fora do escritório. Esta política entra em vigor em um dispositivo quando o dispositivo muda para o modo de fora do escritório. As políticas de ausência não afetam outras políticas através da hierarquia de grupos de administração.

Perfis da política

Aplicar políticas aos dispositivos somente através da hierarquia de grupos de administração pode ser inconveniente em muitas circunstâncias. Pode ser necessário criar diversas instâncias de uma política única que se diferem em uma ou duas configurações para diferentes grupos de administração e que sincronizam os conteúdos destas políticas no futuro.

Para ajudar você a evitar tais problemas, o Kaspersky Security Center suporta os *perfis da política*. Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos alvo em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo cliente (computador ou dispositivo móvel). A ativação de um perfil modifica as configurações da política que estavam ativas no dispositivo antes do perfil ser ativado. Essas configurações assumem valores que foram especificados no perfil.

As seguintes restrições são atualmente impostas aos perfis da política:

- Uma política pode incluir no máximo 100 perfis.
- Um perfil da política não pode conter outros perfis.
- Uma política não pode conter configurações de notificação.

Conteúdo de um perfil

Um perfil da política contém as seguintes partes constituintes:

- Nome. Os perfis com nomes idênticos afetam um ao outro por meio da hierarquia de grupos de administração com regras comuns.
- Subconjunto de configurações da política. Diferente da política, que contém todas as configurações, um perfil somente contém configurações que são de fato necessárias (configurações bloqueadas).
- Condição de ativação é uma expressão lógica com as propriedades do dispositivo. Um perfil está ativo (complementa a política) somente quando a condição de ativação de perfil se torna verdadeira. Em todos os outros casos, o perfil está inativo e é ignorado. As seguintes propriedades de dispositivo podem estar incluídas naquela expressão lógica:
  - Status do modo ausente.
  - Propriedades do ambiente de rede: nome da regra ativa para a conexão do Agente de Rede.
  - Presença ou ausência de identificadores especificados no dispositivo.
  - A alocação do dispositivo em uma unidade organizacional (UO) do Active Directory: explícita (o dispositivo está diretamente na UO especificada), ou implícito (o dispositivo está em uma UO, que está dentro da UO especificada em qualquer nível de aninhamento).
  - A associação do dispositivo no grupo de segurança do Active Directory (explícita ou implícita).
  - A associação do proprietário do dispositivo no grupo de segurança do Active Directory (explícita ou implícita).
- Desativando a caixa de seleção Perfil. Os perfis desativados sempre serão ignorados e as suas respetivas condições de ativação não serão verificadas.
- Prioridade do perfil. As condições de ativação de perfis diferentes são independentes, portanto vários perfis podem ser ativados simultaneamente. Se os perfis ativos contiverem coleções de configurações não de sobreposição, nenhum problema surgirá. No entanto, se dois perfis ativos contiverem valores diferentes da mesma configuração, uma ambiguidade ocorrerá. Esta ambiguidade deve ser evitada através das prioridades do perfil: o valor da variável ambígua será tomado do perfil que tiver a prioridade mais alta (aquele que é classificado como mais alto na lista de perfis).

O comportamento de perfis quando as políticas afetam uma a outra através da hierarquia

Os perfis com o mesmo nome são mesclados de acordo com as regras de mesclagem de política. Os perfis de uma política com fluxo acima têm uma prioridade mais alta do que os perfis de uma política de fluxo abaixo. Se a edição das configurações for proibida na política de fluxo acima (está bloqueada), a política de fluxo abaixo usa as condições de ativação da política de fluxo acima. Se a edição das configurações for permitida na política de fluxo acima, as condições de ativação do perfil da política de fluxo abaixo são usadas.

Como um perfil da política pode conter a propriedade **O dispositivo está offline** em sua condição de ativação, os perfis substituem completamente as políticas de usuário ausente, que não são mais compatíveis.

Uma política de usuário ausente pode conter perfis, mas os seus perfis somente podem ser ativados após que o dispositivo muda para o modo ausente.

Herança de configurações da política

Uma política é especificada para um grupo de administração. As configurações de política podem ser *herdadas*, isto é, recebidas nos subgrupos (grupos secundários) do grupo de administração para o qual elas foram definidas. Depois disso, a política de um grupo principal é também referida como uma *política principal*.

Você pode ativar ou desativar duas opções de herança: **Herdar configurações da política principal** e **Forçar herança de configurações nas políticas secundárias**:

- Se você ativar **Herdar configurações da política principal** para uma política secundária e bloquear algumas configurações na política principal, não poderá alterar essas configurações para o grupo secundário. No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

- Se você desativar **Herdar configurações da política principal** para uma política secundária, você poderá alterar todas as configurações no grupo secundário, mesmo se algumas configurações estiverem bloqueadas na política principal.

- Se você ativar **Forçar herança de configurações nas políticas secundárias** no grupo principal, isso ativará **Herdar configurações da política principal** para cada política secundária. Nesse caso, você não pode desativar esta opção para nenhuma política secundária. Todas as configurações bloqueadas na política principal são herdadas por imposição nos grupos secundários, e você não pode alterar essas configurações nos grupos secundários.

- Nas políticas do grupo **Dispositivos gerenciados**, **Herdar configurações da política principal** não afeta nenhuma configuração, porque o grupo **Dispositivos gerenciados** não tem nenhum grupo acima e, por isso, não herda nenhuma política.

Por padrão, a opção **Herdar configurações da política principal** está ativada para uma nova política.

Se uma política tiver perfis, todas as políticas secundárias herdarão esses perfis.

Gerenciamento de políticas

Os aplicativos instalados em dispositivos cliente são configurados centralmente através de políticas que o definem.

As políticas criadas para aplicativos em um grupo de administração são exibidas no espaço de trabalho, na guia **Políticas**. Antes do nome de cada política, é exibido um ícone com seu status.

Depois de a política ser excluída ou revogada, o aplicativo continua trabalhando com as configurações especificadas na política. Estas configurações subsequentemente podem ser modificadas manualmente.

A política aplica-se da seguinte maneira: se um dispositivo cliente estiver executando tarefas internas (tarefas de proteção em tempo real), elas continuam a ser executadas com os novos valores das configurações. Quaisquer tarefas periódicas (verificação sob demanda, atualização do bancos de dados do aplicativo) iniciadas continuam sendo executadas sem alteração dos valores. Na próxima vez, elas serão executadas com os novos valores da configuração.

As políticas de aplicativos com suporte de multiinquilinato são herdadas de grupos de administração de nível mais baixo bem como de grupos de administração de nível superior: a política é propagada a todos os dispositivos cliente nos quais o aplicativo é instalado.

Se os Servidores de Administração forem estruturados hierarquicamente, os Servidores de Administração secundários recebem políticas do Servidor de Administração principal e distribuem as mesmas para os dispositivos cliente. Quando a herança estiver ativada, as configurações de política podem ser modificadas no Servidor de Administração principal. Depois disso, quaisquer alterações efetuadas às configurações de políticas são propagadas para as políticas herdadas nos Servidores de Administração secundários.

Se a conexão for interrompida entre os Servidores de Administração principais e secundários, a política no Servidor secundário continua, usando as configurações aplicadas. As configurações de política modificadas no Servidor de Administração principal são distribuídas a um Servidor de Administração secundário depois de a conexão ser restabelecida.

Se a herança estiver desativada, as configurações de política podem ser modificadas em um Servidor de Administração secundário independentemente do Servidor de Administração principal.

Se a conexão entre o Servidor de Administração e o dispositivo cliente for interrompida, o dispositivo cliente começa a ser executado sob a política off-line (se estiver definida) ou a política continua a ser executada as configurações aplicadas até que a conexão seja restabelecida.

Os resultados da distribuição de política ao Servidor de Administração secundário são exibidos na janela de propriedades de política do console no Servidor de Administração principal.

Os resultados da propagação de políticas para dispositivos cliente são exibidos na janela Propriedades de política do Servidor de Administração ao qual os mesmos estão conectados.

Não use dados privados nas configurações da política. Por exemplo, evite especificar a senha do administrador do domínio.

Criação de uma política

No Console de Administração, você pode criar políticas diretamente na pasta do grupo de administração para o qual a política deve ser criada, ou no espaço de trabalho da pasta **Políticas**.

Para criar uma política na pasta de um grupo de administração:

1. Na árvore do console, selecione um grupo de administração para o qual você deseja criar uma política.
2. No espaço de trabalho do grupo, selecione a guia **Políticas**.
3. Execute o Assistente de nova política ao clicar no botão **Nova política**.

   O Assistente de nova política é iniciado. Siga as instruções do Assistente.

*Para criar uma política no espaço de trabalho da pasta **Políticas**:*

1. Na árvore do console, selecione a pasta **Políticas**.
2. Execute o Assistente de nova política ao clicar no botão **Nova política**.

   O Assistente de nova política é iniciado. Siga as instruções do Assistente.

Você pode criar várias políticas para um aplicativo do grupo, mas somente uma política de cada vez pode ficar ativa. Quando você cria uma nova política ativa, a política ativa anterior se torna inativa.

Quando está criando uma política, você pode especificar um conjunto mínimo de parâmetros necessários para a operação correta do aplicativo. Todos os outros valores são definidos nos valores predefinidos aplicados durante a instalação local do aplicativo. Você pode alterar a política depois de ter sido criada.

Não use dados privados nas configurações da política. Por exemplo, evite especificar a senha do administrador do domínio.

As configurações dos aplicativos Kaspersky, que são alteradas após a aplicação das políticas, estão descritas em pormenor nos respectivos Guias.

Após a política ter sido criada, as configurações são bloqueadas para edição (marcadas com o ícone de cadeado ( )) e isso se torna efetivo nos dispositivos clientes independentemente de quais configurações tenham sido anteriormente especificadas para o aplicativo.

Exibição de política herdada em um subgrupo

Para habilitar a exibição de políticas herdadas para um grupo de administração alojado:

1. Na árvore do console, selecione o grupo de administração para o qual as políticas herdadas devem ser exibidas.
2. No espaço de trabalho do grupo selecionado, abra a guia **Políticas**.
3. No menu de contexto da lista de políticas, selecione **Exibir** → **Políticas herdadas**.

   As tarefas herdadas serão exibidas na lista de políticas com o seguinte ícone:

- – Se eles foram herdados de um grupo criado no Servidor de Administração principal.
- – Se elas foram herdadas de um grupo de nível superior.

  Quando o modo de herança de configurações é habilitado, as políticas herdadas só estão disponíveis para modificação no grupo, no qual as mesmas foram criadas. A modificação das políticas herdadas não está disponível no grupo que herda as mesmas.

Ativação de uma política

Para tornar uma política ativa para o grupo selecionado:

1. No espaço de trabalho do grupo, na guia **Políticas**, selecione a política que você precisa tornar ativa.
2. Para ativar a política, realize uma das seguintes ações:
   - No menu de contexto da política, selecione **Política ativa**.
   - Na janela de propriedades de política, abra a seção **Geral** e selecione **Política ativa** no grupo de configurações **Status da política**.

A política se torna ativa para o grupo de administração selecionado.

Quando uma política for aplicada a um número grande de dispositivos cliente, a carga no Servidor de Administração e o tráfego de rede aumentam significativamente por algum tempo.

Ativação automática de uma política no evento Ataque de vírus

Para fazer com que uma política execute a ativação automática no evento de um ataque de vírus:

1. Na janela de propriedades do Servidor de Administração, abra a seção **Surto de vírus**.
2. Abra a janela **Ativação da política** clicando no link **Configurar as políticas para ativar em caso de um evento de surto de vírus** e adicione a política à lista selecionada de políticas que são ativadas quando um ataque de vírus for detectado.

   Se uma política tiver sido ativada no evento *Ataque de vírus*, você somente pode voltar à política anterior usando o modo manual.

Aplicar uma política de ausência do escritório

A política de ausência de escritório tem efeito em um dispositivo caso este esteja desconectado da rede corporativa.

Para aplicar uma política de ausência:

Na janela de propriedades da política, abra a seção **Geral** e, no grupo de configurações **Status da política**, selecione **Política de ausência**.

A política de ausência será aplicada aos dispositivos se eles forem desconectados da rede corporativa.

Modificando uma política. Reverter modificações

Para modificar uma política:

1. Na árvore do console, selecione a pasta **Políticas**.
2. No espaço de trabalho da pasta **Políticas**, selecione uma política e prossiga à janela Propriedades de política usando o menu de contexto.
3. Efetuar as alterações relevantes.
4. Clique em **Aplicar**.

As modificações feitas à política serão salvas nas propriedades de política, na seção **Histórico de revisões**.

Você poderá reverter as alterações feitas à política, se necessário.

Para reverter as modificações feitas à política:

1. Na árvore do console, selecione a pasta **Políticas**.
2. Selecione a política na qual as modificações devem ser revertidas, e siga para a janela Propriedades da política usando o menu de contexto.
3. Na janela de propriedades da política, selecione a seção **Histórico de revisões**.
4. Na lista de revisões de política, selecione o número da revisão para a qual você precisa reverter as modificações.
5. Clique no botão **Avançado** e selecione o valor **Reverter** na lista suspensa.

Visualizar o gráfico de status de distribuição da política

No Kaspersky Security Center, é possível visualizar os resultados da aplicação da política em cada dispositivo.

Para analisar o status de distribuição da política em cada dispositivo:

1. No espaço de trabalho do grupo, na guia **Políticas**, selecione a política da qual deseja visualizar o status de distribuição.

   O gráfico no painel direito exibe a visão geral da aplicação da política.
2. Clique em **Detalhes**.

   A janela **Resultados do cumprimento da política** é aberta.

   É possível exportar os resultados da aplicação da política para um arquivo CSV ou TXT.

Comparar políticas

Você pode comparar duas políticas para um único aplicativo gerenciado. Após a comparação, você tem um relatório que exibe quais configurações de política coincidem e quais configurações se diferenciam. Por exemplo, você ter que comparar políticas se os diferentes administradores nos seus respetivos escritórios tiverem criado múltiplas políticas para um único aplicativo gerenciado, ou se uma política de nível superior tiver sido herdada por todos os escritórios locais e modificada para cada escritório. Você pode comparar políticas em uma das seguintes formas: selecionando uma política e comparando-a com o outra, ou comparando quaisquer duas política da lista de políticas.

Só é possível comparar as políticas que tenham as análises atuais no histórico de revisões.

Para comparar uma política com outra:

1. Na árvore do console, selecione a pasta **Políticas**.
2. No espaço de trabalho da pasta **Políticas**, selecione a política que você necessita para comparar com outra.
3. No menu de contexto da política, selecione **Comparar a política com outra política**.
4. Na janela **Selecionar política**, selecione a política com a qual a sua política deve ser comparada.
5. Clique em **OK**.

Um relatório no formato HTML é exibido para a comparação das duas políticas para o mesmo aplicativo.

Para comparar quaisquer duas política da lista de políticas:

1. Na pasta **Políticas**, na lista de políticas, use a tecla **`Shift`** ou **`Ctrl`** para selecionar duas políticas para um único aplicativo gerenciado.
2. No menu de contexto, selecione **Comparar**.

Um relatório no formato HTML é exibido para a comparação das duas políticas para o mesmo aplicativo.

O relatório sobre a comparação de configurações de política para o Kaspersky Endpoint Security for Windows também fornece detalhes da comparação de perfis da política. Você pode minimizar os resultados da comparação de perfil da política. Para minimizar a seção, clique no ícone da seta (▲) ao lado do nome da seção.

Exclusão de uma política

Para excluir uma política:

1. No espaço de trabalho de um grupo de administração, na guia **Políticas**, selecione a política que você desejar excluir.
2. Exclua a política em uma das seguintes formas:
   - Selecionando **Excluir** no menu da política.
   - Clicando no link **Excluir política** na caixa de informações para a política selecionada.

Cópia de uma política

Para copiar uma política:

1. No espaço de trabalho do grupo desejado, na guia **Políticas**, selecione uma política.
2. No menu de contexto da política, selecione **Copiar**.
3. Na árvore do console, selecione um grupo ao qual você deseja adicionar a política.

   Você pode adicionar uma política ao grupo, a partir do qual a mesma foi copiada.
4. No menu de contexto da lista de políticas para o grupo selecionado, na guia **Políticas**, selecione **Colar**.

A política será copiada com todas as suas configurações e aplicada aos dispositivos dentro do grupo para o qual ela foi copiada. Se você colar a política no mesmo grupo a partir do qual ela foi copiada, o índice **(<próximo número da sequência>)** é automaticamente adicionado ao nome da política: por exemplo, **(1)**, **(2)**.

Uma política ativa se torna inativa enquanto é copiada. Se necessário, você pode torná-la ativa.

Exportação de uma política

Para exportar uma política:

1. Exporte uma política numa das seguintes formas:
   - Selecionando **Todas as tarefas** → **Exportar** no menu de contexto da política.
   - Clicando no link **Exportar a política para arquivo** na caixa de informações para a política selecionada.
2. Na janela **Salvar como** que for aberta, especifique o nome e o caminho do arquivo de política. Clique no botão **Salvar**.

Importação de uma política

Para importar uma política:

1. No espaço de trabalho do grupo relevante, na guia **Políticas**, selecione uma das seguintes formas para importar políticas:

   - Selecionando **Todas as tarefas** → **Importar** no menu de contexto da lista de políticas.

   - Clicando no botão **Importar política de arquivo** no bloco de gerenciamento para a lista de políticas.

2. Na janela que se abre, especifique o caminho para o arquivo a partir do qual você deseja importar uma política. Clique no botão **Abrir**.

A política importada é exibida na lista de políticas. As configurações e os perfis da política também são importados. Independentemente do status da política selecionada durante a exportação, a política importada está inativa. Você pode alterar o status da política nas propriedades da política.

Se a política recém-importada tiver um nome idêntico ao de uma política existente, o nome da política importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Converter políticas

O Kaspersky Security Center pode converter políticas de versões mais antigas dos aplicativos Kaspersky gerenciados para as políticas de versões atualizadas dos mesmos aplicativos. As políticas convertidas mantêm as configurações do administrador atual especificadas antes da atualização, bem como incluem novas configurações das versões atualizadas dos aplicativos. Se uma política for convertida para uma versão atualizada de um aplicativo Kaspersky gerenciado, você não poderá abrir a política em um Servidor de Administração que tenha uma versão anterior do plug-in do aplicativo instalada. Os plugins de gerenciamento de aplicativos da Kaspersky determinam se a conversão está disponível para as políticas desses aplicativos. Para obter informações sobre a conversão de políticas para cada aplicativo Kaspersky compatível, consulte a Ajuda relevante na lista a seguir:

- **Aplicativos Kaspersky para estações de trabalho:**
  - 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 (não é compatível com implementação centralizada)
- **Aplicativos Kaspersky para dispositivos móveis:**
  - Kaspersky Endpoint Security for Android
  - Kaspersky Security for iOS
- **Aplicativos Kaspersky para servidores de arquivos:**
  - Kaspersky Security for Windows Server
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Endpoint Security for Linux
- **Aplicativos Kaspersky para máquinas virtuais:**
  - Kaspersky Security for Virtualization Light Agent
  - Kaspersky Security for Virtualization Agentless

- **Aplicativos Kaspersky para sistemas de correio e servidores SharePoint/de colaboração:**
  - Kaspersky Security para Linux Mail Server
  - Kaspersky Security for Microsoft Exchange Servers
- **Aplicativos Kaspersky para detecção de ataques direcionados:**
  - Kaspersky Sandbox
  - Kaspersky Endpoint Detection and Response Optimum
  - Kaspersky Managed Detection and Response
- **Aplicativos Kaspersky para dispositivos KasperskyOS:**
  - Kaspersky IoT Secure Gateway
  - Kaspersky Security Management Suite (plug-in para Kaspersky Thin Client)

Para converter políticas:

1. Na árvore do console, selecione o Servidor de Administração para o qual você deseja converter políticas.
2. No menu de contexto do Servidor de Administração, selecione **Todas as tarefas → Assistente de conversão de políticas e tarefas em lotes**.

O Assistente de conversão de políticas e tarefas em lotes é iniciado. Siga as instruções do Assistente.

Após a conclusão do assistente, são criadas novas políticas que usam as atuais configurações de políticas do administrador e as novas configurações das versões atualizadas dos aplicativos Kaspersky.

Gerenciando perfis de política

Esta seção descreve o gerenciamento de perfis de política e fornece informações sobre como visualizá-los, alterar a prioridade, criar, modificar, copiar, criar uma regra de ativação e excluir perfis de política.

Gerenciando perfis de política

Perfil da política é um conjunto nomeado de configurações de uma política que é ativado em um dispositivo cliente (computador ou dispositivo móvel) quando o dispositivo satisfaz as regras de ativação especificadas. A ativação de um perfil modifica as configurações da política que estavam ativas no dispositivo antes do perfil ser ativado. Essas configurações assumem valores que foram especificados no perfil.

Os perfis de política são destinados para permitir os dispositivos dentro de um grupo de administração único executem sob configurações de política diferentes. Por exemplo, uma situação pode ocorrer quando as configurações da política têm de ser modificadas para alguns dispositivos em um grupo de administração. Neste caso, você pode configurar os perfis de política para tal política, que lhe permitirá editar as configurações da política de dispositivos selecionados no grupo de administração. Por exemplo, a política proíbe executar qualquer software de navegação GPS em todos os dispositivos no grupo de administração de Usuários. O software de navegação de GPS é necessário em um dispositivo único no grupo de administração de Usuários, notadamente que for de propriedade do usuário empregado como um courier. Você pode identificar aquele dispositivo como simplesmente "Correio" e reconfigurar o perfil da política para que ele permita que o software de navegação GPS somente execute no dispositivo identificado como "Correio", preservando todas as configurações de política remanescentes. Neste caso, se um dispositivo identificado como "Correio" aparece no grupo de administração de Usuários, ele terá a permissão de executar o software de navegação GPS. Executar o software de navegação de GPS ainda será proibido em outros dispositivos no grupo de administração de Usuários a menos que eles também estejam identificados como "Correio".

Os perfis somente são suportados pelas seguintes políticas:

- Políticas do Kaspersky Endpoint Security for Windows
- Políticas do Kaspersky Endpoint Security for Mac
- Políticas do plugin Kaspersky Mobile Device Management indo do Service Pack 1 da versão 10 ao Service Pack 3 Maintenance Release 1
- Políticas do Kaspersky Device Management para o plugin iOS
- Políticas do Kaspersky Security for Virtualization 5.1 Light Agent for Windows
- Políticas do Kaspersky Security for Virtualization 5.1 Light Agent for Linux

Os perfis de política simplificam o gerenciamento de dispositivos cliente aos quais as políticas se aplicam:

- As configurações do perfil da política podem diferenciar-se das configurações da política.
- Você não precisa manter e aplicar manualmente várias instâncias de uma única política que diferem somente em algumas configurações.
- Você não precisa alocar uma política separada dos usuários fora do escritório.
- Você pode exportar e importar perfis de política, assim como criar novos perfis de política com base nos existentes.
- Uma política única pode ter múltiplos perfis de política ativos. Somente os perfis que atendam as regras de ativação efetivas no dispositivo serão aplicados àquele dispositivo.
- Os perfis são sujeitos à hierarquia da política. Uma política herdada inclui todos os perfis da política de nível mais alto.

Prioridades de perfis

Os perfis que foram criados para uma política são ordenados de forma descendente por prioridade. Por exemplo, se o perfil X for mais alto na lista de perfis do que o perfil Y, X tem uma prioridade mais alta do que o último. Múltiplos perfis podem ser simultaneamente aplicados a um dispositivo único. Se os valores de uma configuração variarem em perfis diferentes, o valor do perfil da prioridade mais alta será aplicado ao dispositivo.

Regras de ativação de perfis

Um perfil da política é ativado em um dispositivo cliente quando uma regra de ativação for acionada. As *regras de ativação* são um conjunto de condições que, quando atendidas, iniciam o perfil da política em um dispositivo. Uma regra de ativação pode conter as seguintes condições:

- O Agente de Rede em um dispositivo cliente se conecta com o Servidor de Administração com um conjunto especificado de configurações de conexão, como endereço do Servidor de Administração, número da porta e etc.
- O dispositivo cliente está off-line.
- O dispositivo cliente tem tags específicas atribuídas.
- O dispositivo cliente é explicitamente (o dispositivo é imediatamente localizado na unidade especificada) ou implicitamente (o dispositivo é localizado em uma unidade que está na unidade especificada a qualquer nível de aninhamento) localizado em uma unidade específica do Active Directory®, o dispositivo ou o seu proprietário está localizado em um grupo de segurança do Active Directory.
- O dispositivo do cliente é de propriedade de um proprietário especificado, ou os proprietários do dispositivo que está incluído em um grupo de segurança interna do Kaspersky Security Center.
- O proprietário do dispositivo cliente foi atribuído com uma função específica.

Políticas na hierarquia de grupos de administração

Se você estiver criando uma política em um grupo de administração de nível baixo, esta nova política herda todos os perfis da política ativa do grupo de nível mais alto. Os perfis com nomes idênticos são mesclados. Os perfis de política do grupo de nível mais alto têm a prioridade mais alta. Por exemplo, no grupo de administração *A*, a política *P(A)* tem perfis *X1*, *X2* e *X3* (por ordem descendente de prioridade). No grupo de administração *B*, o qual é um subgrupo do grupo *A*, a política *P(B)* foi criada com os perfis *X2*, *X4*, *X5*. A seguir, a política *P(B)* será modificada com a política *P(A)* para que a lista de perfis na política *P(B)* tenha o seguinte aspecto: *X1*, *X2*, *X3*, *X4*, *X5* (por ordem decrescente de prioridade). A prioridade do perfil *X2* dependerá do estado inicial de *X2* da política *P(B)* e *X2* da política *P(A)*. Após a política *P(B)* ter sido criada, a política *P(A)* não mais será exibida no subgrupo *B*.

A política ativa é recalculada cada vez que você executar o Agente de Rede, ativar e desativar o modo offline ou editar a lista de tags atribuídas ao dispositivo cliente. Por exemplo, o tamanho da RAM foi aumentado no dispositivo, que, à sua vez, ativou o perfil da política que é aplicado nos dispositivos com o tamanho de RAM grande.

As propriedades e restrições de perfis de política

Os perfis têm as seguintes propriedades:

- Os perfis de uma política inativa não têm impacto em dispositivos cliente.
- Se uma política for definida com o status de **Política de ausência**, os perfis dessa política também serão aplicados somente quando um dispositivo for desconectado da rede corporativa.
- Os perfis não suportam a análise estática de acesso a arquivos executáveis.
- Um perfil da política não pode conter nenhuma configuração de notificações de evento.

- Se a porta UDP 15000 for usada para conexão de um dispositivo ao Servidor de Administração, você deve ativar o perfil da política correspondente no período de um minuto após atribuir uma tag ao dispositivo.
- Você pode usar regras para conexão do Agente de Rede ao Servidor de Administração ao criar regras de ativação do perfil da política.

Criar um perfil da política

A criação do perfil está disponível apenas para as políticas dos seguintes aplicativos:

- Kaspersky Endpoint Security 10 Service Pack 1 for Windows e versões posteriores
- Kaspersky Endpoint Security 10 Service Pack 1 for Mac
- Plugin Kaspersky Mobile Device Management versão 10, Service Pack versão 10 ao 1 Service Pack 3 Maintenance Release 1
- Plugin Kaspersky Device Management for iOS
- Kaspersky Security for Virtualization 5.1 Light Agent for Windows e Linux

Para criar um perfil da política:

1. Na árvore do console, selecione o grupo de administração para o qual você deseja criar um perfil da política.
2. No espaço de trabalho do grupo de administração, selecione a guia **Políticas**.
3. Selecione uma política e mude para a janela de propriedades da política usando o menu de contexto.
4. Abra a seção **Perfis de política** na janela Propriedades da política e clique no botão **Adicionar**.

   O Assistente Novo perfil da política é iniciado.
5. Na janela **Nome do perfil de política** do Assistente, especifique o seguinte:

   a. Nome do perfil da política

      O nome de um perfil não pode incluir mais do que 100 caracteres.

   b. Status do perfil da política (*Ativado* ou *Desativado*)

      Recomendamos que você crie e ative perfis de política inativos somente após tiver tido concluído por completo as configurações e as condições da ativação do perfil da política.
6. Selecione a caixa de seleção **Após fechar o Assistente de novo perfil de política, siga para a configuração da regra de ativação do perfil de política** para iniciar o Assistente para Nova Regra de Ativação do Perfil de Política. Siga as etapas do assistente.
7. Edite as configurações do perfil da política na janela de propriedades do perfil da política, da forma que você necessita.
8. Salve as alterações clicando em **OK**.

   O perfil é salvo. O perfil será aplicado nos dispositivos que atendem as regras de ativação.

Você pode criar múltiplos perfis para uma única política. Os perfis que foram criados para uma política são exibidos nas Propriedades da política, na seção **Perfis de política**. Você pode modificar um perfil da política e modificar a prioridade do perfil, bem como remover o perfil.

Modificar um perfil da política

Editar as configurações de um perfil da política

A capacidade para editar um perfil da política somente está disponível para políticas do Kaspersky Endpoint Security for Windows.

Para modificar um perfil da política:

1. Na árvore do console, selecione o grupo de administração para o qual o perfil da política deve ser modificado.
2. No espaço de trabalho do grupo, selecione a guia **Políticas**.
3. Selecione uma política e mude para a janela de propriedades da política usando o menu de contexto.
4. Abra a seção **Perfis de política** nas Propriedades da política.

   Essa seção contém uma lista de perfis que foram criados para a política. Os perfis são exibidos na lista de acordo com suas prioridades.
5. Selecione um perfil da política e clique no botão **Propriedades**.
6. Configure o perfil na janela de propriedades:
   - Se necessário, na seção **Geral**, altere o nome do perfil e ative ou desative o perfil usando a caixa de seleção **Ativar perfil**.
   - Na seção **Regras de ativação**, edite as regras de ativação do perfil.
   - Edite as configurações de política nas seções correspondentes.
7. Clique em **OK**.

As configurações que você modificou serão aplicadas após o dispositivo ser sincronizado com o Servidor de Administração (se o perfil da política estiver ativo) ou após a regra de ativação ser acionada (se o perfil da política estiver inativo).

Alterar a prioridade de um perfil da política

As prioridades de perfis de política definem a ordem de ativação de perfis em um dispositivo cliente. As propriedades são usadas se regras de ativação idênticas forem configuradas para diferentes perfis de política.

Por exemplo, foram criados dois perfis de política: *Perfil 1* e *Perfil 2*, os quais diferem pelos valores respetivos de uma única configuração (*Valor 1* e *Valor 2*). A prioridade do *Perfil 1* é superior à prioridade do *Perfil 2*. Além disso, existem também perfis com prioridades mais baixas do que o *Perfil 2*. As regras de ativação para esses perfis são idênticas.

Quando uma regra de ativação é acionada, o *Perfil 1* será ativado. A configuração no dispositivo assumirá o *Valor 1*. Se você remover o *Perfil 1*, o *Perfil 2* terá a prioridade mais alta, portanto a configuração assumirá o *Valor 2*.

Na lista de perfis de política, os perfis são exibidos de acordo com suas prioridades respetivas. O perfil com a prioridade mais alta é colocado primeiro no ranking. É possível alterar a prioridade de um perfil usando os botões seta para cima  e seta para baixo  .

Excluir um perfil de política

Para excluir um perfil de política:

1. Na árvore do console, selecione o grupo de administração para o qual você deseja excluir um perfil da política.
2. No espaço de trabalho do grupo de administração, selecione a guia **Políticas**.
3. Selecione uma política e mude para a janela de propriedades da política usando o menu de contexto.
4. Abra a seção **Perfis de política** nas Propriedades da política do Kaspersky Endpoint Security.
5. Selecione o perfil da política que você desejar excluir e clique no botão **Excluir**.

O perfil da política será excluído. O status ativo será passado para outro perfil da política, cujas regras de ativação são acionadas no dispositivo ou para a política.

Criar uma regra de ativação do perfil da política

Para criar uma regra de ativação do perfil da política:

1. Na árvore do console, selecione o grupo de administração para o qual você deseja criar uma regra de ativação do perfil da política.
2. No espaço de trabalho do grupo, selecione a guia **Políticas**.
3. Selecione uma política e mude para a janela de propriedades da política usando o menu de contexto.
4. Selecione a seção **Perfis de política** na janela Propriedades da política.
5. Selecione o perfil da política para o qual você precisa criar uma regra de ativação, e clique no botão **Propriedades**.

   A janela Propriedades do perfil da política será aberta.

   Se a lista de perfis da política estiver vazia, você pode criar um perfil da política.
6. Selecione a seção **Regras de ativação** e clique no botão **Adicionar**.

   O Assistente para novas regras de ativação do perfil de políticas é iniciado.

7. Na janela **Regras de ativação do perfil de política**, selecione as caixas de seleção junto as condições que devem afetar a ativação do perfil da política que você estiver criando:

- **Regras gerais para a ativação do perfil de política**

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo do status do modo offline de dispositivo, a regra para a conexão ao Servidor de Administração e as tags atribuídas ao dispositivo.

- **Regras para uso do Active Directory**

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo da presença do dispositivo em uma unidade organizacional (UO) do Active Directory ou em uma associação do dispositivo (ou seu proprietário) em um grupo de segurança do Active Directory.

- **Regras para um proprietário de dispositivo específico**

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo do proprietário do dispositivo.

- **Regras para especificações de hardware**

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo do volume de memória e do número de processadores lógicos.

O número de páginas adicionais do assistente depende das configurações que você seleciona no primeiro passo. Você pode modificar as regras de ativação do perfil da política em outro momento.

8. Na janela **Condições gerais**, especifique as seguintes configurações:

- No campo **O dispositivo está offline**, na lista suspensa, especifique a condição para a presença do dispositivo na rede:
  - **Sim**

    O dispositivo está em uma rede externa, o que significa que o Servidor de Administração não está disponível.

  - **Não**

    O dispositivo está na rede, portanto, o Servidor de Administração está disponível.

  - **Nenhum valor está selecionado**

    O critério não será aplicado.

- Na caixa **O dispositivo está no local de rede especificado**, use a lista suspensa para definir a ativação do perfil da política se a regra de conexão ao Servidor de Administração estiver sendo executada / não executada neste dispositivo:
  - **Executada / Não executada**

    A condição da ativação do perfil da política (se a regra está ou não sendo executada).

  - **Nome da regra**

    A descrição da localização do dispositivo para a conexão ao Servidor de Administração, cujas condições devem ser atendidas (ou não devem ser atendidas) para a ativação do perfil da política.

    Uma descrição da localização da rede de dispositivos para conexão a um Servidor de Administração pode ser criada ou configurada em uma regra de troca de Agente de Rede.

A janela **Condições gerais** é exibida se a caixa de seleção **Regras gerais para a ativação do perfil da política** estiver marcada.

9. Na janela **Condições que usam tags**, especifique as seguintes configurações:

- **Lista de tags**

  Na lista de tags, especifique uma regra para a inclusão do dispositivo no perfil da política, selecionando as caixas de seleção ao lado das tags relevantes.

  Você pode adicionar novas tags à lista inserindo-as no campo sobre a lista e clicando no botão **Adicionar**.

  O perfil da política inclui dispositivos com descrições que contêm todas as tags selecionadas. Se as caixas de seleção forem desmarcadas, o critério não é aplicado. Por padrão, estas caixas de seleção estão desmarcadas.

- **Aplicar aos dispositivos sem tags especificadas**

  Ative esta opção se tiver de inverter a seleção de tags.

  Se esta opção estiver selecionada, o perfil da política inclui dispositivos com descrições que não contêm nenhuma das tags selecionadas. Se esta opção estiver desativada, o critério não é aplicado.

  Por padrão, esta opção está desativada.

A janela **Condições que usam tags** é exibida se a caixa de seleção **Regras gerais para a ativação do perfil de política** estiver marcada.

10. Na janela **Condições usando o Active Directory**, especifique as seguintes configurações:

- **Associação do proprietário do dispositivo no grupo de segurança do Active Directory**

  Se esta opção estiver ativada, o perfil da política será ativado no dispositivo cujo proprietário for um membro do grupo de segurança especificado. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **Associação do dispositivo no grupo de segurança do Active Directory**

  Se esta opção estiver ativada, o perfil da política será ativado no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **A alocação do dispositivo está na unidade organizacional do Active Directory**

  Se esta opção estiver ativada, o perfil da política será ativado no dispositivo que estiver incluído na unidade organizacional (OU) do Active Directory especificada. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado.

  Por padrão, esta opção está desativada.

A janela **Condições usando o Active Directory** é exibida se a caixa de seleção **Regras para uso do Active Directory** estiver marcada.

11. Na janela **Condições usando o proprietário do dispositivo**, especifique as seguintes configurações:

- **Proprietário do dispositivo**

  Ative esta opção para configurar e ativar a regra para a ativação do perfil no dispositivo para seu proprietário. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

  - O dispositivo pertence ao proprietário especificado (sinal "=").
  - O dispositivo não pertence ao proprietário especificado (sinal "#").

    Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o proprietário do dispositivo se a opção estiver ativada. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **O proprietário do dispositivo está incluído no grupo de segurança interna**

  Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pela associação do proprietário em um grupo de segurança interna do Kaspersky Security Center. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

  - O proprietário do dispositivo é um membro do grupo de segurança especificado (sinal "=").
  - O proprietário do dispositivo não é um membro do grupo de segurança especificado (sinal "#").

    Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar um grupo de segurança do Kaspersky Security Center. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **Ativar o perfil de política por função específica do proprietário do dispositivo**

  Selecione esta opção para configurar e ativar a regra da ativação do perfil no dispositivo, dependendo da função do proprietário. Adicione a função manualmente da lista de funções existentes.

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados.

A janela **Condições usando o proprietário do dispositivo** será aberta se a caixa de seleção **Regras para um proprietário de dispositivo específico** estiver marcada.

12. Na janela **Condições usando especificações do equipamento**, especifique as seguintes configurações:

- **Tamanho da RAM, em MB**

  Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pelo volume de RAM disponível naquele dispositivo. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

  - O tamanho da RAM do dispositivo é menos do que o valor especificado (sinal "<").
  - O tamanho de RAM de dispositivo é maior do que o valor especificado (sinal ">").

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o volume da RAM no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **Número de Processadores Lógicos**

  Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pelo número de processadores lógicos nesse dispositivo. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

  - O número de processadores lógicos no dispositivo é menor do que ou igual ao valor especificado (sinal "<").
  - O número de processadores lógicos no dispositivo é maior do que ou igual ao valor especificado (sinal ">").

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o número de processadores lógicos no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

A janela **Condições usando especificações do equipamento** é exibida se a caixa de seleção **Regras para especificações de hardware** estiver marcada.

13. Na janela **Nome da regra de ativação do perfil de política** no campo **Nome da regra**, especifique um nome para a regra.

O perfil será salvo. O perfil será ativado no dispositivo quando as regras de ativação forem acionadas.

As regras de ativação do perfil da política criadas para o perfil são exibidas nas propriedades do perfil da política na seção **Regras de ativação**. Você pode modificar ou remover qualquer regra de ativação do perfil da política.

Múltiplas regras de ativação podem ser acionadas simultaneamente.

Regras de migração de dispositivos

Recomendamos definir a alocação automática de dispositivos em grupos de administração por meio das *regras de migração de dispositivos*. A regra de migração de dispositivos é composta por três partes principais: um nome, uma condição de execução (uma expressão lógica com os atributos de dispositivo) e um grupo de administração alvo. Uma regra move um dispositivo para o grupo de administração alvo se os atributos do dispositivo atendam a condição de execução da regra.

Todas as regras para migrar dispositivo têm prioridades. O Servidor de Administração verifica se os atributos do dispositivo atendem a condição de execução de cada regra, na ordem ascendente da prioridade. Se os atributos do dispositivo atenderem a condição de execução de uma regra, o dispositivo é movido para o grupo alvo, portanto o processamento de regra é completo para este dispositivo. Se os atributos do dispositivo atenderem as condições de múltiplas regras, o dispositivo é movido para o grupo alvo da regra com a prioridade mais alta (ou seja, ele tem a classificação mais alta na lista de regras).

As regras para migrar dispositivo podem ser criadas implicitamente. Por exemplo, nas propriedades de um pacote de instalação ou de uma tarefa de instalação remota, você pode especificar o grupo de administração para o qual o dispositivo deve ser movido após que Agente de Rede seja instalado nele. Também, as regras para migrar dispositivos podem ser criadas explicitamente pelo administrador do Kaspersky Security Center na lista de regras para mover. A lista está localizada no Console de Administração, nas propriedades do grupo **Dispositivos não atribuídos**.

Por padrão, a regra de migração de dispositivos se destina à alocação inicial e única dos dispositivos aos grupos de administração. A regra move os dispositivos do grupo **Dispositivos não atribuídos** somente uma vez. Se um dispositivo foi movido uma vez por esta regra, a regra nunca mais o moverá novamente, mesmo se você devolver o dispositivo ao grupo **Dispositivos não atribuídos** manualmente. Esta é a forma recomendada de aplicar regras para mover.

Você pode migrar dispositivos que já foram alocados à alguns dos grupos de administração. Para fazer isso, nas propriedades de uma regra, desmarque a caixa de seleção **Somente mover os dispositivos que não pertencem a um grupo de administração**.

Aplicar a regra de migração aos dispositivos que já foram alocados a alguns dos grupos de administração aumenta significativamente a carga do Servidor de Administração.

A caixa de seleção **Somente mover os dispositivos que não pertencem a um grupo de administração** é bloqueada nas propriedades das regras de movimentação criadas automaticamente. As regras são criadas ao adicionar a tarefa *Instalar aplicativo remotamente* ou ao criar um pacote de instalação independente.

Você pode criar uma regra para mover que iria afetar um único dispositivo repetidamente.

Nós recomendamos com ênfase que você evite mover um dispositivo único de um grupo para outro repetidamente (por exemplo, para poder aplicar uma política especial àquele dispositivo, executar uma tarefa de grupo especial, ou atualizar o dispositivos através de um ponto de distribuição específico).

Tais cenários não são compatíveis, pois eles aumentam a carga no Servidor de Administração e o tráfego da rede para um grau extremo. Estes cenários também estão em conflito com os princípios operacionais do Kaspersky Security Center (em particular na área de direitos de acesso, eventos e relatórios). Outra solução deve ser encontrada, por exemplo, por meio do uso de perfis de política, tarefas para seleções de dispositivo e atribuição de Agentes de Rede de acordo com o cenário padrão.

Clonar as regras para migrar dispositivos

Quando você precisa criar múltiplas regras para migrar dispositivos com configurações semelhantes, é possível clonar uma regra existente e alterar as configurações da regra clonada. Por exemplo, isso é útil quando você deve ter várias regras idênticas para migrar dispositivos com conjuntos de IPs e grupos-alvo diferentes.

Para clonar uma regra para migrar dispositivos:

1. Abra a janela principal do aplicativo.
2. Na pasta **Dispositivos não atribuídos**, clique em **Configurar regras**.
   A janela **Propriedades: Dispositivos não atribuídos** é aberta.
3. Na seção **Migrar dispositivos**, selecione a regra para migrar dispositivos que você quer clonar.
4. Clique em **Clonar regra**.

   Um clone da regra para migrar dispositivos selecionada será adicionado no final da lista.

Uma nova regra é criada no estado desativado. Você pode editar e ativar a regra a qualquer momento.

Categorização de software

A ferramenta principal para monitorar a execução dos aplicativos são as *categorias da Kaspersky* (aqui referidas como *categorias da KL*). As categorias da KL ajudam os administradores do Kaspersky Security Center a simplificar o suporte da categorização de software e minimizar o tráfego indo para os dispositivos gerenciados.

As categorias de usuário somente devem ser criadas para aplicativos que não podem ser classificados em nenhuma das categorias da KL existentes (por exemplo, para o software criado de forma personalizada). As categorias de usuário são criadas com base em um pacote de instalação do aplicativo (MSI) ou uma pasta com pacotes de instalação.

Se uma grande coleção de software estiver disponível, que não foi categorizada através de categorias da KL, pode ser útil criar uma categoria automaticamente atualizada. Os checksums de arquivos executáveis serão automaticamente adicionados a esta categoria em cada modificação da pasta que contém os pacotes de distribuição.

Não crie categorias de software atualizadas automaticamente para as pastas Meus Documentos, %windir%, %ProgramFiles% e %ProgramFiles(x86)%. O conjunto de arquivos nestas pastas está sujeito a modificações frequentes, que conduz a um aumento da no Servidor de Administração e no aumento do tráfego da rede. Você deve criar uma pasta dedicada com a coleção de software e periodicamente adicionar-lhe novos itens.

Prerrequisitos para instalar aplicativos em dispositivos de uma organização cliente

O processo da instalação remota de aplicativos em dispositivos de uma organização cliente é idêntico ao processo de instalação remota dentro de uma empresa.

Para instalar aplicativos nos dispositivos de uma organização cliente, as seguintes condições devem ser executadas:

- Antes de instalar aplicativos nos dispositivos da organização cliente pela primeira vez, você deve instalar o Agente de Rede neles.

  Ao configurar o pacote de instalação do Agente de Rede pelo provedor do serviço, no Kaspersky Security Center, ajuste as seguintes configurações na janela Propriedades do pacote de instalação:

  - Na seção **Conexão**, na sequência de caracteres **Servidor de Administração**, especifique o endereço do mesmo Servidor de Administrador virtual especificado durante a instalação local do Agente de Rede no ponto de distribuição.

  - Na seção **Avançado**, selecione a caixa de seleção **Conectar-se ao Servidor de Administração usando o gateway de conexão**. Na sequência de caracteres **Ender. do gateway-conexão**, especifique o endereço do ponto de distribuição. Você poderá usar o endereço IP ou o nome do dispositivo na rede Windows.

- Selecione **Usando recursos do sistema operacional através de pontos de distribuição** como método de download para o pacote de instalação do Agente de Rede. Você pode selecionar o método de download como segue:

  - Se você instalar o aplicativo usando a tarefa de instalação remota, poderá especificar o método de download em uma das seguintes formas:

    - Criando uma tarefa de instalação remota na janela **Configurações**

    - Na janela de propriedades da tarefa de instalação remota, na seção **Configurações**

  - Se você instalar aplicativos usando o Assistente de instalação remota, poderá selecionar o método de download na janela **Configurações** deste assistente.

- A conta usada pelo ponto de distribuição para autorização deve ter acesso ao recurso Admin$ em todos os dispositivos cliente.

Exibir e editar as configurações do aplicativo local

O sistema de administração do Kaspersky Security Center permite o gerenciar remotamente configurações de aplicativo local em dispositivos através do Console de Administração.

As *configurações de aplicativo locais* são as configurações de um aplicativo é específico para um dispositivo. Você pode usar o Kaspersky Security Center para definir as configurações de aplicativo local para dispositivos incluídos em grupos de administração.

São fornecidas descrições detalhadas das configurações dos aplicativos Kaspersky nos respectivos Guias.

Para exibir ou alterar as configurações locais de um aplicativo:

1. No espaço de trabalho do grupo ao qual o dispositivo relevante pertence, selecione a guia **Dispositivos**.

2. Na janela de propriedades do dispositivo, na seção **Aplicativos**, selecione o aplicativo relevante.

3. Abra a janela de propriedades do aplicativo clicando duas vezes no nome do aplicativo ou clicando no botão **Propriedades**.

A janela de configurações locais do aplicativo selecionado se abre para que você possa visualizar e editar essas configurações.

É possível alterar os valores das configurações que não foram impedidas de ser modificadas por uma política do grupo (ou seja, aquelas que não estão marcadas com o ícone Cadeado (🔒) em uma política).

Atualizar Kaspersky Security Center e os aplicativos gerenciados

Esta seção descreve etapas que você deve seguir para atualizar o Kaspersky Security Center e os aplicativos gerenciados.

Cenário: Atualização regular dos bancos de dados e dos aplicativos Kaspersky

Esta seção fornece um cenário para a atualização regular de bancos de dados, módulos de software e aplicativos da Kaspersky. Após ter concluído o Cenário de configuração de proteção da rede, você precisará manter a confiabilidade do sistema de proteção para ter certeza de que os Servidores de Administração e os dispositivos gerenciados estejam permanentemente protegidos contra várias ameaças, incluindo vírus, ataques à rede e ataques de phishing.

A proteção da rede é mantida atualizada por atualizações regulares dos seguintes:

- Bancos de dados e módulos de software da Kaspersky
- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center

Quando concluir este cenário, você poderá ter certeza do seguinte:

- A sua rede está protegida pelo software da Kaspersky mais recente, inclusive aplicativos de segurança e componentes do Kaspersky Security Center.
- Os bancos de dados de antivírus e outros bancos de dados da Kaspersky críticos para a segurança de rede são sempre atualizados.

Pré-requisitos

Os dispositivos gerenciados devem ter uma conexão com o Servidor de Administração. Se eles não tiverem uma conexão, considere atualizar os bancos de dados, módulos de software e aplicativos da Kaspersky manualmente ou diretamente nos servidores de atualização da Kaspersky.

O Servidor de Administração deve ter uma conexão com a Internet.

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

1. Implementado os aplicativos de segurança da Kaspersky nos dispositivos gerenciados de acordo com o cenário de implementação de aplicativos Kaspersky através do Kaspersky Security Center Web Console.
2. Criado e configurado todos os perfis da política, políticas e tarefas necessários segundo o cenário de configuração da proteção de rede.
3. Atribuído um volume apropriado de pontos de distribuição conforme o número de dispositivos gerenciados e a topologia de rede.

A atualização dos bancos de dados e dos aplicativos da Kaspersky prossegue em estágios:

1. **Seleção de um esquema de atualização**

   Há vários esquemas que você pode usar para instalar atualizações para componentes e aplicativos de segurança do Kaspersky Security Center. Selecione o esquema ou vários esquemas que atendem aos requisitos de sua melhor rede.

2. **Criar a tarefa para baixar as atualizações no repositório do Servidor de Administração**

   Essa tarefa é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Se você não tiver executado o assistente, crie a tarefa agora.

   Essa tarefa é necessária para baixar atualizações de servidores de atualização da Kaspersky para o repositório do Servidor de Administração, bem como atualizar bancos de dados e módulos do software da Kaspersky para o Kaspersky Security Center. Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

   Se a rede tiver pontos de distribuição atribuídos, as atualizações serão baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Nesse caso, os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.

   Instruções de como proceder:

   - Console de Administração: Criação da tarefa para baixar as atualizações para o repositório do Servidor de Administração
   - Kaspersky Security Center Web Console: Criação da tarefa para baixar as atualizações para o repositório do Servidor de Administração

3. **Criar a tarefa para baixar as atualizações para os repositórios de pontos de distribuição (opcional)**

   Por padrão, as atualizações são baixadas para os pontos de distribuição do Servidor de Administração. Você pode configurar o Kaspersky Security Center para baixar as atualizações para os pontos de distribuição diretamente dos servidores de atualização da Kaspersky. Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.

   Quando a rede tiver atribuído pontos de distribuição e a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for criada, os pontos de distribuição baixarão atualizações dos servidores de atualização da Kaspersky, e não do repositório do Servidor de Administração.

   Instruções de como proceder:

   - Console de Administração: Criar a tarefa ao baixar atualizações nos repositórios dos pontos de distribuição
   - Kaspersky Security Center Web Console: Criação da tarefa para baixar as atualizações para os repositórios de pontos de distribuição

4. **Configurar os pontos de distribuição**

   Quando a sua rede tem pontos de distribuição atribuídos, certifique-se de que a opção **Implementar atualizações** esteja ativada nas propriedades de todos os pontos de distribuição necessários. Quando essa opção é desativada para um ponto de distribuição, os dispositivos incluídos no escopo das atualizações de download do ponto de distribuição do repositório do Servidor de Administração.

   Se quiser que os dispositivos gerenciados recebam atualizações somente dos pontos de distribuição, ative a opção **Distribuir os arquivos somente através dos pontos de distribuição** na política de Agente de Rede.

5. **Otimizando o processo de atualização usando o modelo offline de download de atualização ou arquivos diff (opcionais)**

   Você pode otimizar o processo de atualização usando o modelo offline de download de atualização (ativado por padrão) ou usando arquivos diff. Para cada segmento de rede, você precisa escolher qual desses dois recursos ativar, porque eles não podem funcionar simultaneamente.

   Quando o modelo offline de download das atualizações for ativado, o Agente de Rede baixará as atualizações necessárias para o dispositivo gerenciado quando as atualizações forem baixadas para o repositório do Servidor de Administração, antes de o aplicativo de segurança solicitar as atualizações. Isso melhora a confiabilidade do processo de atualização. Para usar o recurso, ative a opção **Fazer antecipadamente o download das atualizações e dos bancos de dados de antivírus via Servidor de Administração (recomendado)** na política do agente de rede.

   Se não usar o modelo offline de download das atualizações, você poderá otimizar o tráfego entre o Servidor de Administração e os dispositivos gerenciados usando arquivos diff. Quando esse recurso for ativado, o Servidor de Administração ou um ponto de distribuição baixará arquivos diff em vez de arquivos inteiros de bancos de dados ou módulos de software da Kaspersky. Um arquivo diff descreve as diferenças entre duas versões de um arquivo de banco de dados ou módulo de software. Por isso, um arquivo diff ocupa menos espaço do que um arquivo inteiro. Isso resulta na redução no tráfego entre o Servidor de Administração ou os pontos de distribuição e os dispositivos gerenciados. Para usar esse recurso, ative a opção **Baixar arquivos diff** nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e/ou da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.

   Instruções de como proceder:

   - Uso de arquivos diff para atualizar bancos de dados e módulos do software da Kaspersky
   - Console de Administração: Ativar e desativar o modelo offline para o download das atualizações
   - Kaspersky Security Center Web Console: Ativar e desativar o modelo offline para o download das atualizações

6. **Verificação das atualizações baixadas (opcional)**

   Antes de instalar as atualizações baixadas, é possível verificar as atualizações pela tarefa de *Verificação de atualizações*. Essa tarefa executa em sequência as tarefas de atualização de dispositivo e as tarefas de verificação de malwares configuradas por meio configurações da coleção especificada de dispositivos de teste. Para obter os resultados da tarefa, o Servidor de Administração inicia ou bloqueia a propagação de atualização para os dispositivos restantes.

   A tarefa de *Verificação de atualizações* pode ser executada como parte da tarefa *Baixar atualizações para o repositório do Servidor de Administração*. Nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*, ative a opção **Verificar atualizações antes de distribuir** no Console de Administração ou na opção **Executar verificação de atualizações** no Kaspersky Security Center Web Console.

   Instruções de como proceder:

   - Console de Administração: Verificação das atualizações baixadas
   - Kaspersky Security Center Web Console: Verificar as atualizações baixadas

7. **Aprovar e recusar atualizações de software**

Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Você pode alterar o status para *Aprovado* ou *Negado*. As atualizações aprovadas sempre são instaladas. Se uma atualização necessitar de análise e aceitação dos termos do Contrato de Licença do Usuário Final, você primeiro precisará aceitar os termos. Depois disso, a atualização poderá ser propagada para os dispositivos gerenciados. As atualizações não definidas só podem ser instaladas no Agente de Rede e em outros componentes do Kaspersky Security Center conforme as configurações de política do Agente de Rede. As atualizações para as quais você define o status *Negado* não serão instaladas em dispositivos. Se uma atualização recusada para um aplicativo de segurança tiver sido instalada anteriormente, o Kaspersky Security Center tentará desinstalar a atualização de todos os dispositivos. As atualizações de componentes do Kaspersky Security Center não podem ser desinstaladas.

Instruções de como proceder:

- Console de Administração: Aprovação e recusa de atualizações de software
- Kaspersky Security Center Web Console: Aprovação e recusa de atualizações de software

8. **Configuração da instalação automática de atualizações e correções para componentes do Kaspersky Security Center**

   As atualizações e os patches baixados para o Agente de Rede e outros componentes do Kaspersky Security Center são instalados automaticamente. Se você deixou a opção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido** ativada nas propriedades do Agente de Rede, todas as atualizações serão instaladas automaticamente após o download no repositório (ou em vários repositórios). Se esta opção estiver desativada, as correções da Kaspersky que foram baixadas e identificadas com o status *Indefinido* somente serão instaladas após você alterar o status para *Aprovado*.

   Instruções de como proceder:

   - Console de Administração: Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center
   - Kaspersky Security Center Web Console: Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center

9. **Instalação de atualizações para o Servidor de Administração**

   As atualizações de software para o Servidor de Administração não dependem dos status de atualização. Elas não são instaladas automaticamente e devem ser previamente aprovadas pelo administrador na guia **Monitoramento** no Console de Administração (**Servidor de Administração** `<nome do servidor>` → **Monitoramento**) ou na seção **Notificações** no Kaspersky Security Center Web Console (**Monitoramento e relatórios** → **Notificações**). Depois disso, o administrador deve executar explicitamente a instalação das atualizações.

10. **Configuração da instalação automática de atualizações para os aplicativos de segurança**

    Crie as tarefas de *atualização* para os aplicativos gerenciados para que forneçam prontamente as atualizações para os aplicativos, módulos do software e bancos de dados Kaspersky, inclusive bancos de dados de antivírus. Para garantir atualizações oportunas, recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório** quando configurar a agenda de tarefas.

    Se sua rede inclui somente dispositivos IPv6 e você deseja atualizar regularmente os aplicativos de segurança instalados neles, certifique-se de que o Servidor de Administração (versão não inferior a 13.2) e o Agente de Rede (versão não inferior a 13.2) estejam instalados nos dispositivos gerenciados.

    Por padrão, atualizações para o Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Security for Linux são instaladas apenas depois que você modifica o status de atualização para *Aprovado*. É possível alterar as configurações de atualização na tarefa de *atualização*.

    Se uma atualização necessitar de análise e aceitação dos termos do Contrato de Licença do Usuário Final, você primeiro precisará aceitar os termos. Depois disso, a atualização poderá ser propagada para os dispositivos gerenciados.

    Instruções de como proceder:

- Console de Administração: A instalação automática do Kaspersky Endpoint Security atualiza em dispositivos
- Kaspersky Security Center Web Console: Instalação automática de atualizações do Kaspersky Endpoint Security em dispositivos

Resultados

Após a conclusão do cenário, o Kaspersky Security Center será configurado para atualizar os bancos de dados da Kaspersky e os aplicativos da Kaspersky instalados após o download das atualizações no repositório do Servidor de Administração ou nos repositórios de pontos de distribuição. Você poderá prosseguir para monitorar o status da rede.

Sobre atualização de bancos de dados, módulos de software e aplicativos da Kaspersky

Para ter certeza de que a proteção dos seus Servidores de Administração e dispositivos gerenciados esteja atualizada, você deverá fornecer atualizações oportunas dos seguintes:

- Bancos de dados e módulos de software da Kaspersky

  Antes de baixar os bancos de dados e módulos de software da Kaspersky, o Kaspersky Security Center verifica se os servidores da Kaspersky estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos. Isso é necessário para garantir que os bancos de dados antivírus sejam atualizados e que o nível de segurança seja mantido para os dispositivos gerenciados.

- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center

Dependendo da configuração da rede, você pode usar os seguintes esquemas de download e distribuição das atualizações necessárias para os dispositivos gerenciados:

- Ao usar uma única tarefa: *Baixar atualizações no repositório do Servidor de Administração*
- Usando duas tarefas:
  - A tarefa *Baixar atualizações no repositório do Servidor de Administração*
  - A tarefa *Baixar atualizações para os repositórios de pontos de distribuição*
- Manualmente por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP
- Diretamente dos servidores de atualização da Kaspersky para o Kaspersky Endpoint Security nos dispositivos gerenciados
- Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Usando a tarefa Baixar atualizações no repositório do Servidor de Administração

Nesse esquema, o Kaspersky Security Center baixa as atualizações através da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Em redes pequenas que contêm menos de 300 dispositivos gerenciados em um segmento de rede único ou menos de 10 dispositivos gerenciados em cada segmento de rede, as atualizações são distribuídas aos dispositivos gerenciados diretamente do repositório do Servidor de Administração (veja a figura abaixo).

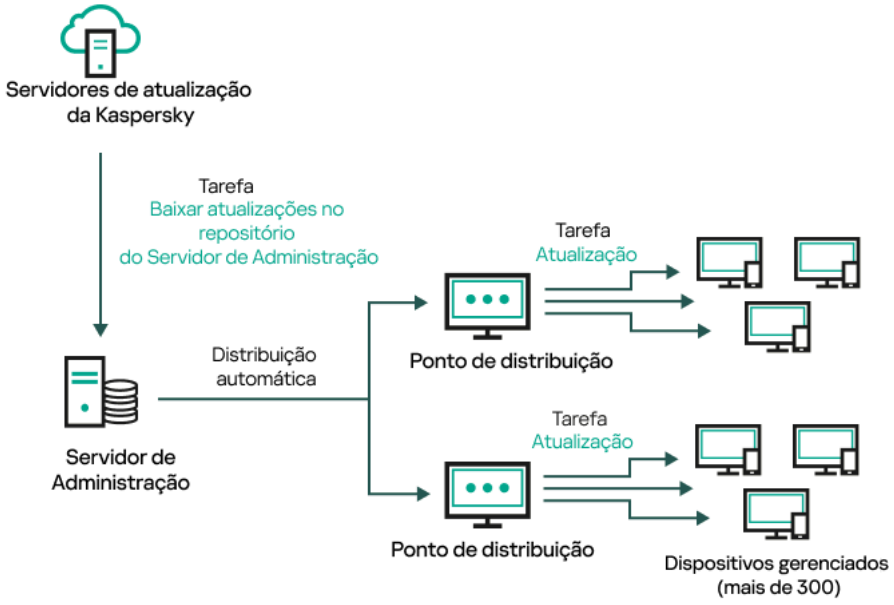


Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração sem pontos de distribuição

Por padrão, o Servidor de Administração comunica-se com os servidores de atualização Kaspersky e baixa as atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração para usar o protocolo HTTP em vez de HTTPS.

Se a rede contiver mais de 300 dispositivos gerenciados em um segmento de rede único ou se a rede consistir vários segmentos de rede com mais de 9 dispositivos gerenciados em cada segmento de rede, recomendamos o uso de pontos de distribuição para propagar as atualizações aos dispositivos gerenciados (veja a figura abaixo). Os pontos de distribuição reduzem a carga no Servidor de Administração e otimizam o tráfego entre o Servidor de Administração e os dispositivos gerenciados. Você pode calcular o número e a configuração de pontos de distribuição necessários para a rede.

Nesse esquema, as atualizações são baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.



Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração com pontos de distribuição.

Quando a tarefa *Baixar atualizações no repositório do Servidor de Administração* for concluída, as seguintes atualizações serão baixadas no repositório do Servidor de Administração:

- Módulos de software e bancos de dados da Kaspersky para o Kaspersky Security Center

  Essas atualizações são instaladas automaticamente.

- Módulos de software e bancos de dados da Kaspersky para os aplicativos de segurança nos dispositivos gerenciados

  Essas atualizações são instaladas por meio da tarefa de Atualização para o Kaspersky Endpoint Security for Windows.

- Atualizações para o Servidor de Administração

  Essas atualizações não são instaladas automaticamente. O administrador deve explicitamente aprovar e executar a instalação das atualizações.

  > É necessário ter direitos de administrador local para a instalação de patches no Servidor de Administração.

- Atualizações dos componentes do Kaspersky Security Center

  Por padrão, essas atualizações são instaladas automaticamente. Você pode alterar as configurações na política do Agente de rede.

- Atualizações dos aplicativos de segurança

  Por padrão, o Kaspersky Endpoint Security for Windows instala apenas as atualizações aprovadas por você. (Você pode aprovar atualizações pelo Console de Administração ou pelo Kaspersky Security Center Web Console). As atualizações são instaladas pela tarefa de *Atualização* e podem ser configuradas nas propriedades desta tarefa.

> A tarefa *Baixar atualizações para o repositório do Servidor de Administração* não está disponível nos Servidores de Administração virtuais. O repositório do Servidor de Administração virtual exibe as atualizações baixadas para o Servidor de Administração principal.

Você pode configurar as atualizações a serem verificadas quanto a operabilidade e erros em um conjunto de dispositivos de teste. Se a verificação for bem-sucedida, as atualizações serão distribuídas para outros dispositivos gerenciados.

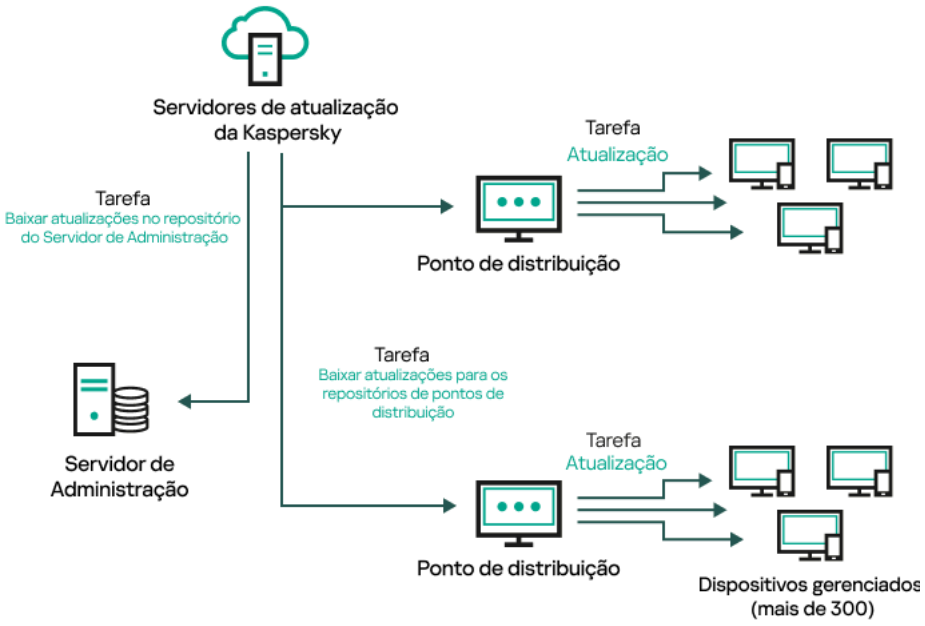
Cada aplicativo da Kaspersky solicita as atualizações necessárias do Servidor de Administração. O Servidor de Administração agrega essas solicitações e baixa somente as que são solicitadas por qualquer aplicativo. Isso garante que as mesmas atualizações não sejam baixadas várias vezes e impede que as atualizações desnecessárias sejam baixadas. Ao executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, o Servidor de Administração envia automaticamente as seguintes informações para os servidores de atualização da Kaspersky para assegurar o download das versões relevantes dos bancos de dados e dos módulos de software da Kaspersky:

- ID e versão do aplicativo
- ID de instalação do aplicativo
- ID da chave ativa
- ID de execução da tarefa *Baixar atualizações para o repositório do Servidor de Administração*

Nenhuma das informações transmitidas contém informações pessoais ou outros dados confidenciais. A AO Kaspersky Lab protege as informações de acordo com os requisitos estabelecidos por lei.

Usando duas tarefas: a tarefa Baixar atualizações no repositório do Servidor de Administração e a tarefa Baixar atualizações para os repositórios de pontos de distribuição

Você pode baixar atualizações para os repositórios de pontos de distribuição diretamente dos servidores de atualização Kaspersky em vez de do repositório do Servidor de Administração e distribuir as atualizações para os dispositivos gerenciados (veja a figura abaixo). Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.



Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração e a tarefa Baixar atualizações para os repositórios de pontos de distribuição

Por padrão, o Servidor de Administração e os pontos de distribuição comunicam-se com Servidores de atualização Kaspersky e baixam de atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração e/ou os pontos de distribuição para usar o protocolo HTTP em vez de HTTPS.

Para implementar esse esquema, crie a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* além da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Depois disso, os pontos de distribuição baixarão atualizações dos servidores de atualização Kaspersky e não do repositório do Servidor de Administração.

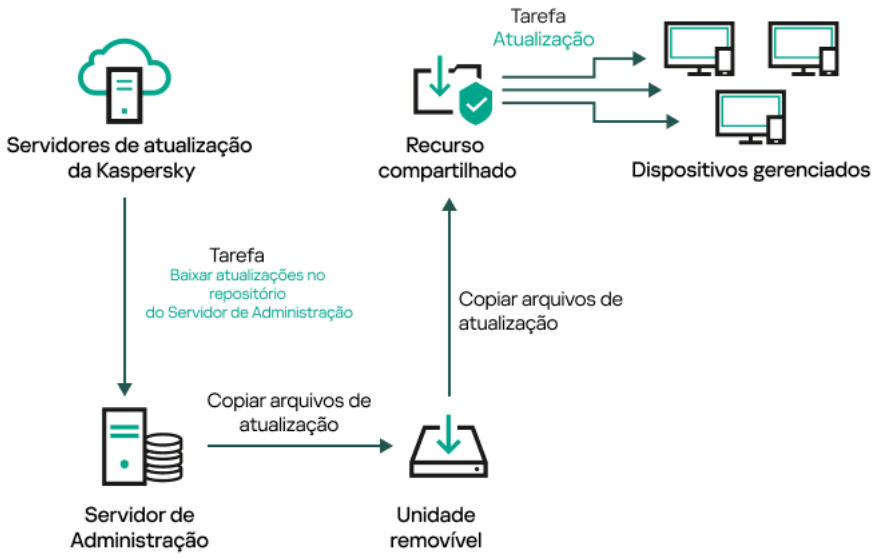
Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky.

Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.

A tarefa *Baixar atualizações no repositório do Servidor de Administração* também é necessária para esse esquema, porque essa tarefa é usada para baixar módulos de software e bancos de dados da Kaspersky para o Kaspersky Security Center.

Manualmente por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

Se os dispositivos cliente não tiverem uma conexão com o Servidor de Administração, você poderá usar uma pasta local ou um recurso compartilhado como uma origem para atualizar bancos de dados, módulos de software e aplicativos Kaspersky. Nesse esquema, você precisa copiar as atualizações necessárias do repositório do Servidor de Administração para uma unidade removível e depois copiar as atualizações para a pasta local ou o recurso compartilhado especificado como uma fonte de atualização nas configurações do Kaspersky Endpoint Security (veja a figura abaixo).



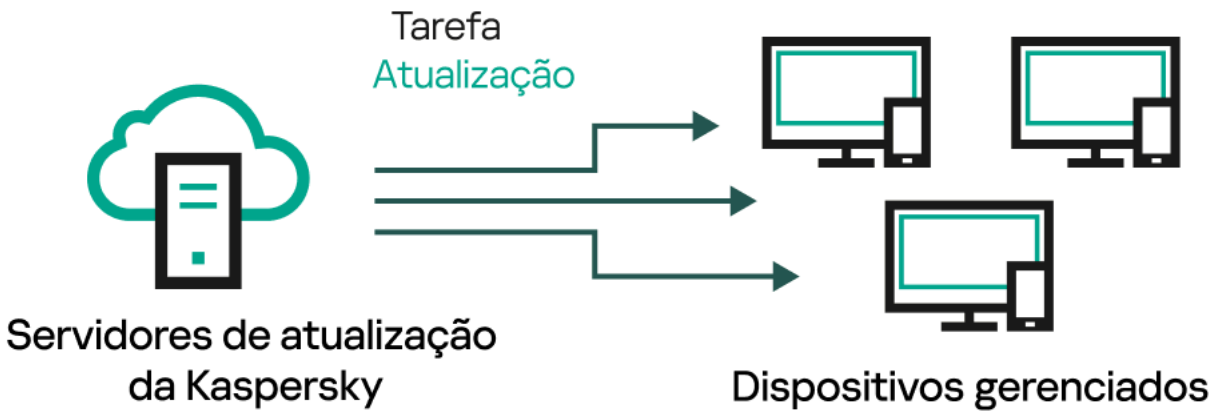
Atualização por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

Para obter mais informações sobre fontes de atualizações no Kaspersky Endpoint Security, consulte a seguinte ajuda:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux

Diretamente dos servidores de atualização da Kaspersky para o Kaspersky Endpoint Security nos dispositivos gerenciados

Nos dispositivos gerenciados, você pode configurar o Kaspersky Endpoint Security para receber atualizações diretamente dos servidores de atualização da Kaspersky (veja a figura abaixo).



Atualização de aplicativos de segurança diretamente dos servidores de atualização da Kaspersky

Nesse esquema, o aplicativo de segurança não usa os repositórios fornecidos pelo Kaspersky Security Center. Para receber atualizações diretamente dos servidores de atualização da Kaspersky, especifique os servidores de atualização da Kaspersky como uma fonte de atualização na interface do aplicativo de segurança. Para obter mais informações sobre essas configurações, consulte as seguintes ajudas:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux

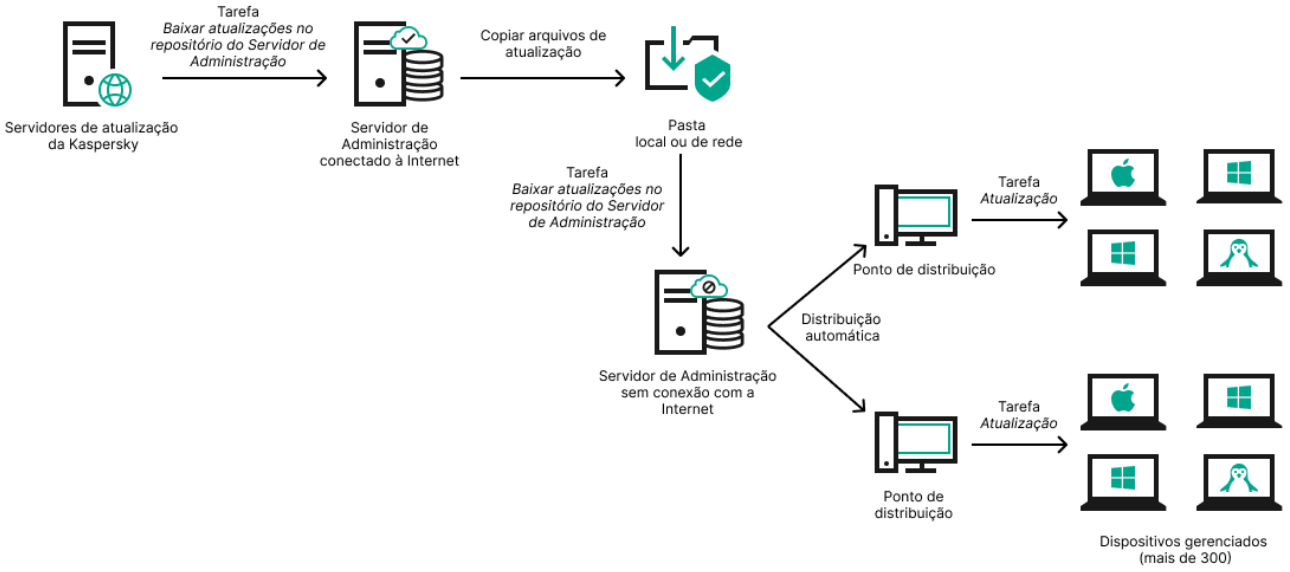
Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Se o Servidor de Administração não tiver conexão com a Internet, você poderá configurar a tarefa *Baixar atualizações no repositório do Servidor de Administração* para baixar atualizações de uma pasta local ou de rede. Nesse caso, você deve copiar os arquivos de atualização necessários para a pasta especificada de tempos em tempos. Por exemplo, você pode copiar os arquivos de atualização necessários de uma das seguintes fontes:

- Servidor de Administração que possui conexão com a Internet (veja a figura abaixo)

  Como um Servidor de Administração baixa apenas as atualizações solicitadas pelos aplicativos de segurança, os conjuntos de aplicativos de segurança gerenciados pelos Servidores de Administração (o que tem conexão com a Internet e o que não tem) devem corresponder.

Se o Servidor de Administração que você usa para baixar atualizações tiver a versão 13.2 ou anterior, abra as propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e, em seguida, ative a opção **Baixar atualizações usando o esquema antigo**.



Atualização por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

- Utilitário de atualização da Kaspersky

  Como este utilitário usa o esquema antigo para baixar atualizações, abra as propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e, em seguida, ative a opção **Baixar atualizações usando o esquema antigo**.

Sobre usar os arquivos diff para atualizar bancos de dados e módulos do software Kaspersky

Quando o Kaspersky Security Center baixa atualizações de servidores de Atualização a partir da Kaspersky, ele otimiza o tráfego usando arquivos diff. Você também pode ativar o uso de arquivos diff pelos dispositivos (Servidores de Administração, pontos de distribuição e dispositivos cliente) que recebem atualizações de outros dispositivos na rede.

Sobre o recurso Baixar arquivos diff

Um arquivo diff descreve as diferenças entre duas versões de um arquivo de banco de dados ou módulo de software. O uso de arquivos diff poupa tráfego na rede da empresa porque os arquivos diff ocupam menos espaço do que arquivos completos de bancos de dados e módulos de software. Se o recurso *Baixar arquivos diff* estiver ativado no Servidor de Administração ou em um ponto de distribuição, os arquivos diff serão salvos no Servidor de Administração ou ponto de distribuição. Como resultado, os dispositivos que recebem atualizações desse Servidor de Administração ou ponto de distribuição podem usar os arquivos diff salvos para atualizar bancos de dados e módulos de software.

Para otimizar o uso de arquivos diff, recomendamos que você sincronize os agendamentos das atualizações dos dispositivos com os do Servidor de Administração ou do ponto de distribuição a partir do qual os dispositivos são atualizados. Entretanto, pode ocorrer economia de tráfego mesmo se os dispositivos forem atualizados com muito menos frequência do que o Servidor de Administração ou o ponto de distribuição a partir do qual os dispositivos são atualizados.

O recurso Baixar arquivos diff pode ser ativado somente nos Servidores de Administração e pontos de distribuição a partir da versão 11. Para salvar arquivos diff nos Servidores de Administração e pontos de distribuição de versões anteriores, basta atualizá-los para a versão 11 ou posterior.

O recurso Baixar arquivos diff é incompatível com o modelo offline de download de atualização. Isso significa que os Agentes de Rede que usam o modelo offline de download de atualizações não baixam arquivos diff, mesmo se o recurso Baixar arquivos diff estiver ativado no Servidor de Administração ou ponto de distribuição que envia atualizações a esses Agentes de Rede.

Os pontos de distribuição não usam multicasting de IP para distribuição automática de arquivos diff.

Ativação do recurso Baixar arquivos diff

Pré-requisitos

Os pré-requisitos do cenário são os seguintes:

- Servidores de Administração e pontos de distribuição são atualizados para a versão 11 ou posterior.
- O modelo offline de download da atualização esteja desativado nas configurações da política do Agente de Rede.

Fases

1. **Como ativar o recurso no Servidor de Administração**

   Ative o recurso nas configurações da tarefa de Baixar atualizações para o repositório do Servidor de Administração.

2. **Como ativar o recurso para um ponto de distribuição**

   Ative o recurso em um ponto de distribuição que recebe atualizações por meio da tarefa Baixar atualizações para os repositórios de pontos de distribuição.

   Em seguida, ative o recurso em um ponto de distribuição que recebe atualizações do Servidor de Administração.

   O recurso é ativado nas configurações de política do Agente de Rede e, se os pontos de distribuição forem atribuídos manualmente e você quiser ignorar as configurações da política, na seção **Pontos de distribuição** das propriedades do Servidor de Administração.

Para verificar se o recurso Baixar arquivos diff está ativado com êxito, você pode medir o tráfego interno antes e depois de executar o cenário.

Criar a tarefa para baixar as atualizações no repositório do Servidor de Administração

A tarefa do Servidor de Administração *baixar atualizações para o repositório do Servidor de Administração* é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Você somente pode criar uma tarefa *Baixar atualizações para o repositório do Servidor de Administração*. Portanto, é possível criar uma tarefa *baixar atualizações para o repositório do Servidor de Administração* somente se a tarefa tiver sido removida da lista de tarefas do Servidor de Administração.

Para criar a tarefa Baixar atualizações para o repositório do Servidor de Administração:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Inicie a criação da tarefa em uma das seguintes formas:
   - No menu de contexto da pasta **Tarefas** na árvore do console, selecione **Novo** → **Tarefa**.
   - No espaço de trabalho da pasta **Tarefas**, clique no botão **Criar uma tarefa**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Na página **Selecionar o tipo de tarefa** do assistente, selecione **Baixar atualizações no repositório do Servidor de Administração**.

4. Na página **Configurações** do assistente, especifique as configurações da tarefa como segue:

- Fontes de atualizações

  Os seguintes recursos podem ser utilizados como uma origem das atualizações do Servidor de Administração:

  - Servidores de atualização da Kaspersky

    Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo. Por padrão, o Servidor de Administração comunica-se com os servidores de atualização Kaspersky e baixa as atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração para usar o protocolo HTTP em vez de HTTPS.

    Selecionado por padrão.

  - Servidor de Administração Principal

    Este recurso é aplicado a tarefas criadas para um Servidor de Administração virtual ou secundário.

  - Pasta local ou de rede

    Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Uma pasta de rede pode ser um servidor FTP ou HTTP, ou um compartilhamento SMB. Se uma pasta de rede exigir autenticação, apenas o protocolo SMB será compatível. Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado.

    Um servidor FTP ou HTTP ou pasta de rede utilizados por uma fonte de atualização devem conter uma estrutura de pastas (com atualizações) que corresponda à estrutura criada ao usar servidores de atualização Kaspersky.

- **Outras configurações**:

  - Forçar a atualização de Servidores de Administração secundários

    Caso esta opção esteja ativada, o Servidor de Administração inicia as tarefas de atualização nos Servidores de Administração secundários assim que as novas atualizações são baixadas. As tarefas de atualização são iniciadas usando a fonte de atualização configurada nas propriedades da tarefa nos Servidores de Administração secundários.

    Caso esta opção esteja desativada, as tarefas de atualização nos Servidores de Administração secundários serão iniciadas de acordo com seus agendamentos.

    Por padrão, esta opção está desativada.

  - Copiar as atualizações baixadas em pastas adicionais

Após recepção das atualizações pelo Servidor de Administração, estas são copiadas para as pastas especificadas. Use esta opção se você deseja gerenciar manualmente a distribuição das atualizações na rede.

Por exemplo, você pode desejar usar esta opção na seguinte situação: a rede de sua organização consiste em várias sub-redes independentes e os dispositivos de cada uma das sub redes não têm acesso a outras sub-redes. Entretanto, os dispositivos em todas das sub-redes têm acesso a um compartilhamento de rede comum. Neste caso, você define o Servidor de Administração em uma das sub-redes para baixar atualizações dos Servidores de Atualização Kaspersky, ativar essa opção e especificar esse compartilhamento de rede. Nas atualizações baixadas para as tarefas de repositório de outros Servidores de Administração, especifique o mesmo compartilhamento de rede como a origem da atualização.

Por padrão, esta opção está desativada.

- **Não forçar a atualização de dispositivos e Servidores de Administração secundários a não ser que a cópia tenha sido concluída**

  As tarefas de download das atualizações nos dispositivos cliente e no Servidor de Administração secundário somente inicia depois das atualizações serem copiadas da pasta principal das atualizações para as pastas de atualização adicionais.

  Essa opção deve ser ativada se os de dispositivos cliente e os Servidores de Administração secundários baixam atualizações de pastas adicionais da rede.

  Por padrão, esta opção está desativada.

- **Baixar atualizações usando o esquema antigo**

  A partir da versão 14, o Kaspersky Security Center baixa as atualizações de bancos de dados e os módulos de software usando o novo esquema. Para que o aplicativo baixe as atualizações usando o novo esquema, a fonte de atualização deve conter os arquivos de atualização com os metadados compatíveis com o novo esquema. Caso a fonte de atualização contenha os arquivos de atualização com os metadados compatíveis apenas com o esquema antigo, ative a opção **Baixar atualizações usando o esquema antigo**. Caso contrário, a tarefa de download de atualizações falhará.

  Por exemplo, é necessário habilitar essa opção quando uma pasta local ou de rede for especificada como fonte de atualização e os arquivos de atualização nessa pasta tiverem sido baixados por um dos seguintes aplicativos:

  - Utilitário de atualização da Kaspersky

    Esse utilitário baixa as atualizações usando o esquema antigo.

  - Kaspersky Security Center 13.2 ou versão anterior

    Por exemplo, o Servidor de Administração 1 não possui uma conexão com a Internet. Nesse caso, é possível baixar as atualizações usando o Servidor de Administração 2, desde que ele tenha conexão com a Internet e, em seguida, colocar as atualizações em uma pasta local ou de rede para usá-la como fonte de atualização para o Servidor de Administração 1. Caso o Servidor de Administração 2 tenha a versão 13.2 ou anterior, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa para o Servidor de Administração 1.

  Por padrão, esta opção está desativada.

5. Na página **Configurar agendamento da tarefa** do assistente, você pode criar um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- **Início agendado:**

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - **A cada N horas**

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - **A cada N dias**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - **A cada N semanas**

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - **A cada N minutos**

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - **Diariamente (não é compatível com horário de verão)**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - **Semanalmente**

    A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

6. Na página **Definir o nome da tarefa** do assistente, especifique o nome para a tarefa que você está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

7. Na página **Concluir a criação da tarefa** no assistente, clique no botão **Concluir** para fechar o assistente.

   Se você desejar que tarefa de inicie assim que o Assistente seja concluído, selecione a caixa de seleção **Executar tarefa após a conclusão do assistente**.

Após a conclusão do assistente, **Baixar atualizações no repositório do Servidor de Administração** será exibido na lista de tarefas do Servidor de Administração no espaço de trabalho.

Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Quando um Servidor de Administração executa a tarefa *baixar atualizações para o repositório do Servidor de Administração*, as atualizações de bancos de dados e módulos de software são baixadas a partir da fonte de atualizações e armazenadas na pasta compartilhada do Servidor de Administração. Se você criar esta tarefa para um grupo de administração, ela somente será aplicada aos Agentes de Rede incluídos no grupo de administração especificado.

As atualizações são distribuídas aos dispositivos clientes e aos Servidores de Administração secundários da pasta compartilhada do Servidor de Administração.

Criar as atualizações de download para a tarefa dos repositórios dos pontos de distribuição

Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky.

> Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.

É possível criar a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* para um grupo de administração. Esta tarefa será executada para pontos de distribuição incluídos no grupo de administração especificado.

Você pode usar esta tarefa, por exemplo, se o tráfego entre o Servidor de Administração e pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet. Caso o ponto de distribuição se conecte à Internet usando um servidor proxy, você precisará especificar as configurações relacionadas à política do Agente de Rede.

Para criar a tarefa "baixar atualizações para os repositórios de pontos de distribuição" para um grupo de administração selecionado:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. No espaço de trabalho da pasta, clique no botão **Nova tarefa**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Na página do assistente **Selecionar o tipo de tarefa**, selecione o nó do **Servidor de Administração do Kaspersky Security Center**, expanda a pasta **Avançado** e, em seguida, selecione a tarefa **Baixar atualizações para os repositórios de pontos de distribuição**.

4. Na página **Configurações** do assistente, especifique as configurações da tarefa como segue:

- **Fontes de atualizações**

  Os seguintes recursos podem ser utilizados como uma origem das atualizações para o ponto de distribuição:

  - Servidores de atualização da Kaspersky

    Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

    Esta opção está marcada por padrão.

  - Pasta local ou de rede

    Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Uma pasta de rede pode ser um servidor FTP ou HTTP, ou um compartilhamento SMB. Se uma pasta de rede exigir autenticação, apenas o protocolo SMB será compatível. Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado.

    Um servidor FTP ou HTTP ou pasta de rede utilizados por uma fonte de atualização devem conter uma estrutura de pastas (com atualizações) que corresponda à estrutura criada ao usar servidores de atualização Kaspersky.

- **Pasta para armazenar atualizações**

  O caminho para a pasta especificada para armazenar atualizações salvas. É possível copiar o caminho da pasta especificada para uma área de transferência. Não é possível alterar o caminho para uma pasta especificada para uma tarefa de grupo.

- **Baixar atualizações usando o esquema antigo**

A partir da versão 14, o Kaspersky Security Center baixa as atualizações de bancos de dados e os módulos de software usando o novo esquema. Para que o aplicativo baixe atualizações usando o novo esquema, a fonte de atualização deve conter os arquivos de atualização com os metadados compatíveis com o novo esquema. Caso a fonte de atualização contenha os arquivos de atualização com os metadados compatíveis apenas com o esquema antigo, ative a opção **Baixar atualizações usando o esquema antigo**. Caso contrário, a tarefa de download de atualizações falhará.

Por exemplo, é preciso habilitar essa opção quando uma pasta local ou de rede for especificada como fonte de atualização, e os arquivos de atualização nesta pasta tiverem sido baixados por um dos seguintes aplicativos:

- Utilitário de atualização da Kaspersky

  Esse utilitário baixa as atualizações usando o esquema antigo.

- Kaspersky Security Center 13.2 ou versão anterior

  Por exemplo, um ponto de distribuição está configurado para receber as atualizações de uma pasta local ou de rede. Nesse caso, é possível baixar as atualizações usando um Servidor de Administração que tenha uma conexão com a Internet e, em seguida, colocar as atualizações na pasta local no ponto de distribuição. Caso o Servidor de Administração tenha a versão 13.2 ou anterior, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa *Baixe atualizações para os repositórios de pontos de distribuição*.

Por padrão, esta opção está desativada.

5. Na página **Selecionar grupo de administração** do assistente, clique em **Browse** e selecione o grupo de administração ao qual a tarefa se aplica.

6. Na página **Configurar agendamento da tarefa** do assistente, você pode criar um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- **Início agendado:**

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - **A cada N horas**

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - **A cada N dias**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - **A cada N semanas**

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - **A cada N minutos**

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - **Diariamente (não é compatível com horário de verão)**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - **Semanalmente**

    A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

7. Na página **Definir o nome da tarefa** do assistente, especifique o nome para a tarefa que você está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

8. Na página **Concluir a criação da tarefa** no assistente, clique no botão **Concluir** para fechar o assistente.

   Se você desejar que tarefa de inicie assim que o Assistente seja concluído, selecione a caixa de seleção **Executar tarefa após a conclusão do assistente**.

Quando o assistente concluir a operação, **Baixar atualizações para os repositórios de pontos de distribuição** será exibida na lista de tarefas do Agente de Rede no grupo de administração alvo, e no espaço de trabalho **Tarefas** do console.

Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Quando a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for executada, as atualizações para bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada. As atualizações baixadas somente serão usadas por pontos de distribuição que estão incluídos no grupo de administração especificado e que não têm nenhuma tarefa de download de atualização explicitamente definida para eles.

Na janela de propriedades do Servidor de Administração, no painel **Seções** selecione **Pontos de distribuição**. Nas propriedades de cada ponto de distribuição, na seção **Fonte de atualização**, você pode especificar a fonte de atualização (**Obter do Servidor de Administração** ou **Usar a tarefa para o download forçado das atualizações**). Por padrão, **Obter do Servidor de Administração** é selecionado para um ponto de distribuição que é atribuído manualmente ou automaticamente. Esses pontos de distribuição usarão os resultados da tarefa *Baixar atualizações para os repositórios dos pontos de distribuição*.

As propriedades de cada ponto de distribuição especificam a pasta da rede que foi configurada para aquele ponto de distribuição individualmente. Os nomes de pastas podem variar para diferentes pontos de distribuição. Por esse motivo, não recomendamos que você modifique a pasta da rede nas propriedades da tarefa se a tarefa for criada para um grupo de dispositivos.

É possível modificar a pasta da rede com atualizações nas propriedades da tarefa *Baixar atualizações para os repositórios de pontos de distribuição* ao criar uma tarefa local para um dispositivo.

Configurar a tarefa de Baixar as atualizações ao repositório do Servidor de Administração

Para configurar a tarefa de Baixar as atualizações ao repositório do Servidor de Administração:

1. No espaço de trabalho da pasta **Tarefas** da árvore do console, selecione a tarefa **Baixar atualizações para o repositório do Servidor de Administração** na lista de tarefas.

2. Abra a janela Propriedades da tarefa em uma das seguintes formas:

   - Ao selecionar **Propriedades** no menu de contexto da tarefa.

   - Clicando no link **Configurar a tarefa** na caixa de informações para a tarefa selecionada.

   A janela de propriedades da tarefa *Baixar Atualizações para o Repositório do Servidor de Administração* é aberta. Nesta janela, você pode configurar a forma como as atualizações são baixadas para o repositório do Servidor de Administração.

Verificação das atualizações baixadas

Antes de instalar as atualizações nos dispositivos gerenciados, é possível verificar primeiro as atualizações sobre operabilidade e erros por meio da tarefa *Verificação de atualizações*. A tarefa de *Verificação de atualizações* é executada automaticamente como parte da tarefa *Baixar atualizações no repositório do Servidor de Administração*. O Servidor de Administração baixa as atualizações da origem, salva-as no armazenamento temporário e executa a tarefa *Verificação de atualizações*. Caso a tarefa seja concluída com êxito, as atualizações são copiadas do repositório temporário para a pasta compartilhada do Servidor de Administração (<pasta de instalação do Kaspersky Security Center>\Share\Updates). Elas são distribuídas à todos os dispositivos clientes para os quais o Servidor de Administração for a fonte de atualizações.

Caso os resultados da tarefa de *Verificação de atualizações* demonstrarem que as atualizações localizadas no repositório temporário estão incorretas ou se a tarefa de *Verificação de atualizações* concluir com erro, as atualizações não serão copiadas para a pasta compartilhada. O Servidor de Administração retém o conjunto anterior de atualizações. Além disso, as tarefas que têm o tipo de agendamento **Quando novas atualizações são baixadas no repositório** não são iniciadas. Essas operações são realizadas no próximo início da tarefa *Baixar atualizações no repositório do Servidor de Administração* se a verificação das novas atualizações for concluída com êxito.

Um conjunto de atualizações é considerado inválido se uma das seguintes condições for atendida em pelo menos um dispositivo de teste:

- Ocorreu um erro na tarefa de atualização.
- O status da proteção em tempo real do aplicativo de segurança foi modificado após a aplicação das atualizações.
- Um objeto infectado foi detectado durante a execução da tarefa de verificação sob demanda.
- Ocorreu um erro de tempo de execução de um aplicativo da Kaspersky.

Caso nenhuma das condições listadas sejam verdadeiras em nenhum dispositivo de teste, o conjunto de atualizações é considerado válido, e a tarefa *Verificação de atualizações* terá sua conclusão considerada como bem-sucedida.

Antes de começar a criar a tarefa *Verificação de atualizações*, execute os pré-requisitos:

1. Criar um grupo de administração com vários dispositivos de teste. O grupo será necessário para verificar as atualizações nele.

   Recomenda-se usar os dispositivos com a proteção mais confiável e com a configuração de aplicativo mais popular na rede. Essa abordagem aumenta a qualidade e a probabilidade de detecção de vírus durante as verificações e minimiza o risco de falsos positivos. Caso sejam detectados vírus nos dispositivos de teste, a tarefa de *Verificação de atualizações* será considerada malsucedida.

2. Crie tarefas para *Atualizar* e *Verificação de malware* para um aplicativo compatível com o Kaspersky Security Center, por exemplo, Kaspersky Endpoint Security for Windows ou Kaspersky Security for Windows Server. Ao criar as tarefas *Atualizar* e *Verificação de malware*, especifique o grupo de administração com os dispositivos de teste.

   A tarefa *Verificação de atualizações* executa sequencialmente as tarefas *Atualizar* e *Verificação de malware* em dispositivos de teste para verificar se todas as atualizações são válidas. Além disso, ao criar a tarefa *Verificação de atualizações*, será necessário especificar as tarefas *Atualizar* e *Verificação de malware*.

3. Crie a tarefa *Baixar atualizações no repositório do Servidor de Administração*.

Para que o Kaspersky Security Center verifique as atualizações baixadas antes de distribuí-las para os dispositivos cliente:

1. No espaço de trabalho da pasta **Tarefas**, selecione a tarefa *Baixar atualizações no repositório do Servidor de Administração* na lista de tarefas.

2. Abra a janela Propriedades da tarefa em uma das seguintes formas:

   - Ao selecionar **Propriedades** no menu de contexto da tarefa.
   - Ao clicar no link **Configurar a tarefa** na caixa de informações da tarefa selecionada.

3. Caso a tarefa *Verificação de atualizações* exista, clique no botão **Procurar**. Na janela aberta, selecione a tarefa *Verificação de atualizações* no grupo de administração com os dispositivos de teste.

4. Caso não tenha criado a tarefa *Verificação de atualizações* anteriormente, clique no botão **Criar**.

   O assistente da tarefa *Verificação de atualizações* é iniciado. Siga as instruções do Assistente.

5. Clique em **OK** para fechar a janela de propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*.

A verificação de atualizações automática é ativada. Agora, é possível executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, e ela começará a partir da verificação de atualização.

Configuração de políticas de teste e tarefas auxiliares

Ao criar uma tarefa de *Verificação de atualizações*, o Servidor de Administração gera políticas de teste, tarefas de atualização de grupo auxiliar e tarefas de verificação sob demanda.

> As tarefas de atualização de grupo auxiliar e de verificação sob demanda demoram ainda algum tempo. Essas tarefas são executadas quando a tarefa de *Verificação de atualizações* for executada. A tarefa de *verificação de atualizações* é realizada durante a execução da tarefa *Baixar atualizações para o repositório*. A duração da tarefa *Baixar atualizações para o repositório* inclui as tarefas de atualização de grupo auxiliar e de verificação sob demanda.

Você pode alterar as configurações de políticas de teste e tarefas auxiliares.

Para alterar as configurações de uma política de teste ou tarefa auxiliar:

1. Na árvore do console, selecione um grupo para o qual a tarefa de *Verificação de atualizações* será criada.

2. No espaço de trabalho do grupo, selecione uma das seguintes guias:

   - **Políticas**, se você quiser editar as configurações da política de teste.

   - **Tarefas**, se você quiser alterar as configurações de tarefa auxiliar.

3. No espaço de trabalho da guia, selecione uma política ou tarefa, cujas configurações você pretende alterar.

4. Abra a janela de propriedades da política (tarefa) numa das seguintes formas:

   - Selecionando **Propriedades** no menu de contexto da política (tarefa).

   - Clicando no link **Configurar política** (**Configurar a tarefa**) na caixa de informações para a política (tarefa) selecionada.

Para verificar as atualizações corretamente, defina as seguintes restrições relativa à modificação das políticas de teste das tarefas auxiliares:

- Nas configurações de tarefa auxiliar:
  - Salve todas as tarefas com os níveis de importância **Evento crítico** e **Falha funcional** no Servidor de Administração. Usando os eventos desses tipos, o Servidor de Administração analisa a operação de aplicativos.
  - Use o Servidor de Administração como a fonte de atualizações.
  - Especifique o tipo de agendamento da tarefa: **Manualmente**.
- Nas configurações das políticas de teste:
  - Desative as tecnologias de aceleração da verificação iChecker e iSwift (**Proteção Essencial contra Ameaças → Proteção Contra Ameaças ao Arquivo → Configurações → Adicional → Tecnologias de Verificação**).
  - Selecione ações em objetos infectados: **Desinfetar; excluir se a desinfecção falhar** / **Desinfetar; bloquear se a desinfecção falhar** / **Bloquear**. (**Proteção Contra Ameaças essencial → Proteção Contra Ameaças ao Arquivo → Ação na detecção de ameaças**).
- Nas configurações das políticas de teste e tarefas auxiliares:

  Se for necessário reiniciar o dispositivo após a instalação de atualizações para os módulos de software, isso deve ser executado imediatamente. Se o dispositivo não for reiniciado, é impossível testar este tipo de atualização. Para alguns aplicativos, a instalação de atualizações que requer um reinício pode ser proibida ou configurada para primeiro solicitar ao usuário uma confirmação. Estas restrições devem ser desabilitadas nas configurações das políticas de teste e tarefas auxiliares.

Visualização de atualizações baixadas

Para visualizar a lista de atualizações baixadas,

Na árvore do console, expanda a pasta **Repositórios**, e selecione a subpasta **Atualizações para os bancos de dados e módulos de software da Kaspersky**.

O espaço de trabalho da pasta **Atualizações para os bancos de dados e módulos de software da Kaspersky** mostra a lista de atualizações que são salvas no Servidor de Administração.

A instalação automática do Kaspersky Endpoint Security atualiza em dispositivos

Você pode configurar as atualizações automáticas dos bancos de dados e módulos de software do Kaspersky Endpoint Security nos dispositivos cliente.

Para configurar o download e a instalação automática das atualizações do Kaspersky Endpoint Security nos dispositivos:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Crie uma tarefa de **Atualização** de uma das seguintes formas:
   - Selecionando **Novo → Tarefa** no menu de contexto da pasta **Tarefas** na árvore do console.
   - Clicando no botão **Nova tarefa** no espaço de trabalho da pasta **Tarefas**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Na página **Selecionar o tipo de tarefa** do Assistente, selecione **Kaspersky Endpoint Security** como o tipo de tarefa e, a seguir, selecione **Atualizar** como o subtipo de tarefa.
4. Siga o restante das instruções do assistente.

   Após o Assistente concluir, uma tarefa de atualização para o Kaspersky Endpoint Security será criada. A tarefa recém criada é exibida na lista de tarefas no espaço de trabalho da pasta **Tarefas**.
5. No espaço de trabalho da pasta **Tarefas**, selecione uma tarefa de atualização que você criou.
6. No menu de contexto da tarefa, selecione **Propriedades**.
7. Na janela de propriedades da tarefa que se abre, no painel **Seções** selecione **Opções**.

   Na seção **Opções**, você pode definir as configurações da tarefa de atualização no modo local ou off-line:
   - **Configurações da atualização para modo local**: a conexão é estabelecida entre o dispositivo e o Servidor de Administração.
   - **Configurações da atualização para modo móvel**: nenhuma conexão é estabelecida entre o Kaspersky Security Center e o dispositivo (por exemplo, quando o dispositivo não está conectado à Internet).
8. Clique no botão **Configurações** para selecionar a fonte da atualização.
9. Selecione a opção **Baixar atualizações dos módulos do aplicativo** para baixar e instalar atualizações do módulo de software junto com bancos de dados do aplicativo.

   Se a caixa de seleção estiver marcada, o Kaspersky Endpoint Security notifica o usuário sobre as atualizações dos módulos de software disponíveis e inclui atualizações nos módulos de software no pacote de atualização ao executar a tarefa de atualização. Configure o uso dos módulos de atualização:
   - **Instalar atualizações críticas e aprovadas**. Se quaisquer atualizações do módulo de software estiverem disponíveis, o Kaspersky Endpoint Security as instala com o status *Crítico*; as atualizações remanescentes serão instaladas após a sua aprovação.
   - **Instale apenas atualizações aprovadas**. Se quaisquer atualizações do módulo de software estiverem disponíveis, o Kaspersky Endpoint Security as instala após a sua aprovação; elas serão instaladas localmente através da interface do aplicativo ou do Kaspersky Security Center.

   Se a atualização do módulo de software requerer a revisão e aceitação dos termos do Contrato de Licença e da Política de Privacidade, o aplicativo instala as atualizações após os termos do Contrato de Licença e da Política de Privacidade terem sido aceitos pelo usuário.

10. Selecione a opção **Copiar atualizações para pasta** para que o aplicativo salve as atualizações baixadas em uma pasta. Depois, clique no botão **Procurar**.

11. Clique em **OK**.

Ao executar a tarefa de **Atualização**, o aplicativo envia solicitações aos servidores de atualização Kaspersky.

Algumas atualizações necessitam da instalação das versões mais recentes dos plug-ins de gerenciamento.

Modelo offline de download da atualização

O Agente de Rede em dispositivos gerenciados as vezes não pode se conectar com o Servidor de Administração para receber atualizações. Por exemplo, um Agente de Rede pode ter sido instalado em um notebook que as vezes não tem acesso à Internet e nenhum acesso a rede local. Mais ainda, o administrador pode limitar o tempo de conexão de dispositivos cliente na rede. Em tais casos, os dispositivos com o Agente de Rede instalado não podem receber as atualizações do Servidor de Administração com base no agendamento existente. Se você configurou a atualização dos aplicativos gerenciados (como o Kaspersky Endpoint Security) usando o Agente de Rede, cada atualização requer uma conexão com o Servidor de Administração. Quando nenhuma conexão estiver estabelecida entre o Agente de Rede e o Servidor de Administração, a atualização é impossível. Você pode configurar a conexão entre o Agente de Rede e o Servidor de Administração para que o Agente de Rede se conecte ao Servidor de Administração em intervalos de tempo especificados. No pior dos casos, se os intervalos de conexão especificados forem sobrepostos com períodos quando nenhuma conexão estiver disponível, os bancos de dados nunca serão atualizados. Além disso, podem ocorrer problemas quando múltiplos aplicativos gerenciados tentam simultaneamente acessar o Servidor de Administração para receber atualizações. Neste caso, o Servidor de Administração poderá parar de responder as solicitações (similar a um ataque DDoS).

Para evitar problemas como os mencionados acima, um modelo offline para baixar atualizações e módulos de aplicativos gerenciados é implementado no Kaspersky Security Center. Este modelo fornece um mecanismo para a distribuição de atualizações, a despeito de problemas temporários causados pela inacessibilidade dos canais de comunicação do Servidor de Administração. Este modelo também reduz a carga no Servidor de Administração.

Como funciona o modelo offline de download da atualização

Quando o Servidor de Administração recebe atualizações, ele notifica o Agente de Rede (nos dispositivos em que ele esteja instalado) sobre as atualizações que serão necessárias para os aplicativos gerenciados. Quando o Agentes de Rede recebe informações sobre essas atualizações, ele baixa dos arquivos relevantes do Servidor de Administração com antecedência. Na primeira conexão com o Agente de Rede, o Servidor de Administração inicia um download de atualizações. Após o Agente de Rede ter baixado todas as atualizações em um dispositivo cliente, as atualizações se tornam disponíveis para os aplicativos naquele dispositivo.

Quando um aplicativo gerenciado em um dispositivo cliente tentar acessar o Agente de Rede quanto a atualizações, o Agente de Rede verifica se ele tem todas as atualizações necessárias. Se as atualizações forem recebidas do Servidor de Administração até 25 horas antes de terem sido solicitadas pelo aplicativo gerenciado, o Agente de Rede não se conectará ao Servidor de Administração, mas fornecerá ao aplicativo gerenciado as atualizações do cache local. A conexão com o Servidor de Administração pode não ser estabelecida quando o Agente de Rede fornecer atualizações aos aplicativos em dispositivos cliente, mas a conexão não é necessária para a atualização.

Para distribuir a carga no Servidor de Administração, os Agentes de Rede em um dispositivo se conecta ao Servidor de Administração e baixar as atualizações em ordem aleatória durante o intervalo de tempo especificado pelo Servidor de Administração. Esse intervalo de tempo depende do número dos dispositivos com o Agente de Rede instalado que baixam as atualizações e do tamanho destas atualizações. Para reduzir a carga no Servidor de Administração, você pode usar Agente de Rede como um ponto de distribuição.

Se o modelo offline para download das atualizações estiver desativado, as atualizações são distribuídas segundo o agendamento da tarefa de download das atualizações.

Por padrão, o modelo offline para download das atualizações está ativado.

O modelo offline de download da atualização somente é usado com os dispositivos gerenciados nos quais a tarefa para recuperar as atualizações por aplicativos gerenciados tiver **Quando novas atualizações são baixadas no repositório** selecionado como o tipo de agendamento. Para outros dispositivos gerenciados, o esquema padrão é usado para recuperar as atualizações do Servidor de Administração no modo de tempo real.

Recomendamos que você desative o modelo offline de download da atualização usando as configurações das políticas de Agente de Rede de grupos de administração relevantes nestes casos: se os aplicativos gerenciados tiverem a recuperação do conjunto de atualizações não do Servidor de Administração, mas de servidores da Kaspersky ou uma pasta na rede, e se a tarefa de download de atualizações tiver **Quando novas atualizações são baixadas no repositório** selecionado como o tipo de agendamento.

Ativar e desativar o modelo offline de download da atualização

Recomendamos que você evite desativar o modelo offline de download da atualização. Sua desativação pode causar falhas na entrega da atualização aos dispositivos. Em determinados casos, o especialista de Suporte Técnico da Kaspersky pode recomendar que você desmarque a caixa de seleção **Baixar atualizações e bancos de dados de antivírus de Servidor de Administração com antecedência**. Então, você terá que assegurar-se de que a tarefa para receber atualizações para aplicativos Kaspersky foi configurada.

Para ativar ou desativar o modelo offline de download da atualização para um grupo de administração:

1. Na árvore do console, selecione o grupo de administração para o qual você precisa ativar o modelo offline de download da atualização.
2. No espaço de trabalho do grupo, abra a guia **Políticas**.
3. Na guia **Políticas**, selecione a política do Agente de Rede.
4. No menu de contexto da política, selecione **Propriedades**.

   Abra a janela de propriedades da política do Agente de Rede.
5. Na janela de propriedades da política, selecione a seção **Gerenciar patches e atualizações**.
6. Selecione ou limpe a caixa de seleção **Fazer antecipadamente o download das atualizações e dos bancos de dados de antivírus via Servidor de Administração (recomendado)** para ativar ou desativar, respectivamente, o modelo offline de download da atualização.

   Por padrão, o modelo offline para download das atualizações está ativado.

O modelo offline de download da atualização será ativado ou desativado.

Atualização automática e correção para componentes do Kaspersky Security Center

Por padrão, quaisquer atualizações e patches baixados são instalados automaticamente para os seguintes componentes do aplicativo:

- Agente de Rede para Windows
- Console de Administração
- Servidor de dispositivos móveis Exchange
- Servidor MDM do iOS

A atualização e correção automática de componentes do Kaspersky Security Center está disponível somente para os dispositivos que executam o Windows. Você pode desativar a atualização e a correção automática para estes componentes. Neste caso, qualquer atualização e correção que foi baixada será instalada somente após você modificar o seu status para *Aprovado*. As atualizações e patches com o status *Indefinido* não serão instaladas.

Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center

A instalação automática de atualizações e patches para componentes do Kaspersky Security Center é ativada por padrão durante a instalação do Agente de Rede no dispositivo. Você pode desativá-lo durante a instalação do Agente de Rede ou desativá-lo em outro momento usando uma política.

Para desativar a atualização automática e a correção para componentes do Kaspersky Security Center durante a instalação local do Agente de Rede em um dispositivo:

1. Inicie a instalação local do Agente de Rede no dispositivo.
2. Na etapa **Configurações avançadas**, desmarque a caixa de seleção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**.
3. Siga as instruções do Assistente.

O Agente de Rede com a atualização e correção automática desativada para os componentes do Kaspersky Security Center será instalado no dispositivo. É possível ativar a atualização e a aplicação de patches automáticas mais tarde usando uma política.

Para desativar a atualização e a correção automática dos componentes do Kaspersky Security Center durante a instalação do Agente de Rede no dispositivo através de um pacote de instalação:

1. Na árvore do console, selecione a pasta **Instalação remota → Pacotes de instalação**.
2. No menu de contexto do pacote do **Agente de Rede do Kaspersky Security Center <número da versão>**, selecione **Propriedades**.
3. Nas propriedades do pacote de instalação, na seção **Configurações** desmarque a caixa de seleção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**.

O Agente de Rede com a atualização e correção automática desativado para os componentes do Kaspersky Security Center será instalado a partir deste pacote. É possível ativar a atualização e a aplicação de patches automáticas mais tarde usando uma política.

Se esta caixa de seleção estiver marcada (ou desmarcada) durante a instalação do Agente de Rede no dispositivo, você pode subsequentemente ativar (ou desativar) a atualização automática usando a política de Agente de Rede.

Para ativar ou desativar a atualização e a correção automática para os componentes do Kaspersky Security Center usando a política de Agente de Rede:

1. Na árvore do console, selecione o grupo de administração para o qual você precisa ativar ou desativar a atualização e correção automática.
2. No espaço de trabalho do grupo, abra a guia **Políticas**.
3. Na guia **Políticas**, selecione a política do Agente de Rede.
4. No menu de contexto da política, selecione **Propriedades**.

   Abra a janela de propriedades da política do Agente de Rede.
5. Na janela de propriedades da política, selecione a seção **Gerenciar patches e atualizações**.
6. Selecione ou desmarque a caixa de seleção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido** para ativar ou desativar, respectivamente, a atualização e correção automática.
7. Defina o bloqueio para esta caixa de seleção.

A política será aplicada aos dispositivos selecionados, e a atualização e a correção automática para componentes do Kaspersky Security Center será ativada (ou desativada) nestes dispositivos.

Distribuição automática de atualizações

O Kaspersky Security Center permite a distribuição e instalação automática das atualizações em dispositivos cliente e Servidores de Administração secundários.

Distribuição automática de atualizações para dispositivos cliente

Para distribuir as atualizações do aplicativo selecionado para dispositivos cliente imediatamente após o download das atualizações para o repositório do Servidor de Administração:

1. Conecte-se ao Servidor de Administração que gerencia os dispositivos cliente.
2. Crie uma tarefa de implementação da atualização para os dispositivos cliente selecionados em uma das seguintes formas:
   - Se você precisar distribuir atualizações para os dispositivos cliente que pertençam ao grupo de administração selecionado, crie uma tarefa para o grupo selecionado.
   - Se você precisar distribuir as atualizações para os dispositivos cliente que pertençam a diferentes grupos de administração ou que não pertençam a nenhum grupo de administração, crie uma tarefa para dispositivos específicos.

   O Assistente para novas tarefas inicia. Siga suas instruções e realize as seguintes ações:

   a. Na janela do assistente **Tipo de tarefa**, no nó do aplicativo desejado, selecione a tarefa de implementação de atualizações.

      O nome da tarefa de implementação de atualizações exibido na janela **Tipo de tarefa** depende do aplicativo para o qual você cria esta tarefa. Para obter informações detalhadas sobre os nomes das tarefas de atualização para os aplicativos Kaspersky selecionados, consulte os Guias correspondentes.

   b. Na janela do assistente **Agendamento**, no campo **Início agendado**, selecione **Quando novas atualizações são baixadas no repositório**.

   A tarefa de distribuição de atualização recentemente criada será iniciada para os dispositivos selecionados sempre que as atualizações forem baixadas no repositório do Servidor de Administração.

Se uma tarefa de distribuição de atualização para o aplicativo necessário for criada para os dispositivos selecionados, para distribuir automaticamente as atualizações para os dispositivos cliente, na janela de propriedades da tarefa na seção **Agendamento**, selecione a opção **Quando novas atualizações são baixadas no repositório**, no campo **Início agendado**.

Distribuindo atualizações para Servidores de Administração secundários automaticamente

Para distribuir as atualizações do aplicativo selecionado para os Servidores de Administração secundários imediatamente após o download das atualizações para o repositório do Servidor de Administração principal:

1. Na árvore do console, no nó do Servidor de Administração principal, selecione a pasta **Tarefas**.
2. Na lista de tarefas no espaço de trabalho, selecione a tarefa Baixar atualizações para o repositório do Servidor de Administração no Servidor de Administração.

3. Abra a seção **Configurações** da tarefa selecionada numa das seguintes formas:

   - Ao selecionar **Propriedades** no menu de contexto da tarefa.
   - Clicando no link **Editar configurações** na caixa de informações para a tarefa selecionada.

4. Na seção **Configurações** da janela Propriedades da tarefa, selecione a subseção **Outras configurações**, e então clique no link **Configurar**.

5. Na janela aberta **Outras configurações**, selecione a caixa de seleção **Forçar a atualização de Servidores de Administração secundários**.

6. Nas configurações da tarefa de download de atualizações do Servidor de Administração, na guia **Configurações** da janela Propriedades da tarefa, selecione a caixa de seleção **Forçar a atualização de Servidores de Administração secundários**.

Após o Servidor de Administração principal coletar as atualizações, as tarefas de download de atualizações se iniciam automaticamente nos Servidores de Administração secundários, independentemente do agendamento.

O Servidor de Administração principal atualiza os bancos de dados antivírus de acordo com os aplicativos instalados nos Servidores de Administração secundários. Não é necessária a instalação de plug-ins adicionais e a criação de pacotes de instalação no Servidor de Administração principal.

Atribuir os pontos de distribuição automaticamente

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos.

Para atribuir os pontos de distribuição automaticamente:

1. Abra a janela principal do aplicativo.

2. Na árvore do console, selecione o nó com o nome do Servidor de Administração para o qual você deseja designar pontos de distribuição automaticamente.

3. No menu de contexto do Servidor de Administração, clique **Propriedades**.

4. Na janela de propriedades do Servidor de Administração, no painel **Seções** selecione **Pontos de distribuição**.

5. Na parte direita da janela, selecione a opção **Atribuir automaticamente os pontos de distribuição**.

   Se a atribuição automática dos dispositivos para agirem como pontos de distribuição estiver ativada, você não pode configurar manualmente os pontos de distribuição nem editar a lista de pontos de distribuição.

6. Clique em **OK**.

O Servidor de Administração atribui e configura automaticamente os pontos de distribuição.

Atribuir um dispositivo como um ponto de distribuição manualmente

O Kaspersky Security Center permite que você atribua dispositivos para agirem como pontos de distribuição.

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos. No entanto, se você tiver de optar por não atribuir pontos de distribuição automaticamente por algum motivo (por exemplo, se você quiser usar servidores exclusivamente atribuídos), poderá atribuir manualmente os pontos de distribuição após calcular seu número e configuração.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Para atribuir manualmente os dispositivos para agir como ponto de distribuição:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, selecione a seção **Pontos de distribuição** e clique no botão **Adicionar**. Este botão está disponível se **Atribuir manualmente os pontos de distribuição** foi selecionado.

   A janela **Adicionar ponto de distribuição** se abre.
4. Na janela **Adicionar ponto de distribuição**, execute as seguintes ações:

   a. Selecione um dispositivo que agirá como um ponto de distribuição (selecione um no grupo de administração ou especifique o endereço IP de um dispositivo). Ao selecionar um dispositivo, tenha em mente os recursos da operação de pontos de distribuição e os requisitos definidos para o dispositivo que age como ponto de distribuição.

   b. Indique os dispositivos específicos aos quais o ponto de distribuição distribuirá as atualizações. Você pode especificar um grupo de administração ou uma descrição da localização da rede.
5. Clique em **OK**.

   O pontos de distribuição que você adicionou será exibido na lista de pontos de distribuição na seção **Pontos de distribuição**.

6. Selecione o ponto de distribuição recém adicionado a lista e clique no botão **Propriedades** para abrir sua janela Propriedades.

7. Configure o ponto de distribuição na janela de propriedades:

- A seção **Geral** contém as configurações de interação entre o ponto de distribuição e os dispositivos cliente.

  - **Porta SSL**

    O número da porta SSL para a conexão criptografada entre dispositivos clientes e o ponto de distribuição usando SSL.

    Por padrão, a porta 13000 é usada.

  - **Usar multicast**

    Se esta opção estiver ativada, o IP multicasting será usado para distribuição automática de pacotes de instalação para dispositivos clientes dentro do grupo.

    O multicast de IP diminui o tempo necessário para instalar um aplicativo de um pacote de instalação em um grupo de dispositivos clientes, mas aumenta o tempo de instalação quando você instala um aplicativo em um único dispositivo cliente.

  - **Endereço IP multicast**

    O endereço IP que será usado para multicasting. Você pode definir um endereço IP no conjunto de 224.0.0.0 – 239.255.255.255

    Por padrão, o Kaspersky Security Center atribui automaticamente um endereço IP multicast exclusivo dentro do conjunto especificado.

  - **Número da porta IP multicast**

    Número da porta para multicasting de IP.

    Por padrão, o número de porta é 15001. Se o dispositivo com o Servidor de Administração instalado for especificado como o ponto de distribuição, por padrão a porta 13001 é usada para conexão SSL.

  - **Implementar atualizações**

    As atualizações são distribuídas para dispositivos gerenciados a partir das seguintes fontes:

    - Este ponto de distribuição, caso esta opção esteja ativada.
    - Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

    Caso utilize os pontos de distribuição para implantar atualizações, será possível economizar tráfego, pois o número de downloads será reduzido. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. É possível calcular o número de pontos de distribuição para a rede e otimizar o tráfego e a carga.

    Caso essa opção seja desativada, o número de downloads de atualização e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

  - **Implementar pacotes de instalação**

Os pacotes de instalação são distribuídos para dispositivos gerenciados a partir das seguintes fontes:

- Este ponto de distribuição, caso esta opção esteja ativada.
- Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

Se você usar pontos de distribuição para implementar pacotes de instalação, poderá economizar tráfego porque reduz o número de downloads. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. É possível calcular o número de pontos de distribuição para a rede e otimizar o tráfego e a carga.

Caso essa opção seja desativada, o número de downloads de pacotes de instalação e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

- **Usar este ponto de distribuição como um servidor push**

  No Kaspersky Security Center, um ponto de distribuição pode funcionar como um servidor push para os dispositivos gerenciados, por meio do protocolo móvel. Por exemplo, um servidor push deve ser ativado se você quiser forçar a sincronização dos dispositivos KasperskyOS com o Servidor de Administração. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Se você tiver vários pontos de distribuição atribuídos ao mesmo grupo de administração, poderá ativar o servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

  Caso os dispositivos sejam gerenciados com KasperskyOS instalado, ou planeja fazê-lo, é preciso usar um ponto de distribuição como servidor push. Você também pode usar um ponto de distribuição como um servidor push se quiser enviar notificações push para dispositivos cliente.

- **Porta do servidor push**

  A porta no ponto de distribuição que os dispositivos clientes usarão para conexão. Por padrão, a porta 13295 é usada.

- Na seção **Escopo**, especifique o escopo ao qual o ponto de distribuição distribuirá as atualizações (grupos de administração e/ou uma localização da rede).

- Na seção **Proxy da KSN**, você pode configurar o aplicativo para usar o ponto de distribuição para encaminhar solicitações da KSN a partir dos dispositivos gerenciados.

  - **Ativar Proxy da KSN no lado do ponto de distribuição**

    O serviço Proxy da KSN é executado no dispositivo que é usado como um ponto de distribuição. Use este recurso para redistribuir e otimizar o tráfego na rede.

    O ponto de distribuição envia as estatísticas da KSN, que são listadas na Declaração da Kaspersky Security Network, à Kaspersky. Por padrão, a Declaração da KSN está localizada em %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    Por padrão, esta opção está desativada. A ativação desta opção somente terá efeito se as opções **Usar Servidor de Administração como um servidor proxy** e **Concordo em usar a Kaspersky Security Network** estiverem ativadas na janela de propriedades do Servidor de Administração.

    É possível atribuir um nó de um cluster ativo-passivo a um ponto de distribuição e habilitar o servidor proxy da KSN nesse nó.

- Encaminhar solicitações do KSN ao Servidor de Administração

  O ponto de distribuição encaminha solicitações do KSN dos dispositivos gerenciados para o Servidor de Administração.

  Por padrão, esta opção está ativada.

- Acessar a KSN Cloud/KSN Privada diretamente pela internet

  O ponto de distribuição encaminha solicitações à KSN dos dispositivos gerenciados para a KSN Cloud ou KSN Privada. As solicitações KSN geradas no próprio ponto de distribuição também são enviadas diretamente à KSN Cloud ou à KSN Privada.

  Os pontos de distribuição com o Agente de Rede versão 11 (ou anterior) instalado não podem acessar diretamente a KSN Privada. Se você deseja reconfigurar os pontos de distribuição para enviar solicitações à KSN à KSN Privada, ative a opção **Encaminhar solicitações da KSN para o Servidor de Administração** para cada ponto de distribuição.

  Os pontos de distribuição com o Agente de Rede versão 12 (ou posterior) instalado podem acessar diretamente a KSN Privada.

- Ignorar configurações do Servidor Proxy ao conectar à KSN Privada

  Ative esta opção, se tiver as configurações do servidor proxy definidas nas propriedades do ponto de distribuição ou na política do Agente de Rede, mas sua arquitetura de rede requer o uso direto da KSN Privada. Caso contrário, as solicitações dos aplicativos gerenciados não alcançarão a KSN Privada.

  Esta alternativa estará disponível caso a opção **Acessar a KSN Cloud/KSN Privada diretamente pela internet** seja selecionada.

- TCP port

  O número da porta TCP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. O número da porta padrão é 13111.

- Porta UDP

  Caso deseje que o Agente de Rede seja conectado com o Servidor de Administração por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de **Porta UDP**. Por padrão, esta opção está ativada. A porta UDP padrão para estabelecer conexão com o Servidor de Administração é 15000.

- Na seção **Descoberta de dispositivos**, configure a sondagem de domínios do Windows, do Active Directory e de conjuntos de IPs pelo ponto de distribuição.

  - Domínios do Windows

    Você pode ativar a descoberta de dispositivos para domínios do Windows e definir o agendamento para a localização.

  - Active Directory

Você pode ativar a sondagem da rede para o Active Directory e definir o agendamento da sondagem.

Se você usar um ponto de distribuição do Windows, poderá selecionar uma das seguintes opções:

- **Sondar o domínio atual do Active Directory**.
- **Sondar a floresta de domínios do Active Directory**.
- **Criar sondagem apenas de domínios selecionados do Active Directory**. Se você selecionar esta opção, adicione um ou mais domínios do Active Directory à lista.

Se você usar um ponto de distribuição do Linux com o Agente de Rede versão 15 instalado, poderá sondar somente domínios do Active Directory para os quais o endereço e as credenciais do usuário foram especificados. A sondagem do domínio atual do Active Directory e da floresta de domínios do Active Directory não está disponível.

- **Intervalos de IPs**

  Você pode ativar a descoberta de dispositivos para conjuntos IPv4 e redes IPv6.

  Ao ativar a opção **Ativar sondagem de conjuntos**, você poderá adicionar conjuntos verificados e definir seu agendamento. Você pode adicionar conjuntos de IPs à lista de conjuntos verificados.

  Ao ativar a opção **Usar Zeroconf para sondar redes IPv6**, o ponto de distribuição sonda automaticamente a rede IPv6 usando rede zero configuração (também referida como *Zeroconf*). Nesse caso, os conjuntos IP especificados são ignorados, pois o ponto de distribuição sonda toda a rede. A opção **Usar Zeroconf para sondar redes IPv6** estará disponível caso o ponto de distribuição execute Linux. Para usar a sondagem do Zeroconf IPv6, é necessário instalar o utilitário avahi-browse no ponto de distribuição.

- Na seção **Avançado**, especifique a pasta que o ponto de distribuição deve usar para armazenar os dados distribuídos.

  - **Usar pasta padrão**

    Se você selecionar esta opção, o aplicativo usa a pasta de Instalação do Agente de Rede no ponto de distribuição.

  - **Usar pasta especificada**

    Se selecionar esta opção, você pode, no campo abaixo, especificar o caminho até a pasta. Pode ser uma pasta local no ponto de distribuição ou pode ser uma pasta em qualquer dispositivo na rede corporativa.

    A conta do usuário usada no ponto de distribuição para executar o Agente de Rede deve ter acesso de leitura/gravação à pasta especificada.

Os dispositivos selecionados agirão como pontos de distribuição.

Somente os dispositivos sendo executados no sistema operacional Windows podem determinar a sua localização na rede. A localização da rede não pode ser determinada para dispositivos que executam outros sistemas operacionais.

Remover um dispositivo da lista de pontos de distribuição

Para remover um dispositivo da lista de pontos de distribuição:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, na seção **Pontos de distribuição**, selecione um dispositivo que esteja agindo como um ponto de distribuição, e clique no botão **Remover**.

O dispositivo será removido da lista de pontos de distribuição e deixará de agir como um ponto de distribuição.

Você não pode remover um dispositivo da lista de pontos de distribuição se ele foi atribuído pelo Servidor de Administração automaticamente.

Baixar atualizações por pontos de distribuição

O Kaspersky Security Center permite que os pontos de distribuição recebem atualizações do Servidor de Administração, dos servidores da Kaspersky ou de uma pasta local ou de rede.

Se não for necessário especificar uma fonte de atualização, recomenda-se usar a tarefa *Baixar atualizações nos repositórios de pontos de distribuição* para um grupo de administração. Consulte o tópico a seguir para obter detalhes: Como criar a tarefa Baixar atualizações nos repositórios de pontos de distribuição.

Para configurar o download da atualização para um ponto de distribuição:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, na seção **Pontos de distribuição**, selecione o ponto de distribuição pelo qual as atualizações serão entregues aos dispositivos cliente no grupo.
4. Clique no botão **Propriedades** para abrir a janela Propriedades do ponto de distribuição selecionado.

5. Na janela de propriedades do ponto de distribuição, selecione a seção **Fontes de atualizações**.

6. Selecione uma origem de atualização para o ponto de distribuição:

   - Para permitir que o ponto de distribuição receba atualizações do Servidor de Administração, selecione **Recuperar do Servidor de Administração**:

     - **Baixar arquivos diff**

       Esta opção ativa o recurso de download dos arquivos diff.

       Por padrão, esta opção está ativada.

   - Para permitir que o ponto de distribuição receba atualizações usando uma tarefa, selecione **Usar a tarefa para o download forçado das atualizações**:

     - Clique no botão **Procurar** se tal tarefa já existir no dispositivo, e selecione a tarefa na lista que aparece.

     - Clique no botão **Nova uma tarefa** para criar uma tarefa se tal tarefa ainda não existe no dispositivo. O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

     A tarefa Baixar atualizações para os repositórios dos pontos de distribuição é uma tarefa local. Você tem que criar uma nova tarefa para cada dispositivo que age como um ponto de distribuição.

O ponto de distribuição receberá as atualizações da origem especificada.

Excluir as atualizações do software do repositório

Para excluir as atualizações de software do repositório do Servidor de Administração:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Atualizações de software**.

2. No espaço de trabalho da pasta **Atualizações de software**, selecione a atualização que você deseja excluir.

3. No menu de contexto da atualização, selecione **Excluir arquivos atualizados**.

As atualizações de software serão excluídas do repositório do Servidor de Administração.

Instalação do patch para um aplicativo Kaspersky no modo de cluster

O Kaspersky Security Center somente suporta a instalação manual de patches para aplicativos Kaspersky no modo de cluster.

Para instalar uma correção para um aplicativo da Kaspersky:

1. Baixar a correção para cada nó do cluster.
2. Executar a instalação da correção no nó ativo.
3. Aguarde até que a correção seja instalada com êxito.
4. Executar a correção em todos os subnós do cluster consecutivamente.

   Se você estiver executando a correção a partir da linha de comando, use a chave `-CLUSTER_SECONDARY_NODE`.

   A correção é agora instalada em todos os nós do cluster.
5. Executar manualmente os serviços de cluster da Kaspersky.

Cada nó do cluster é exibido no Console de Administração como um dispositivo com o Agente de Rede instalado.

Para obter informações sobre os patches instalados, consulte a pasta **Atualizações de software** ou o relatório sobre as versões de atualizações para módulos de software de aplicativos Kaspersky.

Gerenciar aplicativos de terceiros em dispositivos cliente

O Kaspersky Security Center permite o gerenciamento de aplicativos desenvolvidos pela Kaspersky e outros fornecedores e instalados em dispositivos cliente.

O administrador pode executar as seguintes ações:

- Criar categorias de aplicativos com base em critérios especificados.
- Gerenciar categorias de aplicativos que usam regras especialmente criadas.
- Gerenciar aplicativos executados em dispositivos.
- Execute o inventário e mantenha um registro de software instalado nos dispositivos.
- Corrigir vulnerabilidades em software instalado nos dispositivos.
- Instale as atualizações do Windows Update e de outros fornecedores de software nos dispositivos.
- Monitore o uso de chaves de licença para grupos de aplicativos licenciados.

Instalar atualizações de software de terceiros

O Kaspersky Security Center permite gerenciar as atualizações do software instalado em dispositivos cliente e corrigir vulnerabilidades em aplicativos da Microsoft e de produtos de outros fornecedores por meio da instalação das atualizações necessárias.

O Kaspersky Security Center pesquisa por atualizações através da tarefa de pesquisa de atualização e as baixa para o repositórios de atualizações. Após concluir a pesquisa de atualizações, o aplicativo fornece ao administrador informações sobre as atualizações disponíveis e vulnerabilidades em aplicativos que podem ser corrigidas com essas atualizações.

As informações sobre atualizações disponíveis são fornecidas pelo serviço do Windows Update. O Servidor de Administração pode ser usado como um servidor Windows Server Update Services (WSUS). Para usar o Servidor de Administração como um servidor WSUS, você deve configurar a sincronização das atualizações com o Windows Update. Após ter configurado a sincronização dos dados com o Windows Update, o Servidor de Administração fornece atualizações de serviços do Windows Update nos dispositivos no modo centralizado e com a frequência definida.

Você pode também gerenciar as atualizações de software através de uma política do Agente de Rede. Para isso, você deve criar uma política do Agente de Rede e configurar a atualização de software nas janelas correspondentes do Assistente de nova política.

O administrador pode visualizar uma lista de atualizações disponíveis na subpasta **Atualizações de software** incluída na pasta **Gerenciamento de aplicativos**. Essa pasta contém uma lista das atualizações para aplicativos da Microsoft e para produtos de software de outros fornecedores recuperadas pelo Servidor de Administração para que possam ser distribuídas para os dispositivos. Após visualizar as informações sobre as atualizações disponíveis, o administrador pode instalá-las nos dispositivos.

O Kaspersky Security Center atualiza alguns aplicativos ao remover a versão anterior do aplicativo e ao instalar uma nova versão.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Verifique e confirme se a opção **Exibir o Gerenciamento de Patches e Vulnerabilidades** está ativada na janela **Configurar a interface** dos Servidores de Administração principal e secundário. Caso contrário, a tarefa de pesquisa de atualizações processa apenas as atualizações do WSUS.

Por motivos de segurança, todas as atualizações de softwares de terceiros instaladas usando o recurso Gerenciamento de patches e vulnerabilidades são verificadas automaticamente pelas tecnologias da Kaspersky em busca de malwares. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

Antes de instalar as atualizações em todos os dispositivos cliente, você poderá executar uma instalação de teste para se certificar de que as atualizações instaladas não causam falhas no funcionamento dos aplicativos nos dispositivos cliente.

Cenário: Atualizando software de terceiros

Esta seção fornece um cenário para a atualização software de terceiros instalados nos dispositivos cliente. Software de terceiros incluem aplicativos da Microsoft e de outros fornecedores de software. As atualizações para aplicativos Microsoft são fornecidas pelo serviço Windows Update.

Pré-requisitos

O Servidor de Administração deve ter uma conexão com a Internet para instalar atualizações de software de terceiros que não sejam software Microsoft.

Por padrão, a conexão com a Internet não é necessária para que o Servidor de Administração instale atualizações de software da Microsoft nos dispositivos gerenciados. Por exemplo, os dispositivos gerenciados podem baixar as atualizações de software da Microsoft diretamente dos servidores de Atualizações da Microsoft ou do Windows Server com o Microsoft Windows Server Update Services (WSUS) implementado na rede da sua organização. O Servidor de Administração deve estar conectado à Internet quando você usa o Servidor de Administração como servidor WSUS.

Fases

A atualização de software de terceiros prossegue em fases:

1. **Procurar atualizações necessárias**

   Para encontrar as atualizações de softwares de terceiros necessárias para os dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Kaspersky Security Center recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

   A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo Assistente de Início Rápido do Servidor de Administração. Caso não tenha executado o assistente, crie a tarefa ou execute o Assistente de Início Rápido rápido agora.

   Instruções de como proceder:

   - Console de administração: Verificando aplicativos em busca de vulnerabilidades, Agendando a tarefa Encontrar as vulnerabilidades e as atualizações necessárias
   - Kaspersky Security Center Web Console: Criar a tarefa Encontrar as vulnerabilidades e as atualizações necessárias, Configurações da tarefa Encontrar as vulnerabilidades e as atualizações necessárias

2. **Analisar a lista de atualizações encontradas**

   Exiba a lista **Atualizações de software** e decida quais atualizações devem ser instaladas. Para visualizar informações detalhadas sobre cada atualização, clique no nome da atualização na lista. Para cada atualização na lista, você também pode visualizar as estatísticas sobre a instalação da atualização nos dispositivos cliente.

   Instruções de como proceder:

   - Console de administração: Visualizando informações sobre atualizações disponíveis
   - Kaspersky Security Center Web Console: Visualizando informações sobre atualizações de software de terceiros disponíveis

3. **Configurar instalação de atualizações**

Quando o Kaspersky Security Center receber a lista de atualizações de software de terceiros, será possível instalá-las em dispositivos clientes usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. Crie uma dessas tarefas. Você pode criar essas tarefas na guia **Tarefas** ou usando a lista **Atualizações de software**.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para instalar atualizações para aplicativos da Microsoft, incluindo as atualizações fornecidas pelo serviço Windows Update e atualizações de software de outros fornecedores. Observe que esta tarefa pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades.

A tarefa *Instalar as atualizações do Windows Update* não requer uma licença, mas pode ser usada para instalar apenas atualizações do Windows Update.

Para instalar algumas atualizações de software, você deve aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software. Se você recusar o EULA, a atualização do software não será instalada.

Você pode iniciar uma tarefa de instalação de atualizações. Ao especificar o agendamento de tarefas, certifique-se de que a tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

Instruções de como proceder:

- Console de administração: Corrigindo vulnerabilidades em aplicativos, exibindo informações sobre atualizações disponíveis
- Kaspersky Security Center Web Console: Criando a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades, Criando a tarefa Instalar as atualizações do Windows Update, Visualizando informações sobre atualizações de software de terceiros disponíveis

4 Agendar as tarefas

Para garantir que a lista de atualizações esteja sempre atualizada, agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para executá-la automaticamente de tempos em tempos. Por padrão, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é configurada para iniciar manualmente.

Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência. Ao agendar a tarefa *Instalar as atualizações do Windows Update*, observe que, para essa tarefa, é necessário definir a lista de atualizações todas as vezes antes de iniciá-la.

Ao agendar as tarefas, certifique-se de que uma tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

5 Aprovar e recusar atualizações de software (opcional)

Se você tiver criado a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades, poderá especificar regras para instalação da atualização nas propriedades da tarefa. Se você criou a tarefa Instalar as atualizações do Windows Update, pule esta etapa.

Para cada regra, você pode definir as atualizações a serem instaladas, dependendo do status da atualização: *Indefinido*, *Aprovado* ou *Recusado*. Por exemplo, convém criar uma tarefa específica para servidores e definir uma regra para essa tarefa para permitir a instalação apenas de atualizações do Windows Update e somente aquelas com status *Aprovado*. Depois disso, você define manualmente o status *Aprovado* para as atualizações que deseja instalar. Nesse caso, as atualizações do Windows Update com status *Indefinido* ou *Recusado* não serão instaladas nos servidores especificados para a tarefa.

O uso do status *Aprovado* para gerenciar a instalação da atualização é eficiente para uma pequena quantidade de atualizações. Para instalar várias atualizações, use as regras que você pode configurar na tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades*. Recomendamos que você defina o status *Aprovado* apenas para as atualizações específicas que não atendem aos critérios especificados nas regras. Ao aprovar manualmente uma grande quantidade de atualizações, o desempenho do Servidor de Administração é reduzido, o que pode levar à sua sobrecarga.

Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Você pode alterar o status para *Aprovado* ou *Recusado* na lista **Atualizações de software** (**Operações → Gerenciamento de patches → Atualizações de software**).

Instruções de como proceder:

- Console de Administração: Aprovação e recusa de atualizações de software
- Kaspersky Security Center Web Console: Aprovando e recusando atualizações de software de terceiros

6. **Configurando o Servidor de Administração para funcionar como servidor WSUS (Serviços de atualização do Windows Server) (opcional)**

   Por padrão, as atualizações do Windows Update são baixadas para os dispositivos gerenciados diretamente dos servidores da Microsoft. Você pode alterar essa configuração para usar o Servidor de Administração como servidor WSUS. Nesse caso, o Servidor de Administração sincroniza os dados da atualização com o Windows Update na frequência especificada e fornece atualizações no modo centralizado para o Windows Update nos dispositivos em rede.

   Para usar o Servidor de Administração como servidor WSUS, crie a tarefa Executar a sincronização com o Windows Update e marque a caixa de seleção **Usar Servidor de Administração como servidor WSUS** na política do Agente de Rede.

   Instruções de como proceder:

   - Console de Administração: Sincronizando atualizações do Windows Update com o Servidor de Administração, Configurando atualizações do Windows em uma política de Agente de Rede
   - Kaspersky Security Center Web Console: Criação da tarefa Executar a sincronização com o Windows Update

7. **Execução de uma tarefa de instalação de atualização**

   Inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. Quando você inicia essas tarefas, as atualizações são baixadas e instaladas nos dispositivos gerenciados. Após a conclusão da tarefa, verifique se ela possui o status *Concluída com êxito* na lista de tarefas.

8. **Criar o relatório sobre os resultados da instalação da atualização de software de terceiros (opcional)**

   Para ver estatísticas detalhadas sobre a instalação de atualização, gere um **Relatório de resultados da instalação de atualizações de software de terceiros**.

   Instruções de como proceder:

   - Console de Administração: Criando e visualizando um relatório
   - Kaspersky Security Center Web Console: Gerando e visualizando atualizações de software

Resultados

Se você tiver criado e configurado a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, as atualizações serão instaladas nos dispositivos gerenciados automaticamente. Quando novas atualizações são baixadas no repositório do Servidor de Administração, o Kaspersky Security Center verifica se elas atendem aos critérios especificados nas regras de atualização. Todas as novas atualizações que atendem aos critérios serão instaladas automaticamente na próxima tarefa executada.

Se você tiver criado a tarefa *Instalar atualizações do Windows Update*, apenas as atualizações especificadas nas propriedades da tarefa *Instalar atualizações do Windows Update* serão instaladas. No futuro, caso deseje instalar novas atualizações baixadas no repositório do Servidor de Administração, será preciso adicionar as atualizações necessárias à lista de atualizações da tarefa existente ou criar uma nova tarefa *Instalar atualizações do Windows Update*.

Visualização de informações sobre atualizações disponíveis para aplicativos de terceiros

Para exibir uma lista de atualizações disponíveis para aplicativos de terceiros instalados em dispositivos cliente,

Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Atualizações de software**.

No espaço de trabalho da pasta, você poderá ver uma lista de atualizações disponíveis para os aplicativos instalados nos dispositivos.

Para visualizar as propriedades de uma atualização,

No espaço de trabalho da pasta **Atualizações de software**, no menu de contexto da atualização, selecione **Propriedades**.

As seguintes informações estão disponíveis para visualização na janela de propriedades da atualização:

- Na seção **Geral**, é possível visualizar o **Status de aprovação da atualização**:
  - **Indefinido**: a atualização está disponível na lista de atualizações, mas não foi aprovada para instalação.
  - **Aprovado**: a atualização está disponível na lista de atualizações e foi aprovada para instalação.
  - **Negado**: a atualização foi recusada para instalação.
- Na seção **Atributos**, é possível visualizar os valores do campo **Instalado automaticamente**:
  - O valor **Automaticamente** é exibido se a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* puder instalar atualizações para o aplicativo. A tarefa instala automaticamente novas atualizações do endereço da web informado pelo fornecedor do software de terceiros.
  - O valor **Manualmente** é exibido se o Kaspersky Security Center não puder instalar atualizações para o aplicativo automaticamente. Você pode instalar as atualizações manualmente.

  O campo **Instalado automaticamente** não é exibido para atualizações de aplicativos Windows.
- Lista de dispositivos cliente para os quais a atualização se destina.
- Lista de componentes do sistema (pré-requisitos) que devem ser instalados antes da atualização (caso existam).
- Vulnerabilidades do software que a atualização corrigirá.

Aprovar e recusar atualizações de software

As configurações de uma tarefa de instalação de atualização podem necessitar da aprovação de atualizações que devem ser instaladas. Você pode aprovar atualizações que devem ser instaladas e recusar as atualizações que não devem ser instaladas.

Por exemplo, pode ser necessário verificar primeiro a instalação das atualizações em um ambiente de teste, assegurar-se de que elas não interferem na operação dos dispositivos e, só então, permitir a instalação dessas atualizações nos dispositivos cliente.

O uso do status *Aprovado* para gerenciar a instalação de atualizações de terceiros é eficiente para uma pequena quantidade de atualizações. Para instalar várias atualizações de terceiros, use as regras que você pode configurar na tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades*. Recomendamos que você defina o status *Aprovado* apenas para as atualizações específicas que não atendem aos critérios especificados nas regras. Ao aprovar manualmente uma grande quantidade de atualizações, o desempenho do Servidor de Administração é reduzido, o que pode levar à sua sobrecarga.

Para aprovar ou recusar uma ou várias atualizações:

1. Na árvore do console, selecione o nó **Avançado → Gerenciamento de aplicativos → Atualizações de software**.

2. No espaço de trabalho da pasta **Atualizações de software**, clique no botão **Atualizar** no canto superior direito. Uma lista das atualizações aparece.

3. Selecione as atualizações que deseja aprovar ou recusar.

   A caixa de informações dos objetos selecionados é exibida no lado direito do espaço de trabalho.

4. Na lista suspensa **Status de aprovação da atualização**, selecione **Aprovado** para aprovar as atualizações selecionadas ou **Negado** para declinar das atualizações selecionadas.

   O valor predefinido é de **Indefinido**.

As atualizações para as quais você define o status **Aprovado** são colocadas em uma fila para instalação.

As atualizações para as quais o status **Negado** é definido são desinstaladas (caso seja possível) de todos os dispositivos nos quais elas foram anteriormente instaladas. Além disso, elas não serão instaladas em outros dispositivos no futuro.

Algumas atualizações para aplicativos da Kaspersky não podem ser desinstaladas. Caso o status **Negado** seja definido para elas, o Kaspersky Security Center não desinstalará estas atualizações dos dispositivos nos quais elas foram anteriormente instaladas. No entanto, essas atualizações nunca serão instaladas em outros dispositivos no futuro. Se uma atualização para aplicativos Kaspersky não puder ser desinstalada, essa propriedade será exibida na janela de propriedades da atualização: no painel **Seções**, selecione **Geral**, e a propriedade aparecerá no espaço de trabalho sob **Requisitos de instalação**. Caso o status **Negado** seja definido para as atualizações de software de terceiros, as atualizações não serão instaladas em dispositivos para os quais elas foram planejadas, mas que ainda não foram instaladas. As atualizações ainda permanecerão nos dispositivos nos quais elas já foram instaladas. Se você tiver de exclui-las, poderá exclui-las manualmente localmente.

Sincronização de atualizações a partir do Windows Update com Servidor de Administração

Se você selecionou **Usar Servidor de Administração como servidor WSUS** na janela **Atualizar configurações de gerenciamento** do Assistente de Início Rápido, a tarefa de sincronização do Windows Update é criada automaticamente. Você pode executar a tarefa na pasta **Tarefas**. A funcionalidade de atualização de um software da Microsoft somente está disponível após a tarefa **Executar a sincronização com o Windows Update** ter sido concluída com êxito.

As atualizações de software da Microsoft podem exceder 10 GB. Verifique e confirme se o banco de dados do Servidor de Administração é capaz de acomodar esses volumes; caso contrário, a tarefa **Executar a sincronização com o Windows Update** falhará. O banco de dados Microsoft SQL Express não é compatível com a tarefa **Executar a sincronização com o Windows Update**.

A tarefa **Executar a sincronização com o Windows Update** somente baixa metadados de servidores da Microsoft. Se a rede não usar um servidor WSUS, cada dispositivo cliente baixa as atualizações da Microsoft de servidores externos independentemente.

Para criar uma tarefa para sincronização de Atualizações do Windows com o Servidor de Administração:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Atualizações de software**.

2. Clique no botão **Ações adicionais** e selecione **Configurar a sincronização do Windows Update** na lista suspensa.

   O Assistente cria a tarefa **Executar a sincronização com o Windows Update** exibida na pasta **Tarefas**.

   Isso executa o Assistente de Criação de Tarefa de Recuperação de Dados do Windows Update Center. Siga as instruções do Assistente.

Você também pode criar a tarefa Executar sincronização com o Windows Update na pasta **Tarefas** clicando no link **Criar uma tarefa**.

A Microsoft regularmente exclui as atualizações desatualizadas dos servidores da empresa para que número de atualizações atuais sempre esteja entre 200.000 e 300.000. Para reduzir o uso do espaço em disco e o tamanho do banco de dados, o Kaspersky Security Center exclui as atualizações antigas que não estão mais presentes nos servidores de atualização da Microsoft.

Ao executar a tarefa **Executar a sincronização com o Windows Update**, o aplicativo recebe uma lista das atualizações atuais de um servidor de atualização da Microsoft. A seguir, o Kaspersky Security Center compila uma lista das atualizações que se tornaram desatualizadas. Na próxima inicialização da tarefa **Encontrar as vulnerabilidades e as atualizações necessárias**, o Kaspersky Security Center sinaliza todas as atualizações desatualizadas e define a hora de exclusão para as mesmas. Na próxima inicialização da tarefa **Executar a sincronização com o Windows Update**, todas as atualizações sinalizadas para exclusão 30 dias atrás serão excluídas. O Kaspersky Security Center também verifica quanto a atualizações desatualizadas foram sinalizadas para a exclusão há mais de 180 dias, e então exclui estas atualizações mais antigas.

Quando a tarefa **Executar a sincronização com o Windows Update** for concluída e as atualizações desatualizadas são excluídas, o banco de dados ainda pode ter os códigos hash que pertencem aos arquivos de atualizações excluídas, assim como os arquivos correspondentes nos arquivos %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (se eles foram baixados anteriormente). É possível executar a tarefa de **Manutenção do Servidor de Administração** para excluir esses registros desatualizados do banco de dados e dos arquivos correspondentes.

Etapa 1. Definindo se o tráfego deve ser reduzido

Quando o Kaspersky Security Center sincroniza as atualizações com Microsoft Windows Update Servers, as informações sobre todos os arquivos são salvas no banco de dados do Servidor de Administração. Todos os arquivos necessários para uma atualização também são baixados para a unidade durante a interação com o Windows Update Agent. Em particular, o Kaspersky Security Center salva as informações sobre arquivos de atualização expressa no banco de dados e as baixa quando necessário. Baixar os arquivos de atualização expressa conduz a diminuição do espaço livre na unidade.

Para evitar uma redução no volume de espaço em disco e para reduzir o tráfego, você pode desativar a opção **Baixar os arquivos de instalação expressa**.

Se esta opção estiver selecionada, os arquivos de atualização expressas são baixados ao executar a tarefa. Por padrão, esta opção não está selecionada.

Etapa 2. Aplicativos

Nesta seção, você pode selecionar aplicativos para os quais as atualizações serão baixadas.

Se a caixa de seleção **Todos os aplicativos** estiver marcada, as atualizações serão baixadas para todos os aplicativos existentes, e para todos os aplicativos que possam ser lançados no futuro.

Por padrão, esta caixa de seleção **Todos os aplicativos** está selecionada.

Etapa 3. Categorias de atualização

Nesta seção, é possível selecionar as categorias de atualizações que serão baixadas para o Servidor de Administração.

Se a caixa de seleção **Todas as categorias** estiver marcada, as atualizações serão baixadas para todas as categorias existentes, e para todas as categorias que podem aparecer no futuro.

Por padrão, esta caixa de seleção **Todas as categorias** está selecionada.

Etapa 4. Idiomas das atualizações

Nesta janela, é possível definir os idiomas de localização das atualizações que serão baixadas para o Servidor de Administração. Selecione uma das seguintes opções para baixar os idiomas de localização para as atualizações:

- **Baixar todos os idiomas, incluindo os novos**

  Se esta opção estiver selecionada, todos os idiomas de localização disponíveis das atualizações serão baixados para o Servidor de Administração. Por padrão, esta opção está selecionada.

- **Baixar idiomas selecionados**

  Se esta opção estiver selecionada, você pode selecionar na lista os idiomas de localização das atualizações que serão baixados para o Servidor de Administração.

Etapa 5. Selecionar a conta para iniciar a tarefa

Na janela **Selecionar uma conta para executar a tarefa**, você pode especificar qual conta usar ao executar a tarefa. Selecione uma das seguintes opções:

- **Conta padrão**

  A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

  Por padrão, esta opção está selecionada.

- **Especificar conta**

  Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

  - **Conta**

    Conta sob a qual a tarefa é executada.

  - **Senha**

    Senha da conta sob a qual a tarefa será executada.

Etapa 6. Configurar um agendamento de início da tarefa

Na página **Configurar agendamento da tarefa** do Assistente, você pode criar um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- **Início agendado:**

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - **A cada N horas**

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - **A cada N dias**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - **A cada N semanas**

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - **A cada N minutos**

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - **Diariamente (não é compatível com horário de verão)**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - **Semanalmente**

    A tarefa é executada toda semana, no dia e na hora especificados.

  - **Por dias da semana**

A tarefa é executada regularmente, nos dias da semana e no horário especificados.

Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Uma vez**

  A tarefa é executada uma vez, na data e hora especificadas (por padrão, no dia em que a tarefa foi criada).

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

  Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

  Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

  Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

  Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

Etapa 7. Definir o nome da tarefa

Na janela **Definir o nome da tarefa**, especifique o nome para a tarefa que você está criando. Um nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (`"*<>?\:|`). O valor padrão é *Executar sincronização do Windows Update*.

Etapa 8. Concluir a criação da tarefa

Na janela **Concluir a criação da tarefa**, clique no botão **Concluir** para concluir o assistente.

Se você desejar que tarefa de inicie assim que o Assistente seja concluído, selecione a caixa de seleção **Executar tarefa após a conclusão do assistente**.

A tarefa de sincronização do Windows Update recentemente criada aparecerá na lista de tarefas na pasta **Tarefas** da árvore do console.

Instalar manualmente as atualizações nos dispositivos

Caso você tenha selecionado **Encontrar e instalar as atualizações necessárias** na página **Atualizar configurações de gerenciamento** do Assistente de início rápido, a tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades* será automaticamente criada. Você pode executar ou parar a tarefa na pasta **Dispositivos gerenciados** na guia **Tarefas**.

Caso você tenha selecionado **Pesquisar por atualizações necessárias** no Assistente de Início Rápido, poderá instalar as atualizações do software em dispositivos cliente através da tarefa *Instalar atualizações e corrigir vulnerabilidades*.

Você pode realizar uma das seguintes ações:

- Crie uma tarefa para instalar atualizações.
- Adicione uma regra para instalar uma atualização em uma tarefa de instalação de atualização existente.
- Nas configurações de uma tarefa de instalação de atualização existente, configure uma instalação de teste de atualizações.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Instalação de atualizações criando uma tarefa de instalação

Você pode realizar uma das seguintes ações:

- Crie uma tarefa para instalar determinadas atualizações.
- Selecione uma atualização e crie uma tarefa para instalá-la e a atualizações semelhantes.

Para instalar atualizações específicas:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Atualizações de software**.
2. No espaço de trabalho, selecione as atualizações que você deseja instalar.
3. Execute alguma das seguintes ações:
   - Clique com o botão direito em uma das atualizações selecionadas na lista e selecione **Instalar a atualização** → **Nova tarefa**.
   - Clicando no link **Instalar a atualização (criar tarefa)** na caixa de informações para as atualizações selecionadas.

4. Faça a sua escolha na solicitação exibida sobre a instalação de todas as atualizações de aplicativo anteriores. Clique em **Sim** se você concorda com a instalação das versões sucessivas do aplicativo gradativamente caso isso necessário para instalar as atualizações selecionadas. Clique em **Não** se você quiser atualizar aplicativos de uma forma direta, sem instalar as versões sucessivas. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

   O Assistente de instalação de atualizações e de criação de tarefas de correção de vulnerabilidades é iniciado. Siga as etapas do Assistente.

5. Na página **Selecionando uma opção de reinício do sistema operacional** do assistente, selecione a ação a ser executada quando o sistema operacional nos dispositivos cliente precisar ser reinicializado após a operação:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Reiniciar após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

6. Na página **Configurar agendamento da tarefa** do assistente, você pode criar um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- Início agendado:

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - A cada N horas

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - A cada N dias

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - A cada N semanas

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - A cada N minutos

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - Diariamente (não é compatível com horário de verão)

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - Semanalmente

    A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

7. Na página **Definir o nome da tarefa** do assistente, especifique o nome para a tarefa que você está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

8. Na página **Concluir a criação da tarefa** no assistente, clique no botão **Concluir** para fechar o assistente.

   Se você desejar que tarefa de inicie assim que o Assistente seja concluído, selecione a caixa de seleção **Executar tarefa após a conclusão do assistente**.

Após o assistente concluir a operação, a tarefa **Instalar atualizações necessárias e corrigir vulnerabilidades** é exibida na pasta **Tarefas**.

É possível ativar a instalação automática de componentes do sistema (pré-requisitos) antes da instalação de uma atualização, nas propriedades da tarefa *instalar as atualizações necessárias e corrigir vulnerabilidades*. Quando essa opção é ativada, todos os componentes necessários do sistema são instalados antes da atualização. Pode ser encontrada uma lista de componentes requeridos nas propriedades da atualização.

Nas propriedades da tarefa *instalar as atualizações necessárias e corrigir vulnerabilidades*, é possível permitir a instalação de atualizações que atualizam o aplicativo para uma nova versão.

Se as configurações de tarefa fornecerem regras para a instalação de atualizações de terceiros, o Servidor de Administração baixa todas as atualizações relevantes dos sites dos seus fornecedores. As atualizações são salvas no repositório do Servidor de Administração e então distribuídas e instaladas nos dispositivos onde elas são aplicáveis.

Se as configurações da tarefa fornecerem regras para a instalação de atualizações da Microsoft e o Servidor de Administração age como um Servidor WSUS, o Servidor de Administração baixa todas as atualizações relevantes no repositório e então as distribui aos dispositivos gerenciados. Se a rede não usar um servidor WSUS, cada dispositivo cliente baixa as atualizações da Microsoft de servidores externos independentemente.

Para instalar uma determinada atualização e outras semelhantes:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Atualizações de software**.

2. No espaço de trabalho, selecione a atualização que você deseja instalar.

3. Clique no botão **Executar o Assistente de Instalação de Atualização**.

   O Assistente de instalação de atualizações inicia.

   > Os recursos do Assistente de instalação das atualizações somente estão disponíveis sob a licença do Gerenciamento de patches e vulnerabilidades.

   Siga as etapas do Assistente.

4. Na página **Procurar as tarefas existentes de instalação da atualização**, especifique as seguintes configurações:

   - **Procurar tarefas que instalam esta atualização**

     Se esta opção estiver ativada, o Assistente de instalação das atualizações procurará tarefas existentes que instalem a atualização selecionada.

     Se esta opção estiver desativada ou se a pesquisa não recuperar nenhuma tarefa aplicável, o Assistente de instalação das atualizações lhe enviará uma solicitação para criar uma regra ou tarefa para instalar a atualização.

     Por padrão, esta opção está ativada.

   - **Aprovar a instalação da atualização**

     A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

     Por padrão, esta opção está desativada.

5. Se você optar por procurar tarefas de instalação de atualização existentes e se a pesquisa recuperar algumas tarefas, você poderá visualizar as propriedades dessas tarefas ou iniciá-las manualmente. Nenhuma outra ação será necessária.

   Caso contrário, clique no botão **Nova tarefa de instalação de atualização**.

6. Selecione o tipo da regra de instalação a ser adicionada à nova tarefa e clique no botão **Concluir**.

7. Faça a sua escolha na solicitação exibida sobre a instalação de todas as atualizações de aplicativo anteriores. Clique em **Sim** se você concorda com a instalação das versões sucessivas do aplicativo gradativamente caso isso necessário para instalar as atualizações selecionadas. Clique em **Não** se você quiser atualizar aplicativos de uma forma direta, sem instalar as versões sucessivas. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

   O Assistente de instalação de atualizações e de criação de tarefas de correção de vulnerabilidades é iniciado. Siga as etapas do Assistente.

8. Na página **Selecionando uma opção de reinício do sistema operacional** do assistente, selecione a ação a ser executada quando o sistema operacional nos dispositivos cliente precisar ser reinicializado após a operação:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Reiniciar após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

9. Na página **Selecionar os dispositivos aos quais a tarefa será atribuída** do assistente, selecione uma das seguintes opções:

- **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**

  A tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

  Por exemplo, pode ser necessário usar esta opção em uma tarefa de instalação do Agente de Rede em dispositivos não atribuídos.

- **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**

  Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

  Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

- **Atribuir a tarefa a uma seleção de dispositivos**

  A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

  Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

- **Atribuir tarefa a um grupo de administração**

  A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

  Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

  Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

10. Na página **Configurar agendamento da tarefa** do assistente, você pode criar um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- Início agendado:

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - A cada N horas

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - A cada N dias

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - A cada N semanas

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - A cada N minutos

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - Diariamente (não é compatível com horário de verão)

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - Semanalmente

    A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente** (selecionado por padrão)

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)

Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)

Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

11. Na página **Definir o nome da tarefa** do assistente, especifique o nome para a tarefa que você está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

12. Na página **Concluir a criação da tarefa** no assistente, clique no botão **Concluir** para fechar o assistente.

    Se você desejar que tarefa de inicie assim que o Assistente seja concluído, selecione a caixa de seleção **Executar tarefa após a conclusão do assistente**.

Quando o Assistente for concluído, a tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades** é criada e exibida na pasta **Tarefas**.

Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Atualizar para uma nova versão de um aplicativo pode causar problemas na operação de aplicativos dependentes em dispositivos.

Instalar uma atualização adicionando uma regra a uma tarefa de instalação existente

Para instalar uma atualização adicionando uma regra a uma tarefa de instalação existente:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Atualizações de software**.
2. No espaço de trabalho, selecione a atualização que você deseja instalar.
3. Clique no botão **Executar o Assistente de Instalação de Atualização**.

   O Assistente de instalação de atualizações inicia.

   Os recursos do Assistente de instalação das atualizações somente estão disponíveis sob a licença do Gerenciamento de patches e vulnerabilidades.

   Siga as etapas do Assistente.
4. Na página **Procurar as tarefas existentes de instalação da atualização**, especifique as seguintes configurações:

   - Procurar tarefas que instalam esta atualização

     Se esta opção estiver ativada, o Assistente de instalação das atualizações procurará tarefas existentes que instalem a atualização selecionada.

     Se esta opção estiver desativada ou se a pesquisa não recuperar nenhuma tarefa aplicável, o Assistente de instalação das atualizações lhe enviará uma solicitação para criar uma regra ou tarefa para instalar a atualização.

     Por padrão, esta opção está ativada.

   - Aprovar a instalação da atualização

     A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

     Por padrão, esta opção está desativada.
5. Se você optar por procurar tarefas de instalação de atualização existentes e se a pesquisa recuperar algumas tarefas, você poderá visualizar as propriedades dessas tarefas ou iniciá-las manualmente. Nenhuma outra ação será necessária.

   Caso contrário, clique no botão **Adicionar uma regra de instalação de atualização**.

6. Selecione a tarefa à qual você deseja adicionar uma regra e, a seguir, clique no botão **Adicionar regra**.

   Além disso, você pode visualizar as propriedades das tarefas existentes, iniciá-las manualmente ou criar uma nova tarefa.

7. Selecione o tipo da regra a ser adicionada à tarefa selecionada e clique no botão **Concluir**.

8. Faça a sua escolha na solicitação exibida sobre a instalação de todas as atualizações de aplicativo anteriores. Clique em **Sim** se você concorda com a instalação das versões sucessivas do aplicativo gradativamente caso isso necessário para instalar as atualizações selecionadas. Clique em **Não** se você quiser atualizar aplicativos de uma forma direta, sem instalar as versões sucessivas. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

Uma nova regra para instalar a atualização será adicionada à tarefa **Instalar atualizações necessárias e corrigir vulnerabilidades** existente.

Configurar uma instalação de teste de atualizações

Para configurar uma instalação de teste de atualizações:

1. Na árvore do console, selecione a tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades** na pasta **Dispositivos gerenciados** na guia **Tarefas**.

2. No menu de contexto da tarefa, selecione **Propriedades**.

   A janela Propriedades da tarefa **Instalar atualizações necessárias e corrigir vulnerabilidades** será aberta.

3. Na janela de propriedades da tarefa, na seção **Testar instalação**, selecione uma das opções disponíveis para testar a instalação:

   - **Não verificar**. Selecione esta opção se você não quiser efetuar uma instalação de teste de atualizações.

   - **Executar a verificação nos dispositivos selecionados**. Selecione esta opção se você quiser testar a instalação de atualizações nos dispositivos selecionados. Clique no botão **Adicionar** e selecione os dispositivos nos quais você deseja efetuar uma instalação de teste das atualizações.

   - **Executar verificação nos dispositivos no grupo especificado**. Selecione esta opção se você quiser testar a instalação de atualizações em um grupo de dispositivos. No campo **Especifique um grupo de teste**, especifique um grupo de dispositivos nos quais você deseja executar uma instalação de teste.

   - **Executar verificação no percentual de dispositivos especificados**. Selecione esta opção se você quiser testar a instalação de atualizações em alguma quantidade de dispositivos. No campo **Porcentagem de dispositivos de teste de todos os dispositivos de destino**, especifique a porcentagem de dispositivos nos quais você deseja executar uma instalação de teste de atualizações.

4. Após selecionar qualquer uma das opções, exceto **Não verificar**, no campo **Quantidade de tempo para decidir se a instalação deve continuar, em horas**, especifique o número de horas que deve decorrer desde o teste da instalação das atualizações até o início da instalação das atualizações em todos os dispositivos.

Configurar as atualizações do Windows em uma política de Agente de Rede

Para configurar o Windows Update em uma política de Agente de Rede:

1. Na árvore do console, selecione **Dispositivos gerenciados**.
2. No espaço de trabalho, selecione a guia **Políticas**.
3. Selecionar uma política do Agente de Rede.
4. No menu de contexto da política, selecione **Propriedades**.

   A janela de propriedades da política do Agente de Rede abre.
5. No painel **Seções**, selecione **Atualizações e vulnerabilidades de software**.
6. Selecione a opção **Usar Servidor de Administração como servidor WSUS** para baixar as atualizações do Windows no Servidor de Administração e então distribuí-las para os dispositivos cliente por meio do agente de rede.

   Caso a opção esteja ativada, as atualizações do Windows não serão baixadas no Servidor de Administração. Neste caso, os dispositivos cliente recebem as atualizações do Windows diretamente dos servidores do Microsoft.

7. Selecione o conjunto de atualizações que os usuários podem instalar em seus dispositivos manualmente usando o Windows Update.

Em dispositivos que executam o Windows 10, se o Windows Update já tiver encontrado atualizações para o dispositivo, a nova opção selecionada em **Permitir aos usuários gerenciar a instalação de atualizações do Windows Update** será aplicada apenas depois que as atualizações encontradas forem instaladas.

Selecione um item na lista suspensa:

- **Permitir que os usuários instalem todas as atualizações do Windows Update**

  Os usuários podem instalar todas as atualizações do Microsoft Windows Update que são aplicáveis aos seus dispositivos.

  Selecione esta opção se você não quiser interferir na instalação das atualizações.

  Quando o usuário instala atualizações do Microsoft Windows Update manualmente, as atualizações podem ser baixadas de servidores da Microsoft e não do Servidor de Administração. Isso é possível se o Servidor de Administração ainda não tiver baixado as atualizações. Baixar atualizações dos servidores da Microsoft resulta em tráfego extra.

- **Permitir que os usuários instalem apenas atualizações do Windows Update aprovadas**

  Os usuários podem instalar todas as atualizações do Microsoft Windows Update que são aplicáveis aos seus dispositivos e que você aprovou.

  Por exemplo, pode ser necessário verificar primeiro a instalação das atualizações em um ambiente de teste, assegurar-se de que elas não interferem na operação dos dispositivos e, só então, permitir a instalação dessas atualizações aprovadas nos dispositivos cliente.

  Quando o usuário instala atualizações do Microsoft Windows Update manualmente, as atualizações podem ser baixadas de servidores da Microsoft e não do Servidor de Administração. Isso é possível se o Servidor de Administração ainda não tiver baixado as atualizações. Baixar atualizações dos servidores da Microsoft resulta em tráfego extra.

- **Não permitir que os usuários instalem atualizações do Windows Update**

  Os usuários não podem instalar atualizações do Microsoft Windows Update em seus dispositivos manualmente. Todas das atualizações aplicáveis são instaladas conforme configuradas por você.

  Selecione esta opção se você deseja gerenciar a instalação das atualizações centralmente.

  Por exemplo, pode ser necessário otimizar o agendamento da atualização para que a rede não fique sobrecarregada. Você pode agendar atualizações fora do horário para que não interfiram na produtividade dos usuários.

8. Selecione o modo de pesquisa do Windows Update:

- **Ativo**

  Se essa opção estiver selecionada, o Servidor de Administração com suporte do Agente de Rede inicia uma solicitação ao Windows Update Agent no dispositivo cliente por uma fonte de atualização: Servidores do Windows Update ou WSUS. A seguir, o Agente de Rede passa as informações recebidas do Windows Update Agent para o Servidor de Administração.

  A opção entra em vigor somente se **Conectar com o servidor de atualizações para atualizar dados** A opção da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* está selecionada.

  Por padrão, esta opção está selecionada.

- **Passivo**

  Se você selecionar esta opção, o Agente de Rede passa informações ao Servidor de Administração periodicamente sobre atualizações obtidas na última sincronização do Windows Update Agent com a fonte de atualização. Se não for efetuada uma sincronização do Windows Update Agent com uma fonte de atualização, as informações sobre as atualizações no Servidor de Administração se tornam desatualizadas.

  Selecione esta opção se desejar obter atualizações do cache de memória da fonte de atualização.

- **Desativado**

  Se esta opção for selecionada, o Servidor de Administração não solicita qualquer informação sobre atualizações.

  Selecione esta opção se, por exemplo, quiser testar as atualizações no seu dispositivo local primeiro.

9. Selecione a opção **Verificar a vulnerabilidade dos arquivos executáveis ao executá-los** caso queira verificar se há vulnerabilidades nos arquivos executáveis quando eles estiverem sendo executados.

10. Certifique-se de que a edição esteja bloqueada para todas as configurações alteradas. Caso contrário, as alterações não serão aplicadas.

11. Clique em **Aplicar**.

Corrigindo vulnerabilidades de software de terceiros

Esta seção descreve os recursos do Kaspersky Security Center relacionados à correção de vulnerabilidades no software instalado nos dispositivos gerenciados.

Cenário: Encontrar e corrigir vulnerabilidades de software de terceiros

Esta seção fornece um cenário para localizar e corrigir vulnerabilidades nos dispositivos gerenciados que executam o Windows. Você pode encontrar e corrigir vulnerabilidades de software no sistema operacional e em software de terceiros, incluindo software da Microsoft.

Pré-requisitos

- O Kaspersky Security Center está implementado em sua organização.
- Há dispositivos gerenciados executando o Windows na sua organização.
- A conexão com a Internet é necessária para que o Servidor de Administração execute as seguintes tarefas:
  - Para fazer uma lista de correções recomendadas para vulnerabilidades em softwares da Microsoft. A lista é criada e atualizada regularmente por especialistas da Kaspersky.
  - Para corrigir vulnerabilidades em software de terceiros que não sejam software da Microsoft.

Fases

A localização e a correção de vulnerabilidades de software ocorre em fases:

1. **Verificar vulnerabilidades no software instalado nos dispositivos gerenciados**

   Para encontrar vulnerabilidades no software instalado nos dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Kaspersky Security Center recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

   A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Caso não tenha executado o assistente, inicie-o agora ou crie a tarefa manualmente.

   Instruções de como proceder:

   - Console de administração: Verificando aplicativos em busca de vulnerabilidades, Agendando a tarefa Encontrar as vulnerabilidades e as atualizações necessárias
   - Kaspersky Security Center Web Console: Criar a tarefa Encontrar as vulnerabilidades e as atualizações necessárias, Configurações da tarefa Encontrar as vulnerabilidades e as atualizações necessárias

2. **Analisar a lista de vulnerabilidades de software detectadas**

   Visualize a lista **Vulnerabilidades de software** e decida quais vulnerabilidades devem ser corrigidas. Para visualizar informações detalhadas sobre cada vulnerabilidade, clique no nome da vulnerabilidade na lista. Para cada vulnerabilidade na lista, você também pode visualizar as estatísticas sobre a vulnerabilidade nos dispositivos gerenciados.

   Instruções de como proceder:

   - Console de Administração: Visualizar informações sobre vulnerabilidades do software, Visualizar estatísticas das vulnerabilidades em dispositivos gerenciados
   - Kaspersky Security Center Web Console: Visualização das informações sobre as vulnerabilidades de software, Visualização das estatísticas de vulnerabilidades em dispositivos gerenciados

3. **Configurar a correção de vulnerabilidades**

   Quando as vulnerabilidades de software são detectadas, é possível corrigi-las nos dispositivos gerenciados usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa lhe permite instalar várias atualizações e corrigir várias vulnerabilidades de acordo com certas regras. Observe que esta tarefa pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades. Para corrigir vulnerabilidades de software, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* usa as atualizações de software recomendadas.

A tarefa *Corrigir vulnerabilidades* não requer a opção de licença para o recurso Gerenciamento de patches e vulnerabilidades. Para usar esta tarefa, você deve especificar manualmente as correções para vulnerabilidades em softwares de terceiros definidas pelo usuário, listadas nas configurações da tarefa. A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para softwares de terceiros.

É possível iniciar o Assistente para Correção de Vulnerabilidades, que cria uma dessas tarefas automaticamente, ou criá-las manualmente.

Instruções de como proceder:

- Console de administração: Selecionar as correções de usuário para as vulnerabilidades de software de terceiros, Corrigir as vulnerabilidades em aplicativos
- Kaspersky Security Center Web Console: Selecionar as correções do usuário para vulnerabilidades em software de terceiros, Corrigir as vulnerabilidades de software de terceiros, Criar a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades

4 Agendar as tarefas

Para garantir que a lista de vulnerabilidades esteja sempre atualizada, agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para executá-la automaticamente de tempo em tempo. A frequência média recomendada é de uma vez por semana.

Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência. Ao agendar a tarefa *Corrigir vulnerabilidades*, é necessário selecionar correções para o software da Microsoft ou especificar correções de usuário para o software de terceiros sempre que iniciar a tarefa.

Ao agendar as tarefas, certifique-se que uma tarefa para corrigir vulnerabilidades é iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

5 Ignorar vulnerabilidades de software (opcional)

Se você desejar, poderá ignorar as vulnerabilidades de software a ser corrigidas em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

Instruções de como proceder:

- Console de administração: Ignorar as vulnerabilidades do software
- Kaspersky Security Center Web Console: Ignorando vulnerabilidades de software

6 Executando uma tarefa de correção de vulnerabilidades

Inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*. Quando a tarefa estiver concluída, certifique-se que possui o status *Concluído com êxito* na lista de tarefas.

7 Criar o relatório sobre os resultados da correção de vulnerabilidades de software (opcional)

Para visualizar estatísticas detalhadas sobre a correção de vulnerabilidades, gere o Relatório de vulnerabilidades. O relatório exibe informações sobre vulnerabilidades de software que não são corrigidas. Assim, é possível ter uma ideia sobre como encontrar e corrigir vulnerabilidades em softwares de terceiros, incluindo softwares da Microsoft, em sua organização.

Instruções de como proceder:

- Console de Administração: Criando e visualizando um relatório
- Kaspersky Security Center Web Console: Gerando e visualizando atualizações de software

8. **Verificar a configuração para encontrar e corrigir vulnerabilidades em software de terceiros**

   Certifique-se de ter feito o seguinte:

   - Obtenção e revisão da lista de vulnerabilidades de software detectadas nos dispositivos gerenciados
   - Vulnerabilidades de software ignoradas, se desejado
   - A tarefa para corrigir vulnerabilidades está configurada
   - As tarefas para localizar e corrigir vulnerabilidades de software estão agendadas para que sejam iniciadas sequencialmente
   - Verificar se a tarefa para corrigir vulnerabilidades de software foi executada

Resultados

Se você criou e configurou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, as vulnerabilidades são corrigidas nos dispositivos gerenciados automaticamente. Quando a tarefa é executada, ela correlaciona a lista de atualizações de software disponíveis às regras especificadas nas configurações da tarefa. Todas as atualizações de software que atendem aos critérios das regras serão baixadas no repositório do Servidor de Administração e instaladas para corrigir as vulnerabilidades de software.

Se você criou a tarefa *Corrigir vulnerabilidades*, apenas as vulnerabilidades de software no software da Microsoft são corrigidas.

Sobre como encontrar e corrigir vulnerabilidades de software

O Kaspersky Security Center detecta e corrige vulnerabilidades de software em dispositivos gerenciados que executam os sistemas operacionais das famílias Microsoft Windows. As vulnerabilidades são detectadas no sistema operacional e no software de terceiros, incluindo o software da Microsoft.

> A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Localizar vulnerabilidades de software

Para encontrar vulnerabilidades de software, o Kaspersky Security Center usa características do banco de dados de vulnerabilidades conhecidas. Este banco de dados é criado por especialistas da Kaspersky. Ele contém informações sobre vulnerabilidades, como descrição da vulnerabilidade, data de detecção da vulnerabilidade, nível de gravidade da vulnerabilidade. Você pode encontrar os detalhes das vulnerabilidades de software no site da Kaspersky.

O Kaspersky Security Center usa a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para encontrar vulnerabilidades de software.

Em certos casos, as vulnerabilidades detectadas em um sistema operacional Microsoft Windows podem ser corrigidas usando um dos seguintes métodos:

- Instalação de uma atualização para o SO.
- Atualização do SO para uma versão mais recente (por exemplo, do Windows 10 para o Windows 11).

Neste cenário, o Kaspersky Security Center exibe duas entradas para a mesma vulnerabilidade.

Corrigir vulnerabilidades de software

Para corrigir vulnerabilidades de software, o Kaspersky Security Center usa atualizações de software emitidas pelos fornecedores do software. Os metadados das atualizações de software são baixados no repositório do Servidor de Administração como um resultado da execução da tarefa a seguir:

- *Baixar atualizações no repositório do Servidor de Administração*. Esta tarefa tem como objetivo fazer o download de metadados de atualizações para o Kaspersky e software de terceiros. Essa tarefa é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Você pode criar a tarefa Baixar atualizações no repositório do Servidor de Administração manualmente.
- *Executar a sincronização com o Windows Update*. Esta tarefa tem como objetivo baixar metadados de atualizações para o software Microsoft.

As atualizações de software para corrigir vulnerabilidades podem ser representadas como pacotes ou patches de distribuição completos. As atualizações de software que corrigem vulnerabilidades de software são denominadas *correções*. As *correções recomendadas* são aquelas recomendadas para instalação pelos especialistas da Kaspersky. *Correções do usuário* são aquelas especificadas manualmente para instalação pelos usuários. Para instalar uma correção do usuário, você deve criar um pacote de instalação contendo essa correção.

Se você possui a licença do Kaspersky Security Center com o recurso Gerenciamento de patches e vulnerabilidades, para corrigir as vulnerabilidades de software, você pode usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Esta tarefa corrige automaticamente várias vulnerabilidades instalando as correções recomendadas. Para esta tarefa, você pode configurar manualmente certas regras para corrigir várias vulnerabilidades.

Se você não possui a licença do Kaspersky Security Center com o recurso Gerenciamento de patches e vulnerabilidades, para corrigir as vulnerabilidades de software, você pode usar a tarefa *Corrigir vulnerabilidades*. Por meio desta tarefa, você pode corrigir vulnerabilidades instalando as correções recomendadas para o software da Microsoft e as correções do usuário para outros softwares de terceiros.

Por motivos de segurança, todas as atualizações de softwares de terceiros instaladas usando o recurso Gerenciamento de patches e vulnerabilidades são verificadas automaticamente pelas tecnologias da Kaspersky em busca de malwares. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Para corrigir algumas vulnerabilidades de software, é necessário aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software, se o aceite do EULA for solicitado. Se você recusar o EULA, a vulnerabilidade do software não será corrigida.

Exibir informações sobre as vulnerabilidades do software

Para exibir uma lista de vulnerabilidades detectadas nos dispositivos cliente,

Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Vulnerabilidades de software**.

A página exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos gerenciados.

Para obter informações sobre uma vulnerabilidade selecionada,

Selecione **Propriedades** no menu de contexto da vulnerabilidade.

A janela de propriedades da vulnerabilidade abre, exibindo as seguintes informações:

- Aplicativo no qual a vulnerabilidade foi detectada.
- Lista de dispositivos nos quais a vulnerabilidade foi detectada.
- Informações sobre se a vulnerabilidade foi corrigida.

Para ver o relatório sobre todas as vulnerabilidades detectadas,

Na pasta **Vulnerabilidades de software**, clique no link **Visualizar o relatório de vulnerabilidades**.

Um relatório sobre as vulnerabilidades em aplicativos instalados nos dispositivos será gerado. Você pode exibir este relatório no nó com o nome do Servidor de Administração relevante, abrindo a guia **Relatórios**.

Visualizar as estatísticas de vulnerabilidades em dispositivos gerenciados

Você pode visualizar estatísticas para cada vulnerabilidade de software em dispositivos gerenciados. As estatísticas são representadas como um diagrama. O diagrama exibe o número de dispositivos com os seguintes status:

- *Ignorado em: <número de dispositivos>*. O status será atribuído se, nas propriedades da vulnerabilidade, o usuário tiver definido manualmente a opção para ignorá-la.
- *Corrigido em: <número de dispositivos>*. O status será atribuído se a tarefa para correção de vulnerabilidade for concluída com êxito.
- *Correção agendada em: <número de dispositivos>*. O status será atribuído se o usuário tiver criado a tarefa para correção de vulnerabilidades, mas a tarefa ainda não tiver sido executada.

- *Correção aplicada em: <número de dispositivos>*. O status será atribuído se o usuário tiver selecionado manualmente uma atualização de software para correção de vulnerabilidades, mas essa atualização de software não tiver corrigido a vulnerabilidade.

- *Correção necessária em: <número de dispositivos>*. Esse status é atribuído se a vulnerabilidade tiver sido corrigida somente em alguns dispositivos gerenciados e precisar ser corrigida em mais dispositivos gerenciados.

Para exibir as estatísticas de uma vulnerabilidade nos dispositivos gerenciados:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Vulnerabilidades de software**.

   A página exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos gerenciados.

2. Selecione uma vulnerabilidade para a qual você deseja visualizar as estatísticas.

   No bloco para uso com um objeto selecionado, um diagrama do status de vulnerabilidade é exibido. Clicar em um status abre uma lista de dispositivos nos quais a vulnerabilidade tem o status selecionado.

Verificar os aplicativos quanto a vulnerabilidades

Caso o aplicativo tenha sido configurado pelo Assistente de início rápido, a tarefa de *verificação de vulnerabilidades* é criada automaticamente. Você pode exibir a tarefa na pasta **Dispositivos gerenciados** na guia **Tarefas**.

Para criar uma tarefa para a verificação de vulnerabilidades em aplicativos instalados em dispositivos cliente:

1. Na árvore do console, selecione **Avançado** → **Gerenciamento de aplicativos** e, a seguir, selecione a subpasta **Vulnerabilidades de software**.

2. No espaço de trabalho selecione **Ações adicionais** → **Configurar Verificação de Vulnerabilidades**.

   Se uma tarefa de verificação de vulnerabilidades já existir, a guia **Tarefas** da pasta **Dispositivos gerenciados** é exibida, com a tarefa existente selecionada. Caso contrário, o assistente de criação de tarefas de localização de vulnerabilidades e atualizações necessárias é iniciado. Siga as etapas do Assistente.

3. Na janela **Selecionar o tipo de tarefa**, selecione **Encontrar vulnerabilidades e atualizações necessárias**.

4. Na página **Configurações** do assistente, especifique as configurações da tarefa como segue:

- Buscar por vulnerabilidades e atualizações listadas pela Microsoft

  Ao procurar por vulnerabilidades e atualizações, o Kaspersky Security Center usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft, que estão disponíveis no momento.

  Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

  As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

- Conectar com o servidor de atualizações para atualizar dados

O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

- Servidor de Administração do Kaspersky Security Center Cloud Console (consulte as Configurações da política do Agente de Rede)
- Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
- Servidores de atualizações da Microsoft

Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

Caso esta opção esteja desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows recebidas da fonte de atualizações da Microsoft antes.

A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

Por padrão, esta opção está ativada.

A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

- O Windows Update Agent em um dispositivo gerenciado se conecta com o servidor de atualização para obter atualizações somente se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada nas propriedades da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* e a opção **Modo de pesquisa do Windows Update** estiver definida como **Ativo** nas configurações da política do Agente de Rede.
- Caso não precise do Agente de Rede para iniciar uma conexão com a fonte de atualização do Microsoft Windows e as atualizações sejam baixadas durante a execução da tarefa de *Verificação de vulnerabilidades*, será possível definir a opção **Modo de pesquisa do Windows Update** como **Passivo**, enquanto a opção **Conectar com o servidor de atualizações para atualizar dados** deve permanecer ativada. Isso permite economizar recursos e usar atualizações do Windows recebidas anteriormente para verificar vulnerabilidades. É possível usar o modo passivo se o recebimento de atualizações do Microsoft Windows for configurado de uma forma diferente. Caso o recebimento de atualizações do Microsoft Windows não seja configurado de outra forma, não defina a opção **Modo de pesquisa do Windows Update** como **Passivo**, pois, nesse caso, as informações sobre as atualizações nunca serão recebidas.
- Independentemente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativado ou desativado), caso a opção **Modo de pesquisa do Windows Update** esteja definida como **Desativado**, o Kaspersky Security Center não solicitará nenhuma informação sobre as atualizações.

- Buscar por vulnerabilidades e atualizações de terceiros, listadas pela Kaspersky

Se esta opção estiver ativada, o Kaspersky Security Center pesquisará vulnerabilidades e atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

Se esta opção estiver desativada, o Kaspersky Security Center não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

Por padrão, esta opção está ativada.

- **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**

  As pastas nas quais o Kaspersky Security Center pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

  Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista contém pastas do sistema nas quais a maioria dos aplicativos está instalada.

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento mesmo que a gravação de arquivos de rastreamento esteja desativada para o Agente de Rede no Utilitário de Diagnóstico Remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

5. Na página **Configurar agendamento da tarefa** do assistente, você pode criar um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- **Início agendado:**

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - **A cada N horas**

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - **A cada N dias**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - **A cada N semanas**

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - **A cada N minutos**

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - **Diariamente (não é compatível com horário de verão)**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - **Semanalmente**

    A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **Quando novas atualizações são baixadas no repositório**

  A tarefa é executada após as atualizações serem baixadas no repositório. Por exemplo, pode ser necessário usar esse agendamento para a tarefa Encontrar as vulnerabilidades e atualizações necessárias.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

  Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

  Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

  Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

  Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

6. Na página **Definir o nome da tarefa** do assistente, especifique o nome para a tarefa que você está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

7. Na página **Concluir a criação da tarefa** no assistente, clique no botão **Concluir** para fechar o assistente.

   Se você desejar que tarefa de inicie assim que o Assistente seja concluído, selecione a caixa de seleção **Executar tarefa após a conclusão do assistente**.

Após o assistente concluir a operação, a tarefa **encontrar vulnerabilidade e atualizações necessárias** aparece na lista de tarefas na pasta **Dispositivos gerenciados**, na guia **Tarefas**.

Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Quando a tarefa *encontrar as vulnerabilidades e as atualizações necessárias* tiver sido concluída, o Servidor de Administração exibe uma lista de vulnerabilidades encontradas em aplicativos instalados no dispositivo. Ele também exibe todas as atualizações de software necessárias para corrigir as vulnerabilidades detectadas.

Caso o código 0x80240033 "Erro 80240033 do Windows Update Agent ('Não foi possível baixar os períodos da licença.')" seja exibido, será possível resolver esse problema por meio do registro do Windows.

O Servidor de Administração não exibe a lista de atualizações de software necessárias quando duas tarefas são executadas na sequência: a tarefa *executar sincronização da atualização do Windows* que tem a opção **baixar os arquivos de instalação expressa** desativada e depois a tarefa *encontrar vulnerabilidades e atualizações necessárias*. Para exibir a lista de atualizações de software necessárias, é necessário executar a tarefa *encontrar vulnerabilidades e atualizações necessárias* novamente.

O Agente de Rede recebe as informações sobre qualquer atualização de Windows disponível e de outros produtos da Microsoft do Windows Update ou do Servidor de Administração, caso o Servidor de Administração atue como servidor WSUS. As informações são transmitidas quando os aplicativos forem iniciados (caso isso seja fornecido pela política) e em cada execução de rotina da tarefa *encontrar as vulnerabilidades e as atualizações necessárias* nos dispositivos cliente.

Correção das vulnerabilidades em aplicativos

Caso você tenha selecionado **Encontrar e instalar as atualizações necessárias** na página **Atualizar configurações de gerenciamento** do Assistente de início rápido, a tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades* será automaticamente criada. A tarefa é exibida no espaço de trabalho na pasta **Dispositivos gerenciados**, na guia **Tarefas**.

Caso contrário, você pode realizar uma das seguintes ações:

- Crie uma tarefa para corrigir vulnerabilidades instalando as atualizações disponíveis.
- Adicione uma regra para corrigir uma vulnerabilidade em uma tarefa de correção de vulnerabilidades existente.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Corrigir vulnerabilidades criando uma tarefa de correção de vulnerabilidade

Você pode realizar uma das seguintes ações:

- Crie uma tarefa para corrigir várias vulnerabilidades que atendem a determinadas regras.
- Selecione uma vulnerabilidade e crie uma tarefa para corrigi-la e a vulnerabilidades semelhantes.

Para corrigir vulnerabilidades que atendem a determinadas regras:

1. Na árvore do console, selecione Servidor de Administração nos dispositivos para os quais deseja corrigir vulnerabilidades.
2. No menu **Exibir** da janela principal do aplicativo, selecione **Configurar a interface**.
3. Na janela que se abre, marque a caixa de seleção **Exibir o Gerenciamento de Patches e Vulnerabilidades** e clique em **OK**.
4. Na janela com a mensagem do aplicativo, clique em **OK**.
5. Reinicie o Console de Administração para que as alterações entrem em vigor.
6. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.
7. No espaço de trabalho, selecione a guia **Tarefas**.
8. Clique no botão **Criar uma tarefa** para executar o Assistente para novas tarefas. Siga as etapas do Assistente.
9. Na página **Selecionar o tipo de tarefa** do assistente, selecione **Instalar atualizações de aplicativos e corrigir vulnerabilidades**.

   Se a tarefa não for exibida, verifique se sua conta tem direitos para **Ler**, **Modificar** e **Executar** na área funcional **Administração de sistema**: **Gerenciamento de Patches e Vulnerabilidades**. Você não pode criar e configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* sem esses direitos de acesso.

10. Na página **Configurações** do Assistente, especifique as configurações da tarefa como segue:

- **Especificar regras para a instalação de atualizações**

  Estas regras são aplicadas à instalação de atualizações nos dispositivos cliente. Se as regras não forem especificadas, a tarefa não terá nenhuma ação a ser executada. Para informações sobre operações com regras, consulte Regras para instalação da atualização.

- **Iniciar a instalação ao reiniciar ou fechar o dispositivo**

  Se esta opção estiver ativada, as atualizações serão instaladas quando o dispositivo for reiniciado ou desligado. Caso contrário, as atualizações são instaladas segundo o agendamento.

  Use esta opção caso a instalação das atualizações afete o desempenho do dispositivo.

  Por padrão, esta opção está desativada.

- **Instalar os componentes gerais do sistema necessários**

  Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional.

  Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

  Por padrão, esta opção está desativada.

- **Permitir a instalação de novas versões dos aplicativos durante atualizações**

  Se esta opção estiver ativada, as atualizações serão permitidas quando resultarem na instalação de uma nova versão de um aplicativo de software.

  Se esta opção estiver desativada, o software não será atualizado. Você poderá então instalar novas versões do software manualmente ou através de outra tarefa. Por exemplo, você pode usar esta opção se a infraestrutura da sua empresa não tiver como base uma nova versão do software ou se você quiser verificar uma atualização usando uma infraestrutura de teste.

  Por padrão, esta opção está ativada.

  A atualização de um aplicativo pode causar o funcionamento incorreto de aplicativos dependentes instalados em dispositivos cliente.

- **Baixar atualizações para o dispositivo sem instalá-las**

  Se esta opção estiver ativada, o aplicativo baixa as atualizações em um dispositivo cliente, mas não as instala automaticamente. Você então poderá instalar manualmente as atualizações baixadas.

  As atualizações da Microsoft são baixadas no armazenamento de sistema do Windows. Atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky e à Microsoft) são baixados na pasta especificada no campo **Pasta para download de atualizações**.

  Se esta opção estiver desativada, as atualizações serão instaladas no dispositivo automaticamente.

  Por padrão, esta opção está desativada.

- **Pasta para download de atualizações**

  Esta pasta é usada para baixar atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft).

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento mesmo que a gravação de arquivos de rastreamento esteja desativada para o Agente de Rede no Utilitário de Diagnóstico Remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

11. Na página **Selecionando uma opção de reinício do sistema operacional** do assistente, selecione a ação a ser executada quando o sistema operacional nos dispositivos cliente precisar ser reinicializado após a operação:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Reiniciar após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

12. Na página **Configurar agendamento da tarefa** do assistente, você pode criar um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- **Início agendado:**

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - **A cada N horas**

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - **A cada N dias**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - **A cada N semanas**

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - **A cada N minutos**

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - **Diariamente (não é compatível com horário de verão)**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - **Semanalmente**

    A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

13. Na página **Definir o nome da tarefa** do assistente, especifique o nome para a tarefa que você está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

14. Na página **Concluir a criação da tarefa** no assistente, clique no botão **Concluir** para fechar o assistente.

    Se você desejar que tarefa de inicie assim que o Assistente seja concluído, selecione a caixa de seleção **Executar tarefa após a conclusão do assistente**.

Após o assistente concluir a operação, a tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades** é criada e exibida na pasta **Tarefas**.

Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Caso os resultados da tarefa contenham o erro 0x80240033 "Erro do Windows Update Agent 80240033 ('Não foi possível baixar os termos da licença.')", será possível resolver esse problema no registro do Windows.

Para corrigir uma vulnerabilidade específica e outras semelhantes:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Vulnerabilidades de software**.
2. Selecione a vulnerabilidade que você quer corrigir.
3. Clique no botão **Executar o Assistente para Correção de Vulnerabilidades**.

   O assistente para Correção de vulnerabilidades é iniciado.

   Os recursos do Assistente para Correção de Vulnerabilidades somente estão disponíveis sob a licença do Gerenciamento de patches e vulnerabilidades.

   Siga as etapas do Assistente.
4. Na janela **Procurar por tarefas existentes de correção de vulnerabilidades**, especifique os seguintes parâmetros:

   - Exibir apenas tarefas que corrigem esta vulnerabilidade

     Se esta opção estiver ativada, o Assistente para correção de vulnerabilidades procurará tarefas existentes que corrigem a vulnerabilidade selecionada.

     Se esta opção estiver desativada ou se a pesquisa não produzir nenhuma tarefa aplicável, o Assistente para correção de vulnerabilidades lhe enviará uma solicitação para criar uma regra ou tarefa para corrigir a vulnerabilidade.

     Por padrão, esta opção está ativada.

   - Aprovar as atualizações que corrigem esta vulnerabilidade

     As atualizações que corrigem uma vulnerabilidade serão aprovadas para a instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas permitirem apenas a instalação de atualizações aprovadas.

     Por padrão, esta opção está desativada.
5. Se você optar por procurar tarefas de correção de vulnerabilidades existentes e se a pesquisa recuperar algumas tarefas, você poderá visualizar as propriedades dessas tarefas ou iniciá-las manualmente. Nenhuma outra ação será necessária.

   Caso contrário, clique no botão **Nova tarefa de correção de vulnerabilidades**.
6. Selecione o tipo da regra de correção de vulnerabilidades a ser adicionada à nova tarefa e clique no botão **Concluir**.

7. Faça a sua escolha na solicitação exibida sobre a instalação de todas as atualizações de aplicativo anteriores. Clique em **Sim** se você concorda com a instalação das versões sucessivas do aplicativo gradativamente caso isso necessário para instalar as atualizações selecionadas. Clique em **Não** se você quiser atualizar aplicativos de uma forma direta, sem instalar as versões sucessivas. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

   O Assistente de instalação de atualizações e de criação de tarefas de correção de vulnerabilidades é iniciado. Siga as etapas do Assistente.

8. Na página **Selecionando uma opção de reinício do sistema operacional** do assistente, selecione a ação a ser executada quando o sistema operacional nos dispositivos cliente precisar ser reinicializado após a operação:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Reiniciar após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

9. Na página **Selecionar os dispositivos aos quais a tarefa será atribuída** do assistente, selecione uma das seguintes opções:

- Selecionar os dispositivos na rede detectados pelo Servidor de Administração

  A tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

  Por exemplo, pode ser necessário usar esta opção em uma tarefa de instalação do Agente de Rede em dispositivos não atribuídos.

- Especificar endereços de dispositivos manualmente ou importar endereços de uma lista

  Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

  Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

- Atribuir a tarefa a uma seleção de dispositivos

  A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

  Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

- Atribuir tarefa a um grupo de administração

  A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

  Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

  Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

10. Na página **Configurar agendamento da tarefa** do assistente, você pode criar um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- **Início agendado:**

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - **A cada N horas**

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - **A cada N dias**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - **A cada N semanas**

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - **A cada N minutos**

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - **Diariamente (não é compatível com horário de verão)**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - **Semanalmente**

    A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

11. Na página **Definir o nome da tarefa** do assistente, especifique o nome para a tarefa que você está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

12. Na página **Concluir a criação da tarefa** no assistente, clique no botão **Concluir** para fechar o assistente.

    Se você desejar que tarefa de inicie assim que o Assistente seja concluído, selecione a caixa de seleção **Executar tarefa após a conclusão do assistente**.

Quando o Assistente for concluído, a tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades** é criada e exibida na pasta **Tarefas**.

Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Corrigir uma vulnerabilidade adicionando uma regra a uma tarefa de correção de vulnerabilidades existente

Para corrigir uma vulnerabilidade adicionando uma regra a uma tarefa de correção de vulnerabilidades existente:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Vulnerabilidades de software**.

2. Selecione a vulnerabilidade que você quer corrigir.

3. Clique no botão **Executar o Assistente para Correção de Vulnerabilidades**.

   O assistente para Correção de vulnerabilidades é iniciado.

   > Os recursos do Assistente para Correção de Vulnerabilidades somente estão disponíveis sob a licença do Gerenciamento de patches e vulnerabilidades.

   Siga as etapas do Assistente.

4. Na janela **Procurar por tarefas existentes de correção de vulnerabilidades**, especifique os seguintes parâmetros:

   - **Exibir apenas tarefas que corrigem esta vulnerabilidade**

     Se esta opção estiver ativada, o Assistente para correção de vulnerabilidades procurará tarefas existentes que corrigem a vulnerabilidade selecionada.

     Se esta opção estiver desativada ou se a pesquisa não produzir nenhuma tarefa aplicável, o Assistente para correção de vulnerabilidades lhe enviará uma solicitação para criar uma regra ou tarefa para corrigir a vulnerabilidade.

     Por padrão, esta opção está ativada.

   - **Aprovar as atualizações que corrigem esta vulnerabilidade**

     As atualizações que corrigem uma vulnerabilidade serão aprovadas para a instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas permitirem apenas a instalação de atualizações aprovadas.

     Por padrão, esta opção está desativada.

5. Se você optar por procurar tarefas de correção de vulnerabilidades existentes e se a pesquisa recuperar algumas tarefas, você poderá visualizar as propriedades dessas tarefas ou iniciá-las manualmente. Nenhuma outra ação será necessária.

   Caso contrário, clique no botão **Adicionar regra de correção de vulnerabilidades para a tarefa existente**.

6. Selecione a tarefa à qual você deseja adicionar uma regra e, a seguir, clique no botão **Adicionar regra**.

   Além disso, você pode visualizar as propriedades das tarefas existentes, iniciá-las manualmente ou criar uma nova tarefa.

7. Selecione o tipo da regra a ser adicionada à tarefa selecionada e clique no botão **Concluir**.

8. Faça a sua escolha na solicitação exibida sobre a instalação de todas as atualizações de aplicativo anteriores. Clique em **Sim** se você concorda com a instalação das versões sucessivas do aplicativo gradativamente caso isso necessário para instalar as atualizações selecionadas. Clique em **Não** se você quiser atualizar aplicativos de uma forma direta, sem instalar as versões sucessivas. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

Uma nova regra para corrigir a vulnerabilidade será adicionada à tarefa **Instalar atualizações necessárias e corrigir vulnerabilidades** existente.

Correção de vulnerabilidades em uma rede isolada

Esta seção descreve as etapas necessárias para corrigir vulnerabilidades de softwares de terceiros em dispositivos gerenciados conectados a Servidores de Administração que não têm acesso à Internet.

Cenário: correção de vulnerabilidades de softwares de terceiros em uma rede isolada

É possível instalar as atualizações e corrigir as vulnerabilidades do software de terceiros instalado em dispositivos gerenciados em uma rede isolada. Essas redes incluem Servidores de Administração e dispositivos gerenciados conectados a eles sem acesso à Internet. Para corrigir as vulnerabilidades neste tipo de rede, será necessário um Servidor de Administração conectado à Internet. Em seguida, será possível baixar patches (atualizações necessárias) usando o Servidor de Administração com acesso à Internet e depois transmitir os patches para Servidores de Administração isolados.

> É possível baixar as atualizações de softwares de terceiros emitidas por fornecedores de software, mas não é possível baixar as atualizações de software da Microsoft em Servidores de Administração isolados usando o Kaspersky Security Center.

Para saber como funciona o processo de correção de vulnerabilidades em uma rede isolada, consulte a descrição e o esquema do processo.

Pré-requisitos

Antes de começar, faça o seguinte:

1. Aloque um dispositivo para estabelecer conexão com a Internet e baixar patches. Esse dispositivo será contado como o Servidor de Administração com acesso à Internet.

2. Instale o Kaspersky Security Center, posterior à versão 14, nos seguintes dispositivos:

   - Dispositivo alocado, que atuará como Servidor de Administração com acesso à Internet

   - Dispositivos isolados, que atuarão como Servidores de Administração isolados da Internet (também chamados de Servidores de Administração isolados)

3. Certifique-se de que cada Servidor de Administração tenha espaço em disco suficiente para baixar e armazenar as atualizações e patches.

Fases

A instalação de atualizações e a correção de vulnerabilidades de softwares de terceiros em dispositivos gerenciados de Servidores de Administração isolados possuem as seguintes etapas:

1. **Configuração do Servidor de Administração com acesso à Internet**

   Prepare o Servidor de Administração com acesso à Internet para lidar com as solicitações de atualizações de softwares de terceiros necessárias e para fazer download de patches.

2. **Configuração de Servidores de Administração isolados**

   Prepare os Servidores de Administração isolados para que possam formar regularmente listas de atualizações necessárias e lidar com patches baixados pelo Servidor de Administração com acesso à Internet. Após a configuração, os Servidores de Administração isolados não tentam mais baixar os patches da Internet. Em vez disso, eles recebem atualizações por meio de patches.

3. **Transmissão de patches e instalação de atualizações em Servidores de Administração isolados**

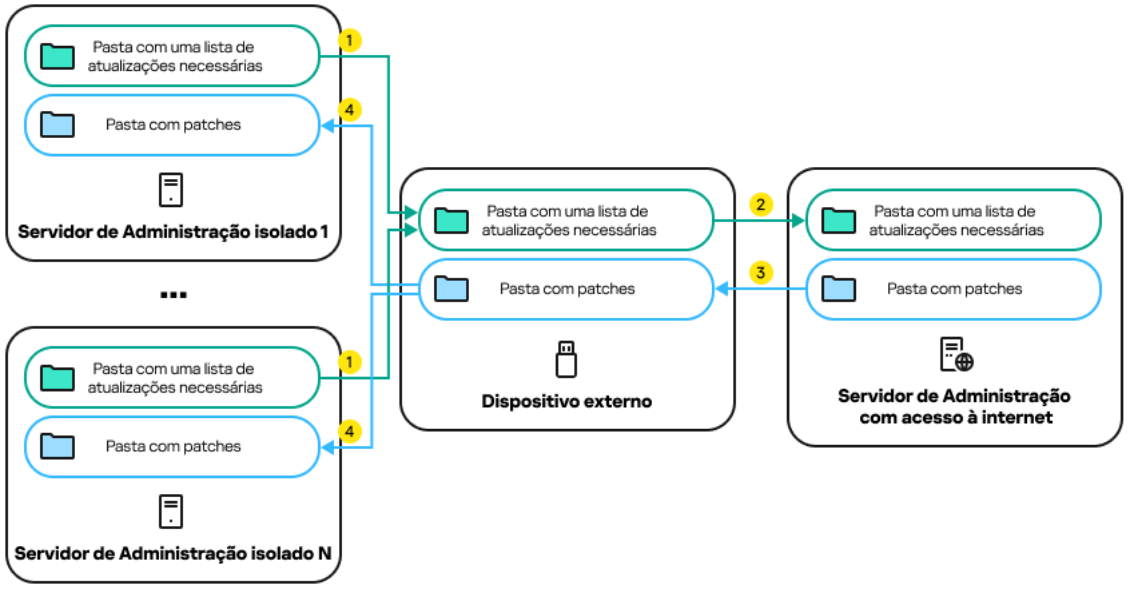
   Depois de configurar os Servidores de Administração, é possível transmitir as listas de atualizações e patches necessários entre o Servidor de Administração com acesso à Internet e os Servidores de Administração isolados. Em seguida, as atualizações de patches serão instaladas em dispositivos gerenciados usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

Resultados

Assim, as atualizações de softwares de terceiros são transmitidas para Servidores de Administração isolados e instaladas em dispositivos gerenciados conectados usando o Kaspersky Security Center. Basta configurar os Servidores de Administração uma vez e, depois disso, será possível obter as atualizações quantas vezes precisar, por exemplo, uma ou várias vezes por dia.

Sobre a correção de vulnerabilidades de softwares de terceiros em uma rede isolada

O processo de correção de vulnerabilidades de softwares de terceiros em uma rede isolada é mostrado na figura e descrito abaixo. Você pode repetir esse processo periodicamente.



O processo de transmissão de patches e a lista de atualizações necessárias entre o Servidor de Administração com acesso à Internet e Servidores de Administração isolados

Cada Servidor de Administração isolado da Internet (aqui denominado Servidor de Administração isolado) gera uma lista de atualizações que devem ser instaladas em dispositivos gerenciados conectados a esse Servidor de Administração. A lista de atualizações necessárias é armazenada em uma pasta específica e apresenta um conjunto de arquivos binários. Cada arquivo tem um nome que contém o ID do patch com a atualização necessária. Como resultado, cada arquivo na lista aponta para um patch específico.

Usando um dispositivo externo, transfira a lista de atualizações necessárias do Servidor de Administração isolado para o Servidor de Administração alocado com acesso à Internet. Depois disso, o Servidor de Administração alocado baixa os patches da Internet e os coloca em uma pasta separada.

Quando todos os patches estiverem baixados e localizados na pasta especial para eles, mova os patches para cada Servidor de Administração isolado do qual você obteve a lista de atualizações necessárias. Salve os patches na pasta criada especialmente para eles no Servidor de Administração isolado. Como resultado, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* executa os patches e instala as atualizações nos dispositivos gerenciados dos Servidores de Administração isolados.

Configuração do Servidor de Administração com acesso à Internet para corrigir vulnerabilidades em uma rede isolada

Para preparar a correção de vulnerabilidades e transmissão de patches em uma rede isolada, primeiro configure um Servidor de Administração com acesso à Internet e, em seguida, configure os Servidores de Administração isolados.

Para configurar um Servidor de Administração com acesso à Internet:

1. Crie duas pastas em um disco onde o Servidor de Administração estiver instalado:

   - Pasta para a lista de atualizações necessárias
   - Pasta para patches

   É possível nomear essas pastas como quiser.

2. Conceda os direitos de acesso Modificar ao grupo KLAdmins nas pastas criadas por meio das ferramentas administrativas padrão do sistema operacional.

3. Use o utilitário klscflag para gravar os caminhos para as pastas nas propriedades do Servidor de Administração.

   Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

4. Digite os seguintes comandos no prompt de comando do Windows:

   - Para definir o caminho para a pasta de patches:
     `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v "<caminho para a pasta>"`
   - Para definir o caminho para a pasta para a lista de atualizações necessárias:
     `klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v "<caminho para a pasta>"`

   Exemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -ts -v "C:\<pasta para patches>"`

5. Se necessário, use o utilitário klscflag para especificar com que frequência o Servidor de Administração deve verificar novas solicitações de patch:
   `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v <valor em segundos>`

   O valor padrão é de 120 segundos.

   Exemplo: `klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PERIOD_SEC -t d -v 150`

6. Crie a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para obter informações sobre patches para o software de terceiros instalado nos dispositivos gerenciados e, em seguida, defina o agendamento da tarefa.

7. Crie a tarefa *Corrigir vulnerabilidades* para especificar patches para o software de terceiros usado para corrigir vulnerabilidades e, em seguida, defina o agendamento da tarefa.

   Execute a tarefa manualmente se desejar que ela seja executada antes do especificado no agendamento. A ordem em que as tarefas são iniciadas é importante. A tarefa *Corrigir vulnerabilidades* deve ser executada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

8. Reinicie o serviço do Servidor de Administração.

Agora, o Servidor de Administração com acesso à Internet está pronto para baixar e transmitir as atualizações para os Servidores de Administração isolados. Antes de começar a corrigir as vulnerabilidades, configurar os Servidores de Administração isolados.

Configuração de Servidores de Administração isolados para corrigir vulnerabilidades em uma rede isolada

Depois que terminar a configuração do Servidor de Administração com acesso à internet, prepare cada Servidor de Administração isolado em sua rede para que seja possível corrigir as vulnerabilidades e instalar as atualizações em dispositivos gerenciados conectados a Servidores de Administração isolados.

Para configurar os Servidores de Administração isolados, execute as seguintes ações em cada Servidor de Administração:

1. Ative uma chave de licença para o recurso Gerenciamento de patches e vulnerabilidades (VAPM).

2. Crie duas pastas em um disco onde o Servidor de Administração estiver instalado:

   - Pasta onde a lista de atualizações necessárias aparecerá
   - Pasta para patches

   É possível nomear essas pastas como quiser.

3. Conceda a permissão *Modificar* ao grupo KLAdmins nas pastas criadas por meio das ferramentas administrativas padrão do sistema operacional.

4. Use o utilitário klscflag para gravar os caminhos para as pastas nas propriedades do Servidor de Administração.

   Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

5. Digite os seguintes comandos no prompt de comando do Windows:

   - Para definir o caminho para a pasta de patches:
     `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v "<caminho da pasta>"`

   - Para definir o caminho para a pasta para a lista de atualizações necessárias:
     `klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v "<caminho para a pasta>"`

   Exemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -ts -v "C:\<pasta para patches>"`

6. Se necessário, use o utilitário klscflag para especificar com que frequência o Servidor de Administração isolado deve verificar novos patches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v <valor em segundos>`

   O valor padrão é de 120 segundos.

   Exemplo: `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PERIOD_SEC -t d -v 150`

7. Se necessário, use o utilitário klscflag para calcular os hashes SHA256 dos patches:
   `klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_VERIFY_HASH -t d -v 1`

   Se você digitar este comando, poderá certificar-se de que os patches não foram modificados durante a transferência para o Servidor de Administração isolado e que você recebeu os patches corretos contendo as atualizações necessárias.

   Por padrão, o Kaspersky Security Center não calcula os hashes SHA256 dos patches. Caso queira habilitar essa opção, depois que o Servidor de Administração isolado receber os patches, o Kaspersky Security Center calculará os hashes e comparará os valores adquiridos com os hashes armazenados no banco de dados do Servidor de Administração. Caso o hash calculado não corresponda ao hash no banco de dados, ocorrerá um erro e será necessário substituir os patches incorretos.

8. Crie a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para obter informações sobre patches para o software de terceiros instalado nos dispositivos gerenciados e, em seguida, defina o agendamento da tarefa.

9. Crie a tarefa *Corrigir vulnerabilidades* para especificar patches para o software de terceiros usado para corrigir vulnerabilidades e, em seguida, defina o agendamento da tarefa.

   Execute a tarefa manualmente se desejar que ela seja executada antes do especificado no agendamento. A ordem em que as tarefas são iniciadas é importante. A tarefa *Corrigir vulnerabilidades* deve ser executada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

10. Reinicie o serviço do Servidor de Administração.

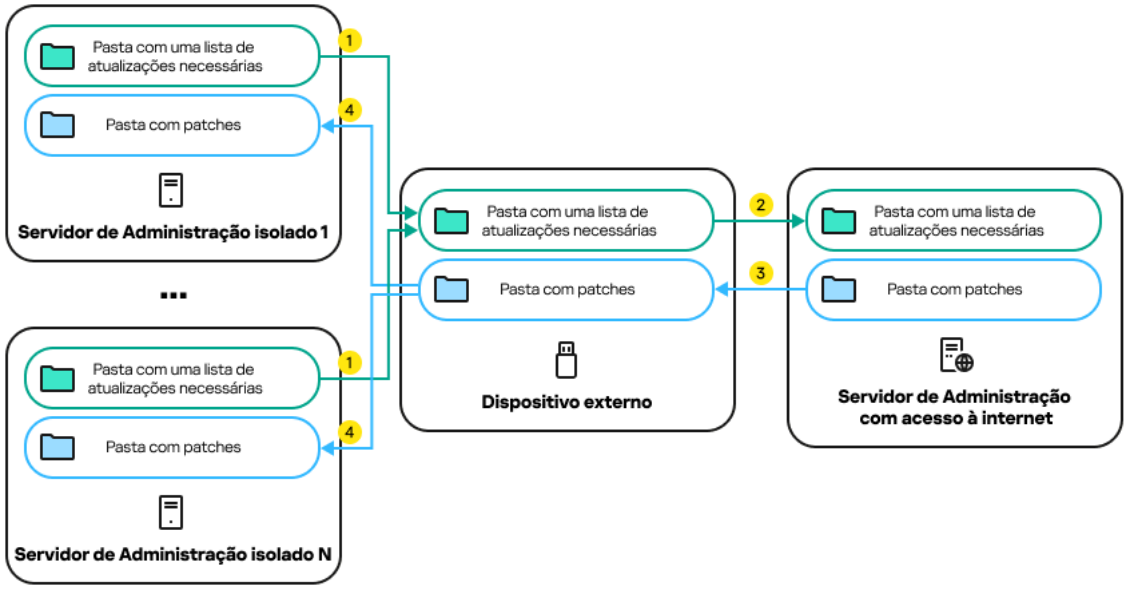
Após configurar todos os Servidores de Administração, será possível mover os patches e listas de atualizações necessárias e corrigir as vulnerabilidades de softwares de terceiros em dispositivos gerenciados na rede isolada.

Transmissão de patches e instalação de atualizações em uma rede isolada

Depois de ter terminado a configuração dos Servidores de Administração, é possível transferir os patches com as atualizações necessárias do Servidor de Administração com acesso à Internet para os Servidores de Administração isolados. É possível transmitir e instalar as atualizações sempre que precisar, por exemplo, uma ou várias vezes por dia.

É necessário um dispositivo externo, como uma unidade removível, para transferir os patches e a lista de atualizações entre os Servidores de Administração. Portanto, certifique-se de que o dispositivo externo tenha espaço em disco suficiente para baixar e armazenar patches.

O processo de transmissão de patches e a lista de atualizações necessárias é exibido na figura e descrito abaixo:



O processo de transmissão de patches e a lista de atualizações necessárias entre o Servidor de Administração com acesso à Internet e Servidores de Administração isolados

Para instalar as atualizações e corrigir as vulnerabilidades em dispositivos gerenciados conectados aos Servidores de Administração isolados:

1. Comece a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* se ainda não estiver em execução.

2. Conecte um dispositivo externo a qualquer Servidor de Administração isolado.

3. Crie duas pastas no dispositivo externo: uma para a lista de atualizações necessárias e outra para os patches. É possível nomear essas pastas como quiser.

   Caso tenha criado essas pastas anteriormente, basta limpá-las.

4. Copie a lista de atualizações necessárias de cada Servidor de Administração isolado e cole essa lista na pasta para a lista de atualizações necessárias no dispositivo externo.

   Como resultado, você une todas as listas adquiridas de todos os Servidores de Administração isolados em uma pasta. Essa pasta contém os arquivos binários com os IDs de patches necessários para todos os Servidores de Administração isolados.

5. Conecte o dispositivo externo ao Servidor de Administração com acesso à Internet.

6. Copie a lista de atualizações necessárias do dispositivo externo e cole essa lista na pasta da lista de atualizações necessárias no Servidor de Administração com acesso à Internet.

   Todos os patches necessários são baixados automaticamente da Internet para a pasta de patches no Servidor de Administração. Isso pode levar várias horas.

7. Certifique-se de que todos os patches necessários foram baixados. Nesse caso, é possível fazer o seguinte:

   - Verifique a pasta para os patches no Servidor de Administração com acesso à Internet. Todos os patches especificados na lista de atualizações necessárias devem ser baixados para a pasta necessária. Isso é mais conveniente caso seja necessário um pequeno número de patches.

   - Prepare um script especial, por exemplo, um script de shell. Caso obtenha um grande número de patches, será difícil verificar por conta própria se todos os patches foram baixados. Nesses casos, é melhor automatizar a verificação.

8. Copie os patches do Servidor de Administração com acesso à Internet e cole-os na pasta correspondente do dispositivo externo.

9. Transfira os patches para cada Servidor de Administração isolado. Coloque os patches em uma pasta específica para eles.

Como resultado, cada Servidor de Administração isolado cria uma lista real de atualizações necessárias para os dispositivos gerenciados conectados ao Servidor de Administração atual. Após o Servidor de Administração com acesso à Internet receber a lista de atualizações necessárias, o Servidor de Administração baixa os patches da Internet. Quando esses patches aparecem nos Servidores de Administração isolados, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* lidará com os patches. Assim, as atualizações são instaladas em dispositivos gerenciados e as vulnerabilidades de softwares de terceiros são corrigidas.

Quando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* estiver em execução, não reinicialize o dispositivo do Servidor de Administração e não execute a tarefa *Backup de dados do Servidor de Administração* (também causará uma reinicialização). Como resultado, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será interrompida e as atualizações não serão instaladas. Nesse caso, é preciso reiniciar essa tarefa manualmente ou aguardar o início da tarefa de acordo com o agendamento configurado.

Desativação da opção de transmissão de patches e instalação de atualizações em uma rede isolada

É possível desativar a transmissão de patches em Servidores de Administração isolados, por exemplo, caso decida retirar um ou mais Servidores de Administração de uma rede isolada. Assim, é possível reduzir o número de patches e o tempo para baixá-los.

Para desabilitar a opção de transmitir patches em Servidores de Administração isolados:

1. Caso queira tirar todos os Servidores de Administração do isolamento, nas propriedades do Servidor de Administração com acesso à Internet, exclua os caminhos para as pastas de patches e a lista de atualizações necessárias. Caso queira manter alguns Servidores de Administração em uma rede isolada, ignore essa etapa.

   Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Digite os seguintes comandos no prompt de comando:

   - Para excluir o caminho para a pasta de patches:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_EXPORT_PATH -t s -v ""
     ```
   - Para excluir o caminho para a pasta para obter a lista de atualizações necessárias:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_IMPORT_PATH -t s -v ""
     ```

2. Reinicie o serviço do Servidor de Administração caso tenha excluído os caminhos para as pastas nesse Servidor de Administração.

3. Nas propriedades de cada Servidor de Administração que deseja tirar do isolamento, exclua os caminhos para as pastas de patches e a lista de atualizações necessárias.

   Digite os seguintes comandos no prompt de comando do Windows, usando direitos de administrador:

   - Para excluir o caminho para a pasta de patches:
     ```
     klscflag -fset -pv klserver -n VAPM_DATA_IMPORT_PATH -t s -v ""
     ```
   - Para excluir o caminho para a pasta para obter a lista de atualizações necessárias:
     ```
     klscflag -fset -pv klserver -n VAPM_REQ_EXPORT_PATH -t s -v ""
     ```

4. Reinicie o serviço em cada Servidor de Administração no qual os caminhos para as pastas foram excluídos.

Como resultado, caso tenha reconfigurado o Servidor de Administração com acesso à Internet, os patches não serão mais recebidos por meio do Kaspersky Security Center. Caso tenha reconfigurado apenas alguns Servidores de Administração isolados, por exemplo, retirando alguns deles da rede isolada, os patches serão obtidos apenas para os Servidores de Administração isolados restantes.

Caso queira começar a corrigir as vulnerabilidades nos Servidores de Administração isolados desabilitados no futuro, será necessário configurar esses Servidores de Administração e o Servidor de Administração com acesso à internet outra vez.

Ignorar as vulnerabilidades de software

Você pode ignorar as vulnerabilidades do software a ser corrigidas. Os motivos para ignorar vulnerabilidades de software, por exemplo, os seguintes:

- A vulnerabilidade de software não é considerada crítica para sua organização.
- Você entende que a correção de vulnerabilidade do software pode danificar os dados relacionados ao software que exigia a correção da vulnerabilidade.
- Você tem certeza de que a vulnerabilidade do software não é perigosa para a rede da sua organização porque usa outras medidas para proteger seus dispositivos gerenciados.

Você pode ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

Para ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Vulnerabilidades de software**.

   O espaço de trabalho da pasta exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos pelo Agente de Rede instalado nos mesmos.

2. Selecione a vulnerabilidade que você deseja ignorar.

3. Selecione **Propriedades** no menu de contexto da vulnerabilidade.

   A janela Propriedades da vulnerabilidade é aberta.

4. Na seção **Geral**, selecione a caixa de seleção **Ignorar vulnerabilidade**.

5. Clique em **OK**.

   A janela de propriedades de vulnerabilidade do software está fechada.

A vulnerabilidade de software é ignorada em todos os dispositivos gerenciados.

Para ignorar uma vulnerabilidade de software no dispositivo gerenciado selecionado:

1. Abra a janela Propriedades do dispositivo gerenciado selecionado e selecione a seção **Vulnerabilidades de software**.

2. Selecione uma vulnerabilidade de software.

3. Ignore a vulnerabilidade selecionada.

A vulnerabilidade de software é ignorada no dispositivo selecionado.

A vulnerabilidade de software ignorada não será corrigida após a conclusão das tarefas *Corrigir vulnerabilidades* ou *Instalar as atualizações necessárias e corrigir vulnerabilidades*. É possível excluir as vulnerabilidades de software ignoradas na lista de vulnerabilidades por meio do filtro.

Selecionar as correções do usuário para vulnerabilidades em software de terceiros

Para usar a tarefa *Corrigir vulnerabilidades*, você deve especificar manualmente as atualizações de software para corrigir as vulnerabilidades em softwares de terceiros listadas nas configurações da tarefa. A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para outros softwares de terceiros. *Correções do usuário* são atualizações de software para corrigir as vulnerabilidade que o administrador especifica manualmente para instalação.

Para selecionar correções do usuário para vulnerabilidades em software de terceiros:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Vulnerabilidades de software**.

   O espaço de trabalho da pasta exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos pelo Agente de Rede instalado nos mesmos.

2. Selecione a vulnerabilidade para a qual deseja especificar uma correção do usuário.

3. Selecione **Propriedades** no menu de contexto da vulnerabilidade.

   A janela Propriedades da vulnerabilidade é aberta.

4. Na seção **Correções do usuário e outras correções**, clique no botão **Adicionar**.

   A lista de pacotes de instalação disponíveis é exibida. A lista de pacotes de instalação exibidos corresponde à lista **Instalação remota** → **Pacotes de instalação**. Se você não criou um pacote de instalação contendo a correção do usuário para a vulnerabilidade selecionada, poderá criar o pacote agora iniciando o Assistente de novo pacote.

5. Selecione um pacote de instalação (ou pacotes) que contenha uma correção (ou correções) do usuário para a vulnerabilidade no software de terceiros.

6. Clique em **OK**.

Os pacotes de instalação que contenham correções do usuário para a vulnerabilidade de software são especificados. Quando a tarefa *Corrigir vulnerabilidades* for iniciada, o pacote de instalação será instalado e a vulnerabilidade de software será corrigida.

Regras para instalação da atualização

Ao corrigir vulnerabilidades em aplicativos, você deve especificar regras para a instalação das atualizações. Essas regras determinam as atualizações a serem instaladas e as vulnerabilidades a serem corrigidas.

As configurações exatas dependem de você criar ou não uma regra para as atualizações de aplicativos da Microsoft, de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft), ou de todos os aplicativos. Ao criar uma regra para aplicativos da Microsoft ou aplicativos de terceiros você pode selecionar aplicativos específicos e versões de aplicativo específicas para os quais você deseja instalar atualizações. Ao criar uma regra para todos os aplicativos, você pode selecionar atualizações específicas que deseja instalar e vulnerabilidades que você deseja corrigir com a instalação de atualizações.

Para criar uma nova regra para as atualizações de todos os aplicativos:

1. Na página **Configurações** do Assistente para novas tarefas, clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Siga as etapas do Assistente.

2. Na página **Tipo de regra**, selecione **Regra para todas as atualizações**.

3. Na página **Critérios gerais**, use as listas suspensas para especificar as seguintes configurações:

- Conjunto de atualizações a instalar

  Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

  - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
  - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
  - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

- Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

  Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

  Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

  Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

  Por padrão, esta opção está desativada.

4. Na página **Atualizações**, selecione as atualizações a serem instaladas:

- **Instalar todas as atualizações adequadas**

  Instale todas as atualizações de software que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Instalar apenas as atualizações da lista**

  Instale somente as atualizações de software que você seleciona manualmente da lista. Essa lista contém todas as atualizações de software disponíveis.

  Por exemplo, pode ser necessário selecionar atualizações específicas nos seguintes casos: para verificar a instalação em um ambiente de teste, para atualizar somente aplicativos críticos ou para atualizar somente aplicativos específicos.

  - **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

    Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

    Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

    Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

    Por padrão, esta opção está ativada.

5. Na página **Vulnerabilidades**, selecione as vulnerabilidades que serão corrigidas instalando as atualizações selecionadas:

- **Corrigir todas as vulnerabilidades que correspondem a outros critérios**

  Corrija todas as vulnerabilidades que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Corrigir somente vulnerabilidades da lista**

  Corrija somente as vulnerabilidades que você seleciona manualmente da lista. Essa lista contém todas as vulnerabilidades detectadas.

  Por exemplo, pode ser necessário selecionar vulnerabilidades específicas nos seguintes casos: para verificar a correção em um ambiente de teste, para corrigir vulnerabilidades somente em aplicativos críticos ou para corrigir vulnerabilidades somente em aplicativos específicos.

6. Na página **Nome**, especifique o nome para a regra que você está criando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Após a conclusão da operação do Assistente de criação de regras, a nova regra será criada e exibida no campo **Especificar regras para a instalação de atualizações** do Assistente para novas tarefas.

Para criar uma nova regra para as atualizações dos aplicativos da Microsoft:

1. Na página **Configurações** do Assistente para novas tarefas, clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Siga as etapas do Assistente.

2. Na página **Tipo de regra**, selecione **Regra para o Windows Update**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

   - Corrigir vulnerabilidades com um nível de gravidade do MSRC igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Categorias de atualizações**, selecione as categorias das atualizações a serem instaladas. Essas categorias são iguais às no Catálogo do Microsoft Update. Por padrão, todas as categorias estão selecionadas.

6. Na página **Nome**, especifique o nome para a regra que você está criando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Após a conclusão da operação do Assistente de criação de regras, a nova regra será criada e exibida no campo **Especificar regras para a instalação de atualizações** do Assistente para novas tarefas.

Para criar uma nova regra para as atualizações de aplicativos de terceiros:

1. Na página **Configurações** do Assistente para novas tarefas, clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Siga as etapas do Assistente.

2. Na página **Tipo de regra**, selecione **Regra para atualizações de terceiros**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:
     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Nome**, especifique o nome para a regra que você está criando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Após a conclusão da operação do Assistente de criação de regras, a nova regra será criada e exibida no campo **Especificar regras para a instalação de atualizações** do Assistente para novas tarefas.

Grupos de aplicativos

Esta seção descreve como gerenciar grupos de aplicativos instalados nos dispositivos.

Criação de categorias de aplicativos

O Kaspersky Security Center permite criar categorias de aplicativos instalados nos dispositivos.

As categorias de aplicativo podem ser criadas de uma das seguintes formas:

- O administrador especifica uma pasta na qual arquivos executáveis foram incluídos na categoria selecionada.
- O administrador especifica um dispositivo a partir do qual os arquivos executáveis devem ser incluídos na categoria selecionada.
- O administrador define os critérios que devem ser usados para incluir aplicativos na categoria selecionada.

Quando a categoria de aplicativos estiver criada, o administrador poderá definir regras para a categoria de aplicativos. As regras definem o comportamento de aplicativos incluídos na categoria especificada. Por exemplo, você pode bloquear ou permitir a inicialização de aplicativos incluídos na categoria.

Gerenciar a execução de aplicativos em dispositivos

O Kaspersky Security Center permite gerenciar a inicialização de aplicativos nos dispositivos no modo lista de permissão. Para obter os detalhes consulte a Ajuda on-line do Kaspersky Endpoint Security for Windows. No modo de Lista de permissão, nos dispositivos cliente selecionados, você só pode inicializar aplicativos incluídos nas categorias especificadas. O administrador pode ver os resultados das análises estatísticas aplicadas às regras de execução de aplicativos nos dispositivos de cada usuário.

Inventário de software instalado nos dispositivos

O Kaspersky Security Center permite executar o inventário de software nos dispositivos executando o Windows e Linux. O Agente de Rede recupera as informações sobre todos os aplicativos instalados nos dispositivos. As informações recuperadas durante o inventário são exibidas no espaço de trabalho da pasta **Registro de aplicativos**. O administrador pode ver as informações detalhadas sobre qualquer aplicativo, incluindo sua versão e fabricante.

O número de arquivos executáveis recebidos de um único dispositivo não pode exceder 150.000. Tendo alcançado este limite, o Kaspersky Security Center não pode receber nenhum novo arquivo.

Gerenciamento do grupo de aplicativos licenciados

O Kaspersky Security Center permite a você criar grupos de aplicativos licenciados. Um grupo de aplicativos licenciados inclui aplicativos que atendem os critérios definidos pelo administrador. O administrador poderá especificar os seguintes critérios para os grupos de aplicativos licenciados:

- Nome do aplicativo
- Versão do aplicativo
- Fabricante
- Identificador do aplicativo

Os aplicativos que cumprem um ou vários critérios são automaticamente incluídos num grupo. Para criar um grupo de aplicativos licenciados, você deve configurar ao menos um critério para inclusão de aplicativos nesse grupo.

Cada grupo de aplicativos licenciados tem sua própria chave de licença. A chave de licença de um grupo de aplicativos licenciados define o número máximo permitido de instalações para aplicativos incluídos nesse grupo. Se o número de instalações tiver excedido o limite definido pela chave de licença, é registrado um evento informativo no Servidor de Administração. O administrador pode especificar uma data de expiração para a chave de licença. Quando chegar essa data, um evento informativo será registrado no Servidor de Administração.

Visualização de informações sobre arquivos executados

O Kaspersky Security Center recupera todas as informações sobre os arquivos executáveis que foram executados nos dispositivos desde a instalação do sistema operacional nos mesmos. As informações sobre os arquivos executáveis são exibidas na janela principal do aplicativo, no espaço de trabalho da pasta **Arquivos executáveis**.

Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos clientes

É possível obter a lista de arquivos executáveis armazenados em dispositivos clientes de uma das seguintes maneiras:

- Habilitar notificações sobre inicialização de aplicativos na política do Kaspersky Endpoint Security.
- Criar uma tarefa de inventário.

Ativar notificações sobre inicialização de aplicativos na política do Kaspersky Endpoint Security

Para habilitar notificações sobre a inicialização de aplicativos:

1. Abra as configurações da política do Kaspersky Endpoint Security e vá para **Configurações gerais** → **Relatórios e armazenamento**.
2. No grupo de configurações **Transferência de dados para o Servidor de Administração**, marque a caixa de seleção **Sobre aplicativos iniciados** e salve as alterações.

Quando um usuário tenta iniciar arquivos executáveis, informações sobre esses arquivos são adicionadas à lista de arquivos executáveis em um dispositivo cliente. O Kaspersky Endpoint Security envia essas informações ao Agente de Rede e, em seguida, o Agente de Rede as envia ao Servidor de Administração.

Criar uma tarefa de inventário

O recurso de inventário de arquivos executáveis está disponível para os seguintes aplicativos:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux versão 11.2 e posterior
- Kaspersky Security for Virtualization 4.0 Light Agent e versões posteriores

É possível reduzir a carga no banco de dados enquanto as informações sobre os aplicativos instalados são obtidas. Para economizar espaço, execute uma tarefa de inventário em dispositivos de referência nos quais um conjunto padrão de software está instalado. O número desejável de dispositivos é entre 1 e 3.

Não recomendamos executar a tarefa de inventário ao usar os seguintes bancos de dados: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (todas as edições).

Para criar uma tarefa de inventário para arquivos executáveis em dispositivos cliente:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. No espaço de trabalho da pasta **Tarefas**, clique no botão **Nova tarefa**.

   O Assistente para novas tarefas inicia.
3. Na janela **Selecionar o tipo de tarefa** do assistente, selecione **Kaspersky Endpoint Security** como o tipo de tarefa e, a seguir, selecione **Inventário** como o subtipo de tarefa e clique em **Avançar**.
4. Siga o restante das instruções do assistente.

   Após a conclusão do Assistente para novas tarefas, a tarefa **Inventário** será criada e configurada. Se desejar, você pode alterar as configurações da tarefa criada. A tarefa recém-criada é exibida na lista de tarefas. Se desejar, você pode alterar as configurações da tarefa criada.

Para uma descrição detalhada da tarefa de inventário, consulte as seguintes ajudas:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Após a tarefa **Inventário** ser executada, a lista de arquivos executáveis armazenados nos dispositivos gerenciados é formada e você pode visualizá-la.

Durante o inventário, arquivos executáveis nos seguintes formatos podem ser detectados (dependendo da opção selecionada nas propriedades da tarefa de inventário): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Visualizar a lista de arquivos executáveis armazenados nos dispositivos gerenciados

Para exibir a lista dos arquivos executáveis armazenados nos dispositivos clientes:

Na árvore do console, vá para **Avançado** → **Gerenciamento de aplicativos** → **Arquivos executáveis**.

Se necessário, é possível enviar um arquivo executável de um dispositivo gerenciado para o dispositivo com o Console de Administração instalado.

Para enviar um arquivo executável:

1. Na árvore do console, vá para **Avançado** → **Gerenciamento de aplicativos** → **Arquivos executáveis**.
2. Clicar no link do arquivo executável que deseja enviar para o dispositivo com o Console de Administração instalado.
3. Na janela que é aberta, vá para a seção **Dispositivos** e marque a caixa de seleção do dispositivo gerenciado do qual você deseja enviar o arquivo executável.

   Antes de enviar o arquivo executável, certifique-se de que o dispositivo gerenciado tenha uma conexão direta com o Servidor de Administração marcando a caixa de seleção **Não desconectar do Servidor de Administração**.

4. Clique no botão **Enviar**, selecione a pasta de destino e clique em **OK**.

   O arquivo executável selecionado é baixado para envio posterior ao dispositivo com o Console de Administração instalado.

Usar o Controle de Aplicativos para gerenciar arquivos executáveis

Você pode usar o componente Controle de Aplicativos para permitir ou bloquear a inicialização de arquivos executáveis nos dispositivos de usuário. O componente Controle de Aplicativos é compatível com sistemas operacionais baseados em Windows e Linux.

Para sistemas operacionais baseados em Linux, o componente Controle de Aplicativos está disponível no Kaspersky Endpoint Security 11.2 para Linux. O componente também está disponível para o Kaspersky Embedded Systems Security para Windows 3.0 ou posterior.

Pré-requisitos

- O Kaspersky Security Center está implementado em sua organização.
- A política do Kaspersky Endpoint Security for Windows ou do Kaspersky Endpoint Security for Linux está criada e ativa.

Fases

O cenário de uso do Controle de Aplicativos prossegue em fases:

1. **Formar e visualizar a lista de arquivos executáveis em dispositivos clientes**

   Esta etapa ajuda a descobrir quais arquivos executáveis são encontrados nos dispositivos gerenciados. Exiba a lista de arquivos executáveis e compare-a com a lista de arquivos executáveis permitidos e proibidos. As restrições sobre a utilização de arquivos executáveis podem estar relacionadas às políticas de segurança da informação em sua organização.

   Instruções de como proceder:

   - Console de administração: Inventário de arquivos executáveis
   - Kaspersky Security Center Web Console: Obtendo e visualizando uma lista de arquivos executáveis armazenados nos dispositivos cliente

2. **Criar categorias para arquivos executáveis usados em sua organização**

   Analise a lista de arquivos executáveis armazenados nos dispositivos gerenciados. Com base na análise, crie categorias para arquivos executáveis. É recomendável criar uma categoria "Aplicativos de trabalho" que cubra o conjunto padrão de arquivos executáveis usados na sua organização. Se diferentes grupos de segurança usarem seus próprios conjuntos de arquivos executáveis em seu trabalho, uma categoria poderá ser criada para cada grupo de segurança.

   Instruções de como proceder:

   - Console de Administração: Criação de uma categoria de aplicativo com conteúdo adicionado manualmente, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir de dispositivos selecionados, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir da pasta selecionada.
   - Kaspersky Security Center Web Console: Criação de uma categoria de aplicativo com conteúdo adicionado manualmente, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir de dispositivos selecionados, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir da pasta específica.

3. **Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security**

   Configure o componente Controle de Aplicativos na política do Kaspersky Endpoint Security usando as categorias criadas no estágio anterior.

   Instruções de como proceder:

   - Console de Administração: Configurar o gerenciamento da inicialização do aplicativo em dispositivos cliente
   - Kaspersky Security Center Web Console: Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows

4. **Ativar o componente Controle de Aplicativos no modo de teste**

   Para garantir que as regras do Controle de Aplicativos não bloqueiem os arquivos executáveis necessários para o trabalho do usuário, é recomendável ativar o teste das regras do Controle de Aplicativos e analisar a sua operação após a criação de novas regras. Quando o teste está ativado, o Kaspersky Endpoint Security for Windows não bloqueia os arquivos executáveis cuja inicialização é proibida pelas regras do Controle de Aplicativos, mas envia notificações sobre a inicialização ao Servidor de Administração.

   Ao testar as regras do Controle de Aplicativos, é recomendável realizar as seguintes ações:

   - Determine o período de teste. O período de teste pode variar de vários dias a dois meses.
   - Examine os eventos resultantes do teste da operação do Controle de Aplicativos.

   Instruções para o Kaspersky Security Center Web Console: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e ative a opção **Modo de teste** no processo de configuração.

5. **Alteração das configurações de categorias do componente Controle de Aplicativos**

   Se necessário, faça alterações nas configurações do Controle de Aplicativos. Com base nos resultados do teste, você pode adicionar arquivos executáveis relativos a eventos do componente Controle de Aplicativos a uma categoria com conteúdo adicionado manualmente.

   Instruções de como proceder:

   - Console de Administração: Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos
   - Kaspersky Security Center Web Console: Adicionar arquivos executáveis relacionados a eventos à categoria de aplicativo

6. **Aplicar as regras do Controle de Aplicativos no modo de operação**

   Após as regras de Controle de Aplicativos terem sido testadas e a configuração das categorias estar concluída, você pode aplicar as regras do Controle de Aplicativos no modo de operação.

   Instruções para o Kaspersky Security Center Web Console: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e desative a opção **Modo de teste** no processo de configuração.

7. **Verificar a configuração do Controle de Aplicativos**

   Certifique-se de ter feito o seguinte:

   - Categorias criadas para arquivos executáveis.
   - Configurado o Controle de Aplicativos usando as categorias.
   - Aplicado as regras do Controle de Aplicativos no modo de operação.

Resultados

Quando o cenário estiver concluído, a inicialização dos arquivos executáveis nos dispositivos gerenciados será controlada. Os usuários podem executar apenas aqueles arquivos executáveis permitidos na sua organização e não podem executar arquivos executáveis proibidos na sua organização.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ajuda do Kaspersky Embedded Systems Security for Windows
- Ajuda do Kaspersky Embedded Systems Security for Linux

Criar categorias de aplicativos para as políticas do Kaspersky Endpoint Security for Windows

Você pode criar categorias de aplicativos para políticas do Kaspersky Endpoint Security for Windows a partir da pasta **Categorias de aplicativos** e da janela **Propriedades** de uma política do Kaspersky Endpoint Security for Windows.

*Para criar uma categoria de aplicativo para uma política do Kaspersky Endpoint Security a partir da pasta **Categorias de aplicativos**:*

1. Na árvore do console, selecione **Avançado** → **Gerenciamento de aplicativos** → **Categorias de aplicativos**.
2. No espaço de trabalho da pasta **Categorias de aplicativos**, clique no botão **Nova categoria**.

   O Assistente para novas categorias é iniciado.
3. Na página **Tipo de categoria**, selecione o tipo de categoria de usuário:

   - **Categoria com conteúdo adicionado manualmente**. Especifique os critérios que serão usados para atribuir arquivos executáveis à categoria que está sendo criada.
   - **Categoria que inclui os arquivos executáveis dos dispositivos selecionados**. Especifique um dispositivo cujos arquivos executáveis devem ser automaticamente atribuídos à categoria.
   - **Categoria que inclui os arquivos executáveis de uma pasta específica**. Especifique um dispositivo cujos arquivos executáveis devem ser atribuídos automaticamente à categoria.
4. Siga as instruções do Assistente.

Quando o assistente é finalizado, uma categoria de aplicativo personalizada é criada. Você pode visualizar as categorias recém criadas usando a lista de categorias no espaço de trabalho da pasta **Categorias de aplicativos**.

Caso queira exportar uma categoria de aplicativo para um arquivo KLC, clique com o botão direito do mouse no nome da categoria, selecione **Exportar** no menu e, na janela aberta, especifique o nome do arquivo e clique em **Salvar**.

Você também pode criar uma categoria de aplicativos a partir da pasta **Políticas**.

*Para criar uma categoria de aplicativo a partir da janela **Propriedades** de uma política do Kaspersky Endpoint Security for Windows:*

1. Na árvore do console, selecione a pasta **Políticas**.
2. No espaço de trabalho da pasta **Políticas**, selecione uma política do Kaspersky Endpoint Security para a qual você quer criar uma categoria.
3. Clique com o botão direito e selecione **Propriedades**.
4. Na janela de **propriedades** que se abre, no painel esquerdo **Seções**, selecione **Controles de Segurança** → **Controle de Aplicativos**.
5. Na seção **Controle de Aplicativos**, nas listas suspensas **Modo de controle** e **Ação**, marque para lista de permissão ou lista de bloqueio e clique no botão **Adicionar**.

   A janela **Regra de Controle de Aplicativos** contendo uma lista de categorias será aberta.
6. Clique no botão **Criar nova**.
7. Digite o nome da nova categoria e clique em **OK**.

   O Assistente para novas categorias inicia.

8. Na página **Tipo de categoria**, selecione o tipo de categoria de usuário:

   - **Categoria com conteúdo adicionado manualmente**. Especifique os critérios que serão usados para atribuir arquivos executáveis à categoria que está sendo criada.
   - **Categoria que inclui os arquivos executáveis dos dispositivos selecionados**. Especifique um dispositivo cujos arquivos executáveis devem ser automaticamente atribuídos à categoria.
   - **Categoria que inclui os arquivos executáveis de uma pasta específica**. Especifique um dispositivo cujos arquivos executáveis devem ser atribuídos automaticamente à categoria.

9. Siga as instruções do Assistente.

   Quando o assistente é finalizado, uma categoria de aplicativo personalizada é criada. Você poderá visualizar categorias recém-criadas na lista de categorias.

As categorias de aplicativo são usadas pelo componente Controle de Aplicativos incluído no Kaspersky Endpoint Security for Windows. O Controle de Aplicativos permite ao administrador impor restrições na inicialização de aplicativos em dispositivos cliente – por exemplo, restringindo a inicialização de aplicativos em uma categoria especificada.

Criar uma categoria de aplicativos com conteúdo adicionado manualmente

Você pode especificar um conjunto de critérios como um modelo de arquivos executáveis cuja inicialização deseja permitir ou bloquear na sua organização. Com base nos arquivos executáveis correspondentes aos critérios, você poderá criar uma categoria de aplicativos e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria de aplicativos com conteúdo adicionado manualmente:

1. Na árvore do console, na pasta **Avançado → Gerenciamento de aplicativos** selecione a subpasta **Categorias de aplicativos**.
2. Clique no botão **Nova categoria**.

   O **Assistente para novas categorias** inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na página do assistente **Tipo de categoria**, selecione **Categoria com o conteúdo adicionado manualmente** como o tipo de categoria de usuário.
4. No assistente da página **Inserir o nome da categoria de aplicativos**, insira o novo nome da categoria de aplicativo.
5. Na página **Configurando condições para inclusão de aplicativos em categorias**, clique no botão **Adicionar**.

6. Na lista suspensa, especifique as configurações relevantes:

- **Da lista de arquivos executáveis**

  Se esta opção estiver selecionada, você poderá utilizar a lista de arquivos executáveis no dispositivo cliente para selecionar e adicionar aplicativos deles à categoria.

- **Das propriedades do arquivo**

  Se esta opção estiver selecionada, você poderá especificar os dados detalhados para os arquivos executáveis que serão adicionados à categoria de aplicativos do usuário.

- **Metadados a partir de arquivos na pasta**

  Especifique uma pasta no dispositivo cliente que contém arquivos executáveis. Os metadados nos arquivos executáveis na pasta especificada serão transferidos para o Servidor de Administração. Os arquivos executáveis que contenham os mesmos metadados serão adicionados à categoria de aplicativos do usuário.

- **Checksums dos arquivos na pasta**

  Se esta opção estiver selecionada, você poderá selecionar ou criar uma pasta no dispositivo cliente. O hash MD5 de arquivos na pasta especificada será enviado para o Servidor de Administração. Os aplicativos que tenham o mesmo hash que os dos arquivos na pasta especificada são adicionados à categoria de aplicativos do usuário.

- **Certificados para arquivos da pasta**

  Se esta opção estiver selecionada, você poderá especificar a pasta no dispositivo cliente que contenha arquivos executáveis assinados com certificados. Certificados de arquivos executáveis são lidos e adicionados às condições da categoria. Arquivos executáveis que tenham sido assinados de acordo com os certificados especificados serão adicionados à categoria de usuário.

- **Metadados dos arquivos do instalador MSI**

  Se esta opção estiver selecionada, você poderá especificar um arquivo de instalador MSI como a condição para adicionar aplicativos à categoria de usuário. Os metadados do instalador do aplicativo serão enviados ao Servidor de Administração. Os aplicativos para os quais o instalador de metadados for o mesmo para o instalador MSI especificado, são adicionados à categoria de aplicativos do usuário.

- **Checksums dos arquivos do instalador MSI do aplicativo**

  Se esta opção estiver selecionada, você poderá especificar um arquivo de instalador MSI como a condição para adicionar aplicativos à categoria de usuário. O hash do instalador do aplicativo será enviados ao Servidor de Administração. Os aplicativos para os quais o hash do instalador MSI for idêntico ao hash especificado são adicionados à categoria de aplicativo do usuário.

- **Da categoria KL**

Se esta opção estiver selecionada, você poderá especificar uma categoria de aplicativos da Kaspersky como a condição para adicionar aplicativos da categoria do usuário. Os aplicativos da categoria da Kaspersky especificada serão adicionados à categoria de aplicativos do usuário.

- **Especificar caminho para o aplicativo (máscaras aceitas)**

  Se esta opção estiver selecionada, você pode especificar o caminho para a pasta no dispositivo cliente contendo os arquivos executáveis a serem adicionados à categoria de aplicativos do usuário. Você pode usar expressões regulares como *C:\path_to_exe**, por exemplo: *C:\Program Files\Internet Explorer**.

- **Selecionar certificado do repositório**

  Se esta opção estiver selecionada, você pode especificar certificados do armazenamento. A condição de categoria só se relaciona com os arquivos executáveis assinados pelo certificado definido.

- **Tipo de unidade**

  Se esta opção estiver selecionada, você pode especificar o tipo de mídia (qualquer unidade ou unidade removível) no qual o aplicativo será executado. Os aplicativos que foram executados no tipo de unidade selecionado são adicionados à categoria de aplicativo do usuário.

7. Na página do assistente **Criando a categoria de aplicativos**, clique no botão **Concluir**.

O Kaspersky Security Center só trata metadados de arquivos digitalmente assinados. Nenhuma categoria pode ser criada com base nos metadados de arquivos que não contêm uma assinatura digital.

Quando o assistente for concluído, uma categoria de aplicativo do usuário é criada, com o conteúdo adicionado manualmente. Você pode visualizar a categoria recém criada usando a lista de categorias no espaço de trabalho da pasta **Categorias de aplicativos**.

Caso queira exportar uma categoria de aplicativo para um arquivo KLC, clique com o botão direito do mouse no nome da categoria, selecione **Exportar** no menu e, na janela aberta, especifique o nome do arquivo e clique em **Salvar**.

Criar uma categoria de aplicativo que inclua arquivos executáveis dos dispositivos selecionados

Você pode usar arquivos executáveis de dispositivos selecionados como um modelo de arquivos executáveis que deseja permitir ou bloquear. Com base nos arquivos executáveis dos dispositivos selecionados, você pode criar uma categoria de aplicativo e usá-la na configuração do componente Controle de Aplicativos.

Para recuperar a lista de arquivos executáveis de dispositivos:

1. Certifique-se de que a política do Kaspersky Endpoint Security for Windows ou do Kaspersky Endpoint Security for Linux foi criada e está ativa. Ative o componente Controle de Aplicativos na política.

2. Obtenha uma lista de arquivos executáveis armazenados nos dispositivos cliente.

Para criar uma categoria de aplicativo que inclui arquivos executáveis de dispositivos selecionados:

1. Na árvore do console, na pasta **Avançado** → **Gerenciamento de aplicativos** selecione a subpasta **Categorias de aplicativos**.

2. Clique no botão **Nova categoria**.

   O **Assistente para novas categorias** inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na página do assistente **Tipo de categoria**, selecione **Categoria que inclui arquivos executáveis de dispositivos selecionados** como o tipo de categoria de usuário.

4. No assistente da página **Inserir o nome da categoria de aplicativos**, insira o novo nome da categoria de aplicativo.

5. Na página do assistente **Configurações**, clique no botão **Adicionar**.

6. Selecione um ou mais dispositivos cujos arquivos executáveis serão usados para criar a categoria de aplicativos.

7. Especificar as seguintes configurações:

- **Algoritmo de cálculo do valor hash**

  Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é necessário selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center de arquivos nessa categoria. As informações de valores de hash calculados por funções de hash são armazenadas no banco de dados do Servidor de Administração.

  SHA256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

  Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center de arquivos na categoria:

  - Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.

  - Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA256 hash criptográfica para arquivos da categoria.

  Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

  A caixa de seleção **Calcular SHA256 para arquivos nesta categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e quaisquer versões posteriores)** está marcada por padrão.

  A caixa de seleção **Calcular o MD5 para os arquivos nesta categoria (suportado pelas versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** é selecionado por padrão.

- **Sincronizar dados com o repositório do Servidor de Administração**

  Selecione esta opção se você desejar que o Servidor de Administração verifique periodicamente as alterações na pasta (ou pastas) especificada.

  Por padrão, esta opção está desativada.

  Se você ativar esta opção, especifique o período (em horas) para verificar as alterações nas pastas especificadas. Por padrão, o intervalo de verificação é de 24 horas.

8. No assistente da página **Filtro**, especifique as seguintes configurações:

   - Tipo de arquivo

     Nesta seção, você pode especificar o tipo de arquivo usado para criar a categoria de aplicativo.

     Todos os arquivos. Todos os arquivos são levados em consideração durante a criação da categoria. Por padrão, esta opção está selecionada.

     Somente arquivos fora das categorias de aplicativos. Somente arquivos fora das categorias de aplicativos são levados em consideração durante a criação da categoria.

   - Pastas

     Nesta seção, você pode especificar quais pastas dos dispositivos selecionados contendo arquivos usados para criar a categoria de aplicativos.

     Todas as pastas. Todas as pastas são levadas em consideração para a categoria de criação. Por padrão, esta opção está selecionada.

     Pasta especificada. Somente a pasta especificada é levada em consideração para a categoria de criação. Se você selecionar esta opção, deverá especificar o caminho para a pasta.

9. Na página do assistente **Criando a categoria de aplicativos**, clique no botão **Concluir**.

   Quando o assistente é finalizado, uma categoria de aplicativo de usuário é criada. Você pode visualizar a categoria recém criada usando a lista de categorias no espaço de trabalho da pasta **Categorias de aplicativos**.

Caso queira exportar uma categoria de aplicativo para um arquivo KLC, clique com o botão direito do mouse no nome da categoria, selecione **Exportar** no menu e, na janela aberta, especifique o nome do arquivo e clique em **Salvar**.

Criar uma categoria de aplicativo que inclua arquivos executáveis de uma pasta específica

Você pode usar arquivos executáveis da pasta selecionada como um padrão de arquivos executáveis que deseja permitir ou bloquear. Com base nos arquivos executáveis da pasta selecionada, você poderá criar uma categoria de aplicativos e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria de aplicativo que inclui arquivos executáveis de uma pasta específica:

1. Na árvore do console, na pasta **Avançado** → **Gerenciamento de aplicativos** selecione a subpasta **Categorias de aplicativos**.

2. Clique no botão **Nova categoria**.

   O **Assistente para novas categorias** inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na página do assistente **Tipo de categoria**, selecione **Categoria que inclui arquivos executáveis de uma pasta específica** como o tipo de categoria de usuário.

4. No assistente da página **Inserir o nome da categoria de aplicativos**, insira o novo nome da categoria de aplicativo.

5. Na página do assistente **Pasta do repositório**, clique no botão **Procurar**.

6. Especifique a pasta cujos arquivos executáveis serão usados para criar a categoria do aplicativo.

7. Defina as seguintes configurações:

- **Incluir bibliotecas de link dinâmico (DLL) nessa categoria**

  A categoria de aplicativo inclui bibliotecas de link dinâmico (arquivos no formato de DLL), e o componente Controle de Aplicativos registra as ações de tais bibliotecas que ocorrem no sistema. A inclusão de arquivos DLL na categoria pode abaixar o desempenho do Kaspersky Security Center.

  Por padrão, esta caixa de seleção está desmarcada.

- **Incluir dados de script nesta categoria**

  A categoria do aplicativo inclui dados sobre scripts, e os scripts não são bloqueados pelo Proteção Contra Ameaças da Web. Incluir os dados de script na categoria pode diminuir o desempenho do Kaspersky Security Center.

  Por padrão, esta caixa de seleção está desmarcada.

- **Algoritmo de cálculo de valor hash**: **Calcular o SHA-256 para arquivos nessa categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores)/Calcular o MD5 para os arquivos nesta categoria (compatível com versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é necessário selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center de arquivos nessa categoria. As informações de valores de hash calculados por funções de hash são armazenadas no banco de dados do Servidor de Administração.

SHA256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center de arquivos na categoria:

- Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.

- Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA256 hash criptográfica para arquivos da categoria.

Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

A caixa de seleção **Calcular SHA256 para arquivos nesta categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e quaisquer versões posteriores)** está marcada por padrão.

A caixa de seleção **Calcular o MD5 para os arquivos nesta categoria (suportado pelas versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** é selecionado por padrão.

- Forçar verificação da pasta para procurar alterações

Se esta opção estiver ativada, o aplicativo verifica regularmente a pasta de inclusão de conteúdo à categoria, buscando por alterações. Você pode especificar a frequência de verificações (em horas) no campo de entrada próximo da caixa de seleção. Por padrão, o tempo de intervalo entre verificações forçadas é de 24 horas.

Se esta opção estiver ativada, o aplicativo não força nenhuma verificação da pasta. O Servidor tenta acessar arquivos se eles tiverem sido modificados, adicionados ou excluídos.

Por padrão, esta opção está desativada.

8. Na página do assistente **Criando a categoria de aplicativos**, clique no botão **Concluir**.

Quando o assistente é finalizado, uma categoria de aplicativo de usuário é criada. Você pode visualizar a categoria recém criada usando a lista de categorias no espaço de trabalho da pasta **Categorias de aplicativos**.

Caso queira exportar uma categoria de aplicativo para um arquivo KLC, clique com o botão direito do mouse no nome da categoria, selecione **Exportar** no menu e, na janela aberta, especifique o nome do arquivo e clique em **Salvar**.

Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos

Você pode adicionar arquivos executáveis relativos aos eventos **Inicialização do aplicativo proibida** e **Inicialização do aplicativo proibida no modo de teste** para uma categoria de aplicativos existente com conteúdo adicionado manualmente ou para uma nova categoria de aplicativos.

Para adicionar arquivos executáveis relativos aos eventos de Controle de Aplicativos para a categoria de aplicativos:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Na guia **Eventos**, selecione os eventos necessários.
4. No menu de contexto de um dos eventos selecionados, selecione **Adicionar à categoria**.

5. Na janela **Ação em arquivo executável relacionado ao evento** que for aberta, especifique as configurações relevantes:

   Selecione um dos seguintes:

   - **Adicionar a uma nova categoria de aplicativos**

     Selecione esta opção se você tiver de criar uma nova categoria de aplicativo.

     Clique no botão **OK** para executar o Assistente para novas categorias. Quando o assistente for concluído, a categoria com as configurações especificadas será criada.

     Por padrão, esta opção não está selecionada.

   - **Adicionar a uma categoria de aplicativos existente**

     Selecione esta opção se você tiver de adicionar regras a uma categoria de aplicativo existente. Selecione a categoria relevante na lista de categorias de aplicativo.

     Esta opção está marcada por padrão.

   Na seção **Tipo de regra**, selecione uma das seguintes configurações:

   - **Adicionar a categoria**

     Selecione esta opção se você tiver de adicionar regras às condições da categoria de aplicativo.

     Esta opção está marcada por padrão.

   - **Regras para adicionar às exclusões**

     Selecione esta opção se você tiver de adicionar regras às exclusões da categoria de aplicativo.

   Na seção **Tipo de informação de arquivo**, selecione uma das seguintes configurações:

   - **Detalhes do certificado (ou hashes SHA256 para arquivos sem certificado)**

     Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

     Cada arquivo tem a sua própria função SHA256 hash única. Quando você seleciona uma função SHA256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

     Selecione esta opção se você quiser adicionar às regras de categoria os detalhes do certificado de um arquivo executável (ou a função SHA256 hash de arquivos sem um certificado).

     Por padrão, esta opção está selecionada.

   - **Detalhes do certificado (arquivos sem certificado serão ignorados)**

Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

Selecione esta opção se você quiser adicionar os detalhes do certificado de um arquivo executável às regras de categoria. Se o arquivo executável não tiver um certificado, este arquivo será ignorado. Nenhuma informação sobre este arquivo será adicionada à categoria.

- **Somente SHA256 (arquivos sem hash serão ignorados)**

  Cada arquivo tem a sua própria função SHA256 hash única. Quando você seleciona uma função SHA256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

  Selecione esta opção se você quiser adicionar somente os detalhes da função SHA256 hash do arquivo executável.

- **MD5 (modo descontinuado, somente para a versão Kaspersky Endpoint Security 10 Service Pack 1)**

  Cada arquivo tem a sua própria função MD5 hash única. Quando você seleciona uma função MD5 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

  Selecione esta opção se você quiser adicionar somente os detalhes da função MD5 hash do arquivo executável. O cálculo função MD5 hash é suportado por versões do Service Pack 1 do Kaspersky Endpoint Security 10 for Windows e posteriores.

6. Clique em **OK**.

Configurar o gerenciamento da inicialização do aplicativo em dispositivos cliente

A categorização de aplicativos permite otimizar o gerenciamento de execuções de aplicativo nos dispositivos. Você pode criar uma categoria de aplicativo e configurar o Controle de Aplicativos para uma política para que somente os aplicativos da categoria especificada serão iniciados nos dispositivos aos quais aquela política está aplicada. Por exemplo, você criou uma categoria que inclui aplicativos denominados *Application_1* e *Application_2*. Após você adicionar esta categoria a uma política, somente dois aplicativos têm permissão para ser iniciados nos dispositivos aos quais aquela política é aplicada: *Application_1* e *Application_2*. Se um usuário tentar iniciar um aplicativo que não foi incluído naquela categoria, por exemplo, *Application_3*, este aplicativo é bloqueado quanto a ser iniciado. Ao usuário é mostrado uma notificação indicando que *Application_3* tem sua inicialização bloqueada, de acordo com a uma regra de Controle de Aplicativos. Você pode criar uma categoria com o conteúdo adicionado automaticamente com base em diversos critérios de uma pasta específica. Neste caso, os arquivos são automaticamente adicionados à categoria da pasta especificada. Os arquivos executáveis de aplicativos são copiados à pasta especificada e processados automaticamente; sua métrica é adicionada à categoria.

Para configurar o gerenciamento da execução de aplicativos nos dispositivos clientes:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Categorias de aplicativos**.

2. No espaço de trabalho da pasta **Categorias de aplicativos**, crie uma categoria de aplicativos que você deseja gerenciar durante a inicialização.

3. Na pasta **Dispositivos gerenciados**, na guia **Políticas**, clique no botão **Nova política** para criar uma nova política para o Kaspersky Endpoint Security for Windows e siga as instruções do assistente.

   Se essa política já existir, você pode ignorar esta etapa. Você pode configurar o gerenciamento da inicialização de aplicativos em uma categoria especificada através das configurações desta política. A nova política criada é exibida na pasta **Dispositivos gerenciados** na guia **Políticas**.

4. Selecione **Propriedades** no menu de contexto da política para o Kaspersky Endpoint Security for Windows.

   A janela Propriedades da política para o Kaspersky Endpoint Security for Windows será aberta.

5. Na janela de propriedades da política do Kaspersky Endpoint Security for Windows, na seção **Controles de Segurança → Controle de Aplicativos**, marque a caixa de seleção **Controle de Aplicativos**.

6. Clique no botão **Adicionar**.

   A janela **Regra de Controle de Aplicativos** abre.

7. Na janela **Regra de Controle de Aplicativos**, na lista suspensa **Categoria** selecione a categoria de aplicativos que a regra de inicialização abrangerá. Configure a regra de inicialização para a categoria de aplicativos selecionada.

   Para o Kaspersky Endpoint Security 10 Service Pack 2 e posterior, nenhuma categoria é exibida se elas foram criadas sobre o critério do hash MD5 de um arquivo executável.

   Não recomendamos adicionar categorias criadas de acordo com o critério do hash SHA256 de um arquivo executável para versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2. Isto pode resultar em falhas do aplicativo.

   As instruções detalhadas sobre a configuração de regras de controle são fornecidas na Ajuda on-line do Kaspersky Endpoint Security for Windows.

8. Clique em **OK**.

Os aplicativos serão executados nos dispositivos incluídos na categoria especificada de acordo com a regra que você criou. A regra recentemente criada é exibida na janela Propriedades da política do Kaspersky Endpoint Security for Windows, na seção **Controle de Aplicativos**.

Visualização dos resultados da análise estática das regras de inicialização aplicadas a arquivos executáveis

Pra ver informações sobre que arquivos executáveis os usuários estão proibidos de executar:

1. Na pasta **Dispositivos gerenciados** na árvore do console, selecione a guia **Políticas**.

2. Selecione **Propriedades** no menu de contexto da política para o Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política de aplicativos é aberta.

3. No painel **Seções**, selecione **Controles de segurança** e, a seguir, selecione a subseção **Controle de Aplicativos**.

4. Clique no botão **Análise estática**.

   A janela **Análise da lista de direitos de acesso** se abre. Na parte esquerda da janela, é exibida uma lista de usuários com base nos dados do Active Directory.

5. Selecione um usuário da lista.

   A parte direita da janela exibe categorias de aplicativos atribuídas a este usuário.

6. Para visualizar os arquivos executáveis que o usuário está proibido de executar, na janela **Análise da lista de direitos de acesso** clique no botão **Visualizar arquivos**.

   Uma janela é aberta, exibindo uma lista de arquivos executáveis proibidos.

7. Para visualizar uma lista de arquivos executáveis incluídos em uma categoria, selecione uma categoria de aplicativos e clique no botão **Exibir arquivos na categoria**.

   Uma janela é aberta, exibindo uma lista de arquivos executáveis incluídos na categoria de aplicativos.

Visualização do registro de aplicativos

O Kaspersky Security Center executa um inventário de todos os softwares instalados nos dispositivos gerenciados.

O Agente de Rede compila uma lista de aplicativos instalados em um dispositivo Windows ou Linux e, então, transmite essa lista para o Servidor de Administração. Para dispositivos clientes baseados no Windows, o Agente de Rede recebe a maioria das informações sobre os aplicativos instalados do registro do Windows. Para dispositivos clientes baseados em Linux, os gerenciadores de pacotes fornecem ao Agente de Rede informações sobre os aplicativos instalados.

Para exibir o registro de aplicativos instalados nos dispositivos cliente,

Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Registro de aplicativos**.

O espaço de trabalho da pasta **Registro de aplicativos** exibe uma lista de aplicativos que foram instalados nos dispositivos cliente e no Servidor de Administração.

Você pode exibir os detalhes de qualquer aplicativo abrindo o seu menu de contexto e selecionando **Propriedades**. A janela Propriedades do aplicativo exibe os detalhes do aplicativo e informações sobre seus arquivos executáveis, assim como uma lista de dispositivos nos quais o aplicativo está instalado.

No menu de contexto de qualquer aplicativo na lista, você pode:

- Adicionar este aplicativo em uma categoria de aplicativos.
- Atribua uma tag ao aplicativo.
- Exportar a lista de aplicativos instalados no dispositivo para um arquivo CSV ou um arquivo TXT.
- Exiba as propriedades do aplicativo, por exemplo, nome do fornecedor, número da versão, lista de arquivos executáveis, lista de dispositivos nos quais o aplicativo está instalado, lista das atualizações do software disponíveis ou a lista de vulnerabilidades do software detectadas.

Para visualizar aplicativos que atendem aos critérios especificados, você pode usar os campos de filtragem no espaço de trabalho da pasta **Registro de aplicativos**.

Na janela de propriedades do dispositivo selecionado, na seção **Registro de aplicativos** você pode exibir a lista dos aplicativos instalados no dispositivos.

Gerar um relatório sobre os aplicativos instalados

No espaço de ytabalho **Registro de aplicativos**, você também pode clicar no botão **Visualizar o relatório de os aplicativos instalados**, para gerar um relatório contendo estatísticas detalhadas sobre os aplicativos instalados, incluindo o número de dispositivos nos quais cada aplicativo está instalado. Esse relatório que é aberto na página **Relatório dobre os aplicativos instalados**, contém informações sobre os aplicativos Kaspersky e de software de terceiros. Se você deseja obter informações somente sobre os aplicativos Kaspersky instalados nos dispositivos cliente, na lista **Resumo**, selecione AO Kaspersky Lab.

As informações sobre os aplicativos Kaspersky e de terceiros instalados em dispositivos cliente que estejam conectados com os Servidores de Administração secundários e virtuais também são armazenadas no registro de aplicativos do Servidor de Administração principal. Após você ter adicionado os dados dos Servidores de Administração secundários e virtuais, clique no botão **Visualizar o relatório de os aplicativos instalados** e na página **Relatório de aplicativos instalados** aberta, você poderá visualizar estas informações.

Para adicionar informações de Servidores de Administração secundários e virtuais no relatório sobre aplicativos instalados:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Na guia **Relatórios**, selecione **Relatório de aplicativos instalados**.
4. Selecione **Propriedades** no menu de contexto do relatório.

   A janela **Propriedades: Relatório de aplicativos instalados** é aberta.
5. Na seção **Hierarquia de Servidores de Administração**, selecione a caixa de seleção **Incluir dados dos Servidores de Administração secundários e virtuais**.
6. Clique em **OK**.

   As informações dos Servidores de Administração secundários e virtuais serão incluídas no **Relatório de aplicativos instalados**.

Alterar o horário de início do inventário de software

O Kaspersky Security Center executa um inventário de todos os softwares instalados nos dispositivos cliente gerenciados que executam o Windows.

O Agente de Rede compila uma lista de aplicativos instalados em um dispositivo cliente e, a seguir, transmite esta lista para o Servidor de Administração. O Agente de Rede recebe automaticamente as informações sobre os aplicativos instalados do registro do Windows.

Para economizar recursos do dispositivo, o Agente de Rede por padrão começa a receber informações sobre os aplicativos instalados a cada 10 minutos após o início do Agente de Rede.

Para alterar a hora de início do inventário de software, que decorre após a execução do serviço de Agente de Rede em um dispositivo:

1. Abra o registro do sistema do dispositivo cliente no qual o Agente de Rede está instalado (por exemplo, localmente usando o comando regedit no menu **Iniciar** → **Executar**).
2. Vá ao seguinte hive:
   - Para sistemas de 32 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\NagentFlags
   - Para sistemas de 64 bits:
     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\NagentF
3. Para a chave KLINV_INV_COLLECTOR_START_DELAY_SEC, defina o valor necessário em segundos.
   O valor padrão é de 600 segundos.
4. Reinicie o serviço do Agente de Rede.

A hora de início do inventário de software, que decorre após a execução do serviço de Agente de Rede, será alterada.

Sobre o gerenciamento de chaves de licença de aplicativos de terceiros

O Kaspersky Security Center permite rastrear o uso da chave de licença para aplicativos de terceiros instalados nos dispositivos gerenciados. A lista de aplicativos para os quais é possível rastrear o uso da chave de licença é obtida a partir do registro de aplicativos. Para cada chave de licença, é possível especificar e rastrear a violação das seguintes restrições:

- O número máximo de dispositivos nos quais o aplicativo que usa essa chave de licença pode ser instalado
- A data de expiração da chave de licença

O Kaspersky Security Center não verifica se uma chave de licença real é especificada ou não. Só é possível rastrear as restrições especificadas. Se uma das restrições impostas a uma chave de licença for violada, o Servidor de Administração registra um evento informativo, de aviso ou de falha funcional.

As chaves de licença estão vinculadas a grupos de aplicativos. Um grupo de aplicativos é um grupo de aplicativos de terceiros combinados com base em um ou mais critérios. É possível definir aplicativos pelo nome do aplicativo, versão, fornecedor e tag. Um aplicativo é adicionado ao grupo se ao menos um dos critérios for atendido. Para cada grupo de aplicativos, é possível vincular várias chaves de licença, mas cada chave de licença pode ser vinculada a um único grupo de aplicativos.

Outra ferramenta que você pode usar para rastrear o uso da chave de licença é o Relatório de status de grupos de aplicativos licenciados. Esse relatório fornece informações sobre o status atual dos grupos de aplicativos licenciados, incluindo:

- Número de instalações de chaves de licença em cada grupo de aplicativos
- Número de chaves de licença em uso e chaves de licença vagas
- Lista detalhada de aplicativos licenciados instalados em dispositivos gerenciados

As ferramentas para gerenciamento de chaves de licença de aplicativos de terceiros estão localizadas na subpasta **Uso de licenças de terceiros** (**Avançado** → **Gerenciamento de aplicativos** → **Uso de licenças de terceiros**). Nessa subpasta, é possível criar grupos de aplicativos, adicionar chaves de licença e gerar o Relatório de status em grupos de aplicativos licenciados.

As ferramentas para gerenciamento de chave de licença de aplicativos de terceiros estão disponíveis apenas se você ativou a opção Gerenciamento de patches e vulnerabilidades na janela **Configurar interface**.

Criar grupo de aplicativos licenciados

Para criar um grupo de aplicativos licenciados:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Uso de licenças de terceiros**.

2. Clique no botão **Adicionar um grupo de aplicativos licenciados** para executar o Assistente de adição de grupos de aplicativos licenciados.

   O Assistente de adição de grupos de aplicativos licenciados é iniciado.

3. Na etapa **Detalhes do grupo de aplicativos licenciados**, especifique quais aplicativos deseja incluir no grupo de aplicativos:

   - **Nome do grupo de aplicativos licenciados**

   - **Rastrear restrições violadas**

     Se uma das restrições impostas a uma chave de licença do grupo de aplicativos for violada, o Servidor de Administração registra um evento informativo, de aviso ou de falha funcional:

     - Evento informativo: **O limite de instalações está prestes a ser excedido (mais de 95% já foram utilizados) para um dos grupos de aplicativos licenciados**

     - Evento de aviso: **O limite de instalações está prestes a ser excedido para um dos grupos de aplicativos licenciados**

     - Evento de falha funcional: **O limite de instalações foi excedido para um dos grupos de aplicativos licenciados**

       Um evento é registrado apenas uma vez, quando a condição estabelecida for atendida. Da próxima vez, o mesmo evento poderá ser registrado apenas quando o número de instalações retornar ao nível normal e, em seguida, o evento ocorrer novamente. Um evento não pode ser registrado mais de uma vez por hora.

   - **Critérios para adicionar aplicativos detectados a esse grupo de aplicativos licenciados**

     Especifique os critérios para definir quais aplicativos deseja incluir no grupo de aplicativos. É possível definir aplicativos pelo nome do aplicativo, versão, fornecedor e tag. É necessário especificar pelo menos um critério. Um aplicativo é adicionado ao grupo se ao menos um dos critérios for atendido.

4. Na etapa **Inserir dados sobre chaves de licença existentes**, especifique as chaves de licença que deseja rastrear. Selecione a opção **Controlar se o limite da licença é excedido** e, em seguida, adicione as chaves de licença:

   a. Clique no botão **Adicionar**.

   b. Selecione a chave de licença que deseja adicionar, e, em seguida, clique no botão **OK**. Se a chave de licença necessária não estiver listada, clique no botão **Adicionar** e especifique as propriedades da chave de licença.

5. Na etapa **Adicionar grupo de aplicativos licenciados**, clique no botão **Concluir**.

Um grupo de aplicativos licenciados é criado e exibido na pasta **Uso de licenças de terceiros**.

Gerenciamento de chaves de licença para grupos de aplicativos licenciados

Para criar uma chave de licença para um grupo de aplicativos licenciados:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Uso de licenças de terceiros**.

2. No espaço de trabalho da pasta **Uso de licenças de terceiros**, clique no botão **Gerenciar chaves de licença de aplicativos licenciados**.

   A janela **Gerenciamento de chaves de licença em aplicativos licenciados** se abre.

3. Na janela **Gerenciamento de chaves de licença em aplicativos licenciados**, clique no botão **Adicionar**.

   A janela **Chave de licença** se abre.

4. Na janela **Chave de licença**, especifique as propriedades da chave de licença e as restrições impostas pela chave de licença no grupo de aplicativos licenciados.

   - **Nome**. O nome da chave de licença.
   - **Comentário**. Observações sobre a chave de licença selecionada.
   - **Restrição**. O número de dispositivos nos quais o aplicativo que usa esta chave de licença pode ser instalado.
   - **Expira**. A data de expiração da chave de licença.

As chaves de licença criadas são exibidas na janela **Gerenciamento de chaves de licença em aplicativos licenciados**.

Para aplicar uma chave de licença a um grupo de aplicativos licenciados:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Uso de licenças de terceiros**.

2. Na pasta **Uso de licenças de terceiros**, selecione um grupo de aplicativos licenciados aos quais você desejar aplicar uma chave de licença.

3. Selecione **Propriedades** no menu de contexto do grupo de aplicativos licenciados.

   Isso abre a janela Propriedades do grupo de aplicativos licenciados.

4. Na janela de propriedades do grupo de aplicativos licenciados, na seção **Chaves de licença**, selecione **Controlar se o limite da licença é excedido**.

5. Clique no botão **Adicionar**.

   A janela **Selecionando uma chave de licença** abre.

6. Na janela **Selecionando uma chave de licença**, selecione a chave de licença que você desejar aplicar a um grupo de aplicativos licenciados.

7. Clique em **OK**.

As restrições impostas a um grupo de aplicativos licenciados e especificadas na chave de licença também serão aplicadas ao grupo de aplicativos licenciados selecionado.

Inventário de arquivos executáveis

Você pode obter uma lista de arquivos executáveis armazenados em dispositivos gerenciados. Para o inventário de arquivos executáveis, você deve criar uma tarefa de inventário.

O recurso de inventário de arquivos executáveis está disponível para os seguintes aplicativos:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization 4.0 Light Agent e versões posteriores

O número de arquivos executáveis recebidos de um único dispositivo não pode exceder 150.000. Tendo alcançado este limite, o Kaspersky Security Center não pode receber nenhum novo arquivo.

Antes de começar, ative as notificações sobre a inicialização dos aplicativos na política do Kaspersky Endpoint Security e do Agente de Rede, para que seja possível transferir dados para o Servidor de Administração.

Para habilitar notificações sobre a inicialização de aplicativos:

- Abra as configurações de política do Kaspersky Endpoint Security e faça o seguinte:

  1. Acesse **Configurações gerais → Relatórios e armazenamento**.
  2. Na seção **Transferência de dados para o Servidor de Administração**, selecione a caixa de seleção **Sobre os aplicativos iniciados**.
  3. Salve as alterações.

- Abra as configurações de política do Agente de Rede e faça o seguinte:

  1. Siga para a seção **Repositórios**.
  2. Marque a caixa de seleção **Detalhes dos aplicativos instalados**.
  3. Salve as alterações.

Para criar uma tarefa de inventário para arquivos executáveis em dispositivos cliente:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. No espaço de trabalho da pasta **Tarefas**, clique no botão **Nova tarefa**.

   O Assistente para novas tarefas inicia.
3. Na janela **Selecionar o tipo de tarefa** do assistente, selecione **Kaspersky Endpoint Security** como o tipo de tarefa e, a seguir, selecione **Inventário** como o subtipo de tarefa e clique em **Avançar**.
4. Siga o restante das instruções do assistente.

   Após a conclusão do assistente, uma tarefa de inventário para o Kaspersky Endpoint Security será criada. A tarefa recém criada é exibida na lista de tarefas no espaço de trabalho da pasta **Tarefas**.

Uma lista de arquivos executáveis que foram detectados nos dispositivos durante o inventário, é exibida no espaço de trabalho da pasta **Arquivos executáveis**.

Durante o inventário, o aplicativo detecta arquivos executáveis nos seguintes formatos: arquivos MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Visualização de informações sobre arquivos executados

Para exibir uma lista de todos os arquivos executáveis detectados nos dispositivos cliente,

Na pasta **Gerenciamento de aplicativos** na árvore do console, selecione a subpasta **Arquivos executáveis**.

O espaço de trabalho da pasta **Arquivos executáveis** exibe uma lista de arquivos executáveis que foram executados em dispositivos cliente ou que foram detectados ao executar a tarefa de inventário do Kaspersky Endpoint Security for Windows.

Para exibir dados sobre os arquivos executáveis que atendem aos critérios especificados, você pode usar a filtragem.

Para visualizar as propriedades de um arquivo executável,

No menu de contexto do arquivo, selecione **Propriedades**.

É exibida uma janela que contém informações sobre o arquivo executável, junto com uma lista de dispositivos cliente nos quais o arquivo executável foi executado.

Monitoramento e relatórios

Esta seção descreve os recursos de monitoramento e emissão de relatórios no Kaspersky Security Center. Esses recursos fornecem a você uma visão geral da infraestrutura, dos status de proteção e das estatísticas.

Após a implementação do Kaspersky Security Center ou durante a operação, você pode configurar os recursos de monitoramento e emissão de relatórios de forma a melhor atender às suas necessidades.

- **Sinais luminosos**

  O Console de Administração permite avaliar rapidamente o status atual do Kaspersky Security Center e dos dispositivos gerenciados ao verificar os sinais luminosos.

- **Estatísticas**

  As informações estatísticas sobre a proteção do sistema e dos dispositivos gerenciados são exibidas na forma de painéis de informações que podem ser personalizados.

- **Relatórios**

  O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las.

- **Eventos**

  As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. Esses conjuntos de eventos são agrupados de acordo com as seguintes categorias:

  - Por nível de importância – **Eventos críticos**, **Falhas funcionais**, **Advertências** e **Eventos de informações**
  - Por tempo – **Eventos recentes**
  - Por tipo – **Pedidos de usuário** e **Eventos de auditoria**

Você pode criar e visualizar seleções de eventos definidas pelos usuários baseado nas configurações disponíveis para configuração na interface do Kaspersky Security Center Web Console.

Cenário: Monitoramento e relatórios

Esta seção fornece um cenário para a configuração do recurso de monitoramento e de relatórios no Kaspersky Security Center.

Pré-requisitos

Após ter implementado o Kaspersky Security Center na rede de uma organização, você poderá iniciar o seu monitoramento e gerar relatórios sobre o seu funcionamento.

Fases

O monitoramento e relatórios em na rede de uma organização prossegue em estágios:

1. **Configurar a alternância dos status do dispositivo**

   Familiarize-se com as configurações que definem a atribuição de status do dispositivo, dependendo de condições específicas. Modificando essas configurações, você pode alterar o número de eventos com os níveis de importância *Crítico* ou *Advertência*.

   Ao configurar a alternância de status de dispositivo, certifique-se de que as novas configurações não entrem em conflito com as políticas de segurança da informação de sua organização, e que você seja capaz de reagir a eventos de segurança importantes na rede em tempo hábil.

2. **Configurar as notificações de eventos em dispositivos cliente**

Configure a notificação (por e-mail, SMS ou executando um arquivo executável) de eventos em dispositivos cliente, de acordo com as necessidades da sua organização.

3. **Alteração da resposta da sua rede de segurança para o evento de Surto de vírus**

   Para ajustar a resposta da rede a novos eventos, você pode alterar os limites específicos nas propriedades do Servidor de Administração. Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência do evento.

4. **Gerenciar estatísticas**

   Configure a exibição de estatísticas de acordo com as necessidades da sua organização.

5. **Análise do status de segurança da rede da sua organização**

   Para revisar o status de segurança da rede da sua organização, você pode fazer o seguinte:

   - Na área de trabalho do nó do **Servidor de Administração**, na guia **Estatísticas**, abra a subguia (página) **Status da proteção** e revise o painel de informações **Status da proteção em tempo real**
   - Gere e revise o **Relatório do status da proteção**
   - Gere e revise o **Relatório de erros**

6. **Localize dispositivos cliente que não estão protegidos**

   Para localizar dispositivos clientes desprotegidos, acesse o espaço de trabalho do nó do **Servidor de Administração**, na guia **Estatísticas**, abra a subguia (página) **Status da proteção** e revise o painel de informações **Histórico de descoberta de novos dispositivos na rede**. Você também pode gerar e revisar o **Relatório de implementação de proteção**.

7. **Verificação da proteção de dispositivos cliente**

   Para verificar a proteção dos dispositivos cliente, acesse o espaço de trabalho do nó do **Servidor de Administração** na guia **Estatísticas**, abra a subguia (página) **Implementação** ou **Estatísticas de ameaças** e revise os devidos painéis de informações. Você também pode iniciar e revisar a **Eventos críticos**.

8. **Avaliação e limitação da carga de eventos no banco de dados**

   As informações sobre eventos que ocorrem durante a operação de aplicativos gerenciados são transferidas a partir de um dispositivo cliente e registradas no banco de dados do Servidor de Administração. Para reduzir a carga do Servidor de Administração, avalie e limite o número máximo de eventos que podem ser armazenados no banco de dados.

   Para avaliar a carga de eventos no banco de dados, calcule o espaço do banco de dados. Você também pode limitar o número máximo de eventos para evitar o estouro do banco de dados.

9. **Análise de informações de licença**

   Para revisar as informações, acesse o espaço de trabalho do nó do **Servidor de Administração**, na guia **Estatísticas**, abra a subguia (página) **Implementação** e revise o painel de informações **Uso de chaves de licença**. Você também pode gerar e revisar o **Relatório de uso das chaves de licença**.

Resultados

Após a conclusão do cenário, você é informado sobre a proteção da rede da sua organização e, portanto, poderá planejar ações para proteção adicional.

Monitorando as luzes de tráfego e os eventos registrados no Console de Administração

O Console de Administração permite avaliar rapidamente o status atual do Kaspersky Security Center e dos dispositivos gerenciados ao verificar os sinais luminosos. Os sinais luminosos são mostrados no espaço do nó do **Servidor de Administração**, na guia **Monitoramento**. A guia fornece seis painéis de informações com luzes de tráfego e eventos registrados. O sinal luminoso é uma barra vertical colorida no lado esquerdo de um painel. Cada painel com um sinal luminoso corresponde a um escopo funcional específico do Kaspersky Security Center (veja a tabela abaixo).

Escopos cobertos por sinais luminosos no Console de Administração

Nome do painel	Escopo do sinal luminoso
Implementação	Instalar Agente de Rede e aplicativos de segurança em dispositivos em uma rede da organização
Esquema do gerenciamento	Estrutura de grupos de administração. Verificação da rede. Regras de migração de dispositivos
Configurações de proteção	Funcionalidade do aplicativo de segurança: status de proteção, verificação de malwares
Atualizar	Atualizações e patches
Monitoramento	Status de proteção
Servidor de Administração	Recursos e propriedades do Servidor de Administração

Cada sinal luminoso pode ser para qualquer de uma destas quatro cores (veja a tabela abaixo). A cor de um sinal luminoso depende do status atual do Kaspersky Security Center e dos eventos que foram registrados.

Códigos em cores de sinais luminosos

Status	Cor do sinal luminoso	Significação da cor do sinal luminoso
Informativo	Verde	Intervenção do administrador não é necessária.
Advertência	Amarelo	Intervenção do administrador é necessária.
Crítico	Vermelho	Problemas sérios foram encontrados. A intervenção do administrador é necessária para solucioná-los.
Informativo	Azul-claro	Os eventos foram registrados e que são não relacionados com ameaças potenciais ou reais à segurança de dispositivos gerenciados.

A meta do administrador é manter verdes os sinais luminosos em todos dos painéis de informações da guia **Monitoramento**.

Os painéis de informações também mostram eventos registrados que afetam as luzes de tráfego e o status do Kaspersky Security Center (consulte a tabela abaixo).

Nome, descrição e cores das luzes de tráfego de eventos registrados

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Vermelho	**A licença expirou em %1 dispositivo(s)**	IDS_AK_STATUS_LIC_EXPAIRED	Eventos desse tipo ocorrem quando a licença comercial expirou. Uma vez ao dia, o Kaspersky Security Center verifica se a licença expirou nos dispositivos. Quando a licença comercial expirar, o Kaspersky Security Center fornecerá apenas a funcionalidade básica. Para continuar usando o Kaspersky Security Center, é necessário renovar sua licença comercial.
Vermelho	**O aplicativo de segurança não está em execução em: %1 dispositivos**	IDS_AK_STATUS_AV_NOT_RUNNING	Eventos desse tipo ocorrem quando o aplicativo de segurança instalado no dispositivo não está em execução. Verifique e confirme se o Kaspersky Endpoint Security está em execução no dispositivo.
Vermelho	**A proteção está desativada em: %1 dispositivos**	IDS_AK_STATUS_RTP_NOT_RUNNING	Eventos desse tipo ocorrem quando o aplicativo de segurança no dispositivo foi desativado por mais tempo que o intervalo especificado. Verifique o status atual da proteção em tempo real no dispositivo e confirme se todos os componentes da proteção necessários estão ativados.
Vermelho	**Foi detectada uma vulnerabilidade de software nos dispositivos**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Eventos desse tipo ocorrem quando a tarefa *Encontrar vulnerabilidades e atualizações necessárias* detecta vulnerabilidades com o nível de gravidade especificado em aplicativos instalados no dispositivo. Verifique a lista de atualizações disponíveis na subpasta **Atualizações de Software** updates incluída na pasta **Gerenciamento de aplicativos**. Essa pasta contém uma lista das atualizações para aplicativos da Microsoft e para produtos de software de outros fornecedores recuperadas pelo Servidor de Administração para que possam ser distribuídas para os dispositivos. Após visualizar as informações sobre as atualizações disponíveis, instale-as nos dispositivos.
Vermelho	**Eventos críticos registrados no Servidor de Administração**	IDS_AK_STATUS_EVENTS_OCCURED	Eventos desse tipo ocorrem quando eventos críticos do Servidor de Administração são detectados. Verifique a lista de eventos armazenados no Servidor de Administração e, a seguir, corrija os eventos críticos um a um.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Vermelho	**Foram registrados erros em eventos no Servidor de Administração**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Eventos desse tipo ocorrem quando os erros inesperados são registrados no lado do Servidor de Administração. Verifique a lista de eventos armazenados no Servidor de Administração e, a seguir, corrija os erros um a um.
Vermelho	**Conexão perdida para %1 dispositivos**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Eventos desse tipo ocorrem quando a conexão entre o Servidor de Administração e o dispositivo é perdida. Visualize a lista de dispositivos desconectados e tente reconectá-los.
Vermelho	**%1 dispositivos(s) não conectado(s) ao Servidor de Administração há muito tempo**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Eventos desse tipo ocorrem quando o dispositivo não se conectou ao Servidor de Administração dentro do intervalo de tempo especificado, pois o dispositivo foi desligado. Verifique e confirme se o dispositivo está ligado e se que o Agente de Rede está em execução.
Vermelho	**%1 dispositivo(s) com status diferente de OK**	IDS_AK_STATUS_HOST_NOT_OK	Eventos desse tipo ocorrem quando o status *OK* do dispositivo conectado ao Servidor de Administração muda para *Crítico* ou *Aviso*. É possível solucionar o problema usando o utilitário de diagnóstico remoto do Kaspersky Security Center.
Vermelho	**Bancos de dados desatualizados em: %1 dispositivo(s)**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Eventos desse tipo ocorrem quando os bancos de dados de antivírus não foram atualizados no dispositivo dentro do intervalo de tempo especificado. Siga as instruções para atualizar os bancos de dados da Kaspersky.
Vermelho	**Dispositivos nos quais a verificação de atualizações do Windows Update não é executada há muito tempo: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Eventos desse tipo ocorrem quando a tarefa *Executar a sincronização do Windows Update* não foi executada dentro do intervalo de tempo especificado. Siga as instruções para sincronizar as atualizações do Windows Update com o Servidor de Administração.
Vermelho	**%1 plug-in(s) do Kaspersky Security Center deve(m) ser instalado(s)**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Eventos desse tipo ocorrem quando é necessário instalar plug-ins adicionais para aplicativos da Kaspersky. Baixe e instale os plug-ins de gerenciamento necessários para o aplicativo Kaspersky a partir da página da Web do Suporte Técnico da Kaspersky.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Vermelho	**As ameaças ativas são detectadas em %1 dispositivo(s)**	IDS_AK_STATUS_NONCURED_FOUND	Eventos desse tipo ocorrem quando ameaças ativas são detectadas em dispositivos gerenciados. Visualize informações sobre as ameaças detectadas e siga as recomendações.
Vermelho	**A tarefa %1 foi concluída com um erro**	IDS_AK_STATUS_TASK_FAILED	Eventos desse tipo ocorrem quando a execução de uma tarefa é concluída com um erro. Verifique as propriedades da tarefa e, a seguir, reconfigure a tarefa.
Vermelho	**Muitos vírus foram detectados em: %1 dispositivo(s)**	IDS_AK_STATUS_TOO_MANY_THREATS	Eventos desse tipo ocorrem quando vírus são detectados em dispositivos gerenciados. Visualize informações sobre os vírus detectados e siga as recomendações.
Vermelho	**Ataque de vírus**	IDS_AK_STATUS_VIRUS_OUTBREAK	Eventos deste tipo ocorrem quando o número de objetos maliciosos detectados em diversos dispositivos gerenciados exceder o limite dentro de um curto período de tempo. Visualize informações sobre as ameaças detectadas e siga as recomendações.
Vermelho	**Os bancos de dados no repositório não foram atualizados há muito tempo**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	Eventos desse tipo ocorrem quando os bancos de dados de antivírus não são atualizados no dispositivo em dois dias. Verifique a frequência de atualização dos bancos de dados de antivírus e, a seguir, atualize os bancos de dados de antivírus.
Amarelo	**Os bancos de dados no repositório não foram atualizados há muito tempo**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	Eventos desse tipo ocorrem quando os bancos de dados de antivírus não são atualizados no dispositivo por mais de um dia, mas menos de dois dias. Verifique a frequência de atualização dos bancos de dados de antivírus e, a seguir, atualize os bancos de dados de antivírus.
Amarelo	**O conflito de nomes NetBIOS foi detectado nos dispositivos**	IDS_AK_STATUS_ADM_NAME_CONFLICT	Eventos desse tipo ocorrem quando os dispositivos têm os mesmos nomes de NetBIOS. Renomeie os dispositivos.
Amarelo	**No(s) dispositivo(s) %s, a criptografia de dados mudou para o status especificado nos critérios de detecção de status do dispositivo**	IDS_AK_STATUS_ENCRYPTION_FAULTS_FOUND	Eventos desse tipo ocorrem quando a criptografia de dados falha em dispositivos gerenciados.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Amarelo	**A licença %1 expira em %2 dias**	IDS_AK_STATUS_LIC_EXPAIRING	Eventos desse tipo ocorrem quando a licença no dispositivo expira em um número de dias especificado. Para continuar usando o Kaspersky Security Center, é necessário renovar sua licença comercial.
Amarelo	**Dispositivos não atribuídos que tiveram o Agente de Rede instalado: %1**	IDS_AK_STATUS_NAGENTS_IN_UNASSIGNED	Eventos desse tipo ocorrem quando novos dispositivos são descobertos na rede. Mova os dispositivos com o Agente de Rede para os grupos de dispositivos gerenciados.
Amarelo	**Os Agentes de Rede em %1 dispositivo(s) não poderão ser executados até o reinício. Da última vez, este estado era %2**	IDS_AK_STATUS_NAGENTS_NOT_RUNNING_UNTIL_REBOOT	Eventos desse tipo ocorrem quando o Agente de Rede não está em execução nos dispositivos. Reiniciar os dispositivos.
Amarelo	**Os arquivos detectados devem ser enviados para a Kaspersky para análise adicional**	IDS_AK_STATUS_NEW_APS_FILE_APPEARED	Eventos desse tipo ocorrem quando os arquivos provavelmente infectados com vírus são detectados e movidos para a Quarentena. Envie os arquivos para a Kaspersky para análise adicional.
Amarelo	**Dispositivo(s) gerenciado(s): %1. O aplicativo de segurança está instalado em: %2 dispositivo(s)**	IDS_AK_STATUS_NO_AV	Eventos desse tipo ocorrem quando o Kaspersky Endpoint Security não está instalado em todos os dispositivos gerenciados. Instale o Kaspersky Endpoint Security em todos os dispositivos gerenciados.
Amarelo	**A tarefa de instalação %1 foi concluída com êxito em %2 dispositivo(s); a reinicialização é necessária em %3 dispositivo(s)**	IDS_AK_STATUS_RI_NEED_REBOOT	Eventos desse tipo ocorrem quando o Kaspersky Endpoint Security acaba de ser instalado em dispositivos gerenciados. Reinicialize os dispositivos após a instalação do Kaspersky Endpoint Security.
Amarelo	**A verificação de malware não foi executada por um longo tempo em: %1 dispositivo(s)**	IDS_AK_STATUS_SCAN_LATE	Eventos desse tipo ocorrem quando é necessário executar uma verificação de malware em dispositivos gerenciados. Execute uma verificação de vírus.
Amarelo	**Dispositivo(s) com vulnerabilidades de software detectadas: %1**	IDS_AK_STATUS_VULNERABLE_HOSTS_FOUND	Eventos desse tipo ocorrem quando vulnerabilidades são detectadas em um dispositivo gerenciado. Visualize as informações sobre as vulnerabilidades detectadas e as corrija.
Verde	**Dispositivo(s) gerenciado(s): %3. Dispositivo(s) não atribuído(s) detectado(s): %1**	IDS_AK_STATUS_ADM_OK1	Eventos desse tipo ocorrem quando novos dispositivos são detectados nos grupos de administração.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Verde	**O aplicativo de segurança é instalado em todos os dispositivos gerenciados**	IDS_AK_STATUS_DEPLOYMENT_OK	Eventos desse tipo ocorrem quando o Kaspersky Endpoint Security é instalado em todos os dispositivos gerenciados.
Verde	**O Kaspersky Security Center está funcionando corretamente**	IDS_AK_STATUS_GENERAL_OK	Eventos desse tipo ocorrem quando o Kaspersky Security Center está funcionando corretamente.
Verde	**O aplicativo de proteção em tempo real não está instalado**	IDS_AK_STATUS_RTP_NA	Eventos desse tipo ocorrem quando o aplicativo antivírus não está instalado nos dispositivos gerenciados.
Verde	**A proteção está ativada**	IDS_AK_STATUS_RTP_OK	Eventos desse tipo ocorrem quando a proteção em tempo real é ativada em dispositivos gerenciados.
Verde	**O aplicativo de segurança não está instalado**	IDS_AK_STATUS_SCAN_NA	Eventos desse tipo ocorrem quando o aplicativo antivírus não está instalado nos dispositivos gerenciados.
Verde	**A verificação de malware está sendo executada conforme o agendamento**	IDS_AK_STATUS_SCAN_OK	Eventos desse tipo ocorrem quando a tarefa de *Verificação de malware* está sendo executada conforme o agendamento.
Verde	**O repositório de atualizações foi atualizado pela última vez: %1**	IDS_AK_STATUS_UPD_OK	Eventos desse tipo ocorrem quando o repositório de atualizações é atualizado.
Azul-claro	**Os bancos de dados no repositório não foram atualizados há muito tempo**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	Eventos desse tipo ocorrem quando os bancos de dados de antivírus são atualizados durante o dia.
Azul-claro	**A Declaração da Kaspersky Security Network aceita está obsoleta**	IDS_AK_STATUS_ACCEPTED_KSN_AGREEMENT_OBSOLETE	Eventos desse tipo ocorrem quando a Declaração da Kaspersky Security Network está desatualizada.
Azul-claro	**As atualizações de software da Kaspersky não foram aprovadas**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_NOT_APPROVED	Eventos desse tipo ocorrem quando o administrador ainda não aprovou os patches aplicáveis para os aplicativos Kaspersky gerenciados.
Azul-claro	**As atualizações do aplicativo Kaspersky foram revogadas**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_REVOKED	Eventos desse tipo ocorrem quando o administrador ainda não recusou os patches revogados.
Azul-claro	**O Contrato de Licença de Usuário Final do software móvel da Kaspersky não foi aceito**	IDS_AK_STATUS_KL_MOBILE_EULAS_NOT_ACCEPTED	Eventos desse tipo ocorrem quando o administrador ainda não aceitou o Contrato de Licença de Usuário Final para o software móvel da Kaspersky.
Azul-claro	**O Contrato de Licença de Usuário Final para atualizações de software da Kaspersky não foi aceito**	IDS_AK_STATUS_KL_PATCHES_EULAS_NOT_ACCEPTED	Eventos desse tipo ocorrem quando o administrador ainda não aceitou o Contrato de Licença de Usuário Final para as atualizações de software da Kaspersky.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Azul-claro	**A Declaração da Kaspersky Security Network para atualizações de software da Kaspersky não foi aceita**	IDS_AK_STATUS_KL_PATCHES_KSN_AGREEMENTS_NOT_ACCEPTED	Eventos desse tipo ocorrem quando o administrador ainda não aceitou a Declaração da Kaspersky Security Network para as atualizações de software da Kaspersky.
Azul-claro	**O usuário deve aceitar o Contrato de Licença para instalar as atualizações**	IDS_AK_STATUS_NEED_ACCEPT_EULA	Eventos desse tipo ocorrem quando novas atualizações estão disponíveis para instalação, mas o administrador ainda não aceitou o Contrato de Licença.
Azul-claro	**Novas versões dos aplicativos da Kaspersky estão disponíveis**	IDS_AK_STATUS_NEW_DISTRIBUTIVES_AVAILABLE	Eventos desse tipo ocorrem quando novas versões dos aplicativos Kaspersky estão disponíveis para instalação em dispositivos gerenciados.
Azul-claro	**As atualizações estão disponíveis para os componentes do Kaspersky Security Center**	IDS_AK_STATUS_NEW_KSC_VERSIONS_AVAILABLE	Eventos desse tipo ocorrem quando as atualizações estão disponíveis para os componentes do Kaspersky Security Center.
Azul-claro	**As atualizações estão disponíveis para os aplicativos da Kaspersky**	IDS_AK_STATUS_NEW_VERSIONS_AVAILABLE	Eventos desse tipo ocorrem quando as atualizações estão disponíveis para os aplicativos da Kaspersky.
Azul-claro	**A tarefa de instalação do aplicativo %1 foi concluída com êxito em %2 dispositivo(s), mas falhou em %3 dispositivo(s)**	IDS_AK_STATUS_RI_FAILED	Eventos desse tipo ocorrem quando a tarefa *Instalação do aplicativo* apenas instalou o software em alguns dispositivos no pool especificado.
Azul-claro	**Execução da tarefa de implementação - %1 (%2%%)**	IDS_AK_STATUS_RI_RUNNING	Eventos desse tipo ocorrem quando a tarefa de implementação está sendo executada em dispositivos gerenciados.
Azul-claro	**A verificação completa nunca foi executada em %1 dispositivo(s)**	IDS_AK_STATUS_SCAN_NOT_SCANNED	Eventos desse tipo ocorrem quando uma verificação completa nunca foi executada no número especificado de dispositivos.
Azul-claro	**Executando a tarefa de download da atualização (progresso: %1 %%)**	IDS_AK_STATUS_UPD_SRV_UPDATE_IN_PROGRESS	Eventos desse tipo ocorrem quando uma tarefa para baixar atualizações está sendo executada em dispositivos gerenciados.

Trabalhar com relatórios, estatísticas e notificações

Esta seção fornece informações sobre como trabalhar com relatórios, estatísticas e seleções de eventos e dispositivos no Kaspersky Security Center e como configurar as notificações do Servidor de Administração.

Trabalhar com relatórios

Os relatórios no Kaspersky Security Center contêm informações sobre o status dos dispositivos gerenciados. Os relatórios são gerados com base nas informações armazenadas no Servidor de Administração. Você poderá criar relatórios para os seguintes tipos de objetos:

- Para seleções de dispositivos criadas de acordo com configurações específicas.
- Para grupos de administração.
- Para dispositivos específicos de diferentes grupos de administração.
- Para todos os dispositivos na rede (disponível no relatório de implementação).

O aplicativo tem uma seleção de modelos padrão de relatório. Também é possível criar modelos de relatório personalizados. Os relatórios são exibidos na janela principal do aplicativo, na pasta **Servidor de Administração** na árvore do console.

Criação de um modelo de relatório

Para criar um modelo de relatório:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Clique no botão **Novo modelo de relatório**.

   O assistente de novo modelo de relatório é iniciado. Siga as instruções do Assistente.

Após o assistente concluir sua operação, o modelo de relatório recentemente criado é adicionado à pasta **Servidor de Administração** na árvore do console. Você pode usar este modelo para gerar e visualizar relatórios.

Visualização e edição das propriedades do modelo de relatório

Você pode visualizar e editar propriedades básicas de um modelo de relatório como, por exemplo, o nome do modelo de relatório ou os campos exibidos no relatório.

Para visualizar e editar propriedades de um modelo de relatório:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Na lista de modelos de relatório, selecione o modelo de relatório necessário.

4. No menu de contexto do modelo de relatório selecionado, selecione **Propriedades**.

   Como uma alternativa, você pode primeiro gerar o relatório e depois clicar no botão **Abrir propriedades do modelo de relatório** ou no botão **Configurar colunas do relatório**.

5. Na janela que se abre, edite as propriedades do modelo de relatório. As propriedades de cada relatório podem conter apenas algumas das seções descritas abaixo.

   - Seção **Geral**:
     - Nome do modelo de relatório
     - Número máximo de entradas a exibir

       Se esta opção estiver ativada, o número de entradas exibidas na tabela com dados de relatório detalhados não será maior que o valor especificado.

       As entradas de relatório são primeiro classificadas segundo as regras especificadas na seção **Campos → Campos de detalhes** das propriedades do modelo de relatório e, em seguida, apenas a primeira das entradas resultantes é mantida. O cabeçalho da tabela com dados de relatório detalhados mostra o número de entradas exibidas e o número total de entradas disponíveis que combinam com outras configurações do modelo de relatório.

       Se esta opção estiver desativada, a tabela com dados de relatório detalhados exibe todas as entradas disponíveis. Não recomendamos que você desative essa opção. Limitar o número de entradas de relatório exibidas reduz a carga do sistema de gerenciamento de banco de dados (DBMS) e reduz o tempo necessário para gerar e exportar o relatório. Alguns dos relatórios contêm entradas excessivas. Se este for o caso, você pode ter dificuldade para ler e analisar todas elas. Além disso, o seu dispositivo pode ficar sem memória ao gerar um relatório e, consequentemente, você não poderá exibir o relatório.

       Por padrão, esta opção está ativada. O valor predefinido é de 1.000.

     - Versão para impressão

       A saída do relatório é otimizada para impressão: os caracteres de espaço são adicionados entre alguns valores para melhorar a visibilidade.

       Por padrão, esta opção está ativada.

   - Seção **Campos**.

     Selecione os campos que serão exibidos no relatório e a ordem desses campos, e configure se as informações no relatório devem ser classificadas e filtradas segundo cada um dos campos.

   - Seção **Intervalo de tempo**.

     Modificar o período do relatório. Os valores disponíveis são:

     - Entre as duas datas especificadas
     - A partir da data especificada até à data de criação do relatório
     - Desde a data de criação do relatório menos o número especificado de dias, até a data de criação do relatório

   - **Grupo**, **Seleção de dispositivos** ou seção de **dispositivos**.

     Alterar o conjunto de dispositivos cliente para os quais o relatório é criado. Só uma destas seções pode estar presente, dependendo das configurações especificadas durante a criação do modelo de relatório.

- Seção **Configurações**.

  Alterar as configurações do relatório. O conjunto exato de configurações depende do relatório específico.

- Seção de **Segurança**. Herdar configurações do Servidor de Administração

  Se esta opção estiver ativada, as configurações de segurança do relatório são herdadas do Servidor de Administração.

  Se esta opção estiver desativada, você pode estabelecer as configurações de segurança para o relatório. Você pode atribuir uma função a um usuário ou grupo de usuários ou atribuir permissões a um usuário ou grupo de usuários, conforme aplicado ao relatório.

  Por padrão, esta opção está ativada.

  A seção **Segurança** está disponível se a caixa de seleção **Exibir as seções das configurações de segurança** for selecionada na janela de configurações da interface.

- Seção **Hierarquia de Servidores de Administração**:

  - Incluir dados dos Servidores de Administração secundários e virtuais

    Se esta opção estiver ativada, o relatório inclui as informações dos Servidores de Administração secundário e virtual subordinados ao Servidor de Administração para o qual o modelo de relatório é criado.

    Desative esta opção se você quiser visualizar dados somente do Servidor de Administração atual.

    Por padrão, esta opção está ativada.

  - Até o nível de aninhamento

    O relatório inclui dados de servidores de administração secundários e virtuais localizados sob o Servidor de administração atual a um nível de agrupamento menor ou igual ao valor especificado.

    O valor padrão é 1. Convém alterar esse valor caso necessite recuperar as informações dos Servidores de administração secundários localizados em níveis mais baixos na árvore.

  - Intervalo de espera dos dados (min.)

    Antes de gerar o relatório, o Servidor de administração para o qual o modelo de relatório é criado aguarda pelos dados de Servidores de administração secundários durante o número de minutos especificado. Se nenhum dado for recebido de um Servidor de administração secundário ao fim desse período, o relatório é executado mesmo assim. Em vez de dados reais, o relatório exibe os dados retirados do cache (caso a opção **Dados em cache dos Servidores de Administração secundários** esteja ativada) ou, caso contrário, **N/A** (não acessível).

    O valor predefinido é de 5 (minutos).

  - Dados em cache dos Servidores de Administração secundários

Os Servidores de Administração secundários regularmente transferem dados para o Servidor de Administração para o qual o modelo de relatório é criado. Nesse local, os dados transferidos são armazenados em cache.

Se o Servidor de administração atual não puder receber dados de um Servidor de administração secundário enquanto o relatório estiver sendo gerado, o relatório exibirá dados retirados do cache. A data em que os dados foram transferidos para o cache também é exibida.

Ativar essa opção permite a visualização das informações dos Servidores de administração secundários, mesmo se os dados atualizados não puderem ser recuperados. Entretanto, os dados exibidos podem ser obsoletos.

Por padrão, esta opção está desativada.

- **Frequência de atualização de cache (h)**

  Os Servidores de administração secundários regularmente transferem dados para o Servidor de administração para o qual o modelo de relatório é criado. É possível especificar o período em horas. Se o valor for 0, os dados serão transferidos somente quando o relatório for gerado.

  O valor padrão é 0.

- **Transferir informações detalhadas dos Servidores de Administração secundários**

  No relatório gerado, a tabela contendo dados de relatório detalhados inclui dados dos Servidores de Administração secundários do Servidor de Administração para o qual o modelo de relatório é criado.

  Ativar esta opção reduz a velocidade de geração de relatórios e aumenta o tráfego entre Servidores de Administração. Entretanto, você pode visualizar todos os dados em um relatório.

  Em vez de ativar a opção, convém analisar dados de relatório detalhados para detectar um Servidor de administração secundário defeituoso e, em seguida, gerar o mesmo relatório apenas para o Servidor de administração defeituoso.

  Por padrão, esta opção está desativada.

Formato de filtro estendido nos modelos de relatório

No Kaspersky Security Center 14.2, você pode aplicar o formato de filtro estendido a um modelo de relatório. O formato de filtro estendido fornece mais flexibilidade em comparação com o formato padrão. Você pode criar condições de filtragem complexas usando um conjunto de filtros, que serão aplicados ao relatório através do operador lógico OR durante a criação do relatório, conforme mostrado abaixo:

Filter[1](Field[1] AND Field[2]... AND Field[n]) OR Filter[2](Field[1] AND Field[2]... AND Field[n]) OR... Filter[n](Field[1] AND Field[2]... AND Field[n])

Além disso, com o formato de filtro estendido, você pode definir um valor de intervalo de tempo em um formato de horário relativo (por exemplo, usando uma condição "Nos últimos N dias") para campos específicos em um filtro. A disponibilidade e o conjunto de condições do intervalo de tempo dependem do tipo do modelo de relatório.

Convertendo o filtro no formato estendido

O formato de filtro estendido para modelos de relatório é compatível apenas no Kaspersky Security Center 12 e versões posteriores. Após a conversão do filtro padrão no formato estendido, o modelo de relatório se torna incompatível com os Servidores de Administração da sua rede que possuem versões anteriores do Kaspersky Security Center instaladas. As informações desses Servidores de Administração não serão recebidas para o relatório.

Para converter o filtro padrão do modelo de relatório no formato estendido:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Na lista de modelos de relatório, selecione o modelo de relatório necessário.
4. No menu de contexto do modelo de relatório selecionado, selecione **Propriedades**.
5. Na janela de propriedades que se abre, selecione a seção **Campos**.
6. Na guia **Campos de detalhes**, clique no link **Converter filtro**.
7. Na janela que se abre, clique no botão **OK**.

   A conversão no formato de filtro estendido é irreversível para o modelo de relatório ao qual é aplicado. Se você clicou no link **Converter filtro** acidentalmente, poderá cancelar as alterações clicando no botão **Cancelar** na janela de propriedades do modelo de relatório.

8. Para aplicar as alterações, feche a janela de propriedades do modelo de relatório clicando no botão **OK**.

   Quando a janela de propriedades do modelo de relatório é aberta novamente, a seção **Filtros** disponível recentemente é exibida. Nesta seção, você pode configurar o filtro estendido.

Configurando o filtro estendido

Para configurar o filtro estendido nas propriedades do modelo de relatório:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Na lista de modelos de relatório, selecione o modelo que foi convertido anteriormente para o formato de filtro estendido.
4. No menu de contexto do modelo de relatório selecionado, selecione **Propriedades**.
5. Na janela de propriedades que se abre, selecione a seção **Filtros**.

   A seção **Filtros** não será exibida se o modelo de relatório não tiver sido convertido anteriormente para o formato de filtro estendido.

   Na seção **Filtros** da janela de propriedades do modelo de relatório, você pode revisar e modificar a lista de filtros aplicados ao relatório. Cada filtro na lista tem um nome exclusivo e representa um conjunto de filtros para os campos correspondentes no relatório.

6. Abra a janela Configurações de filtro de uma das seguintes maneiras:

   - Para criar um novo filtro, clique no botão **Adicionar**.
   - Para modificar o filtro existente, selecione o filtro necessário e clique no botão **Modificar**.

7. Na janela que se abre, selecione e especifique os valores dos campos obrigatórios do filtro.
8. Clique no botão **OK** para salvar as configurações e fechar a janela.

   Se estiver criando um novo filtro, o nome do filtro deverá ser especificado no campo **Nome do filtro** antes de clicar no botão **OK**.

9. Feche a janela de propriedades do modelo de relatório clicando no botão **OK**.

   O filtro estendido no modelo de relatório está configurado. Agora você pode criar relatórios usando este modelo de relatório.

Criação e visualização de um relatório

Para criar e visualizar um relatório:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Na lista de modelos de relatório, clique duas vezes no modelo de relatório de que você precisa.

   Um relatório do modelo selecionado é exibido.

O relatório exibe os seguintes dados:

- O nome e tipo de relatórios, uma breve descrição e o período de relatórios, assim como as informações sobre o grupo de dispositivos para os quais o relatório é gerado.
- Gráfico que mostra os dados do relatório mais representativos.
- Tabela consolidada com os indicadores do relatório calculados.
- Tabela com os dados do relatório detalhado.

Para salvar um relatório

Para salvar um relatório criado:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Na lista de modelos de relatório, selecione o modelo de relatório de que você precisa.
4. No menu de contexto do modelo de relatório selecionado, selecione **Salvar**.

O Assistente de salvar relatório é iniciado. Siga as instruções do Assistente.

Após o assistente for concluído, a pasta abre na qual você salvou o arquivo de relatório.

Ao salvar um relatório como um arquivo XLS, todas as imagens relacionadas, como o logotipo e o datagrama, serão salvas como arquivos separados.

Criação de uma tarefa de entrega de relatório

Os relatórios podem ser enviados por e-mail. A entrega de relatórios no Kaspersky Security Center é realizada usando a tarefa de entrega de relatório.

Para criar uma tarefa de entrega para um relatório único:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Na lista de modelos de relatório, selecione o modelo de relatório de que você precisa.
4. No menu de contexto do modelo de relatório selecionado, selecione **Entregar relatórios**.

   O Assistente de criação da tarefa de geração de relatórios é iniciado. Siga as instruções do Assistente.

Para criar uma tarefa de entrega para múltiplos relatórios:

1. Na árvore do console, sob o nó com o nome do Servidor de Administração necessário, selecione a pasta **Tarefas**.
2. No espaço de trabalho da pasta **Tarefas**, clique no botão **Criar uma tarefa**.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

   A tarefa de entrega do relatório recém criada é exibida na pasta **Tarefas** na árvore do console.

A tarefa de entrega de relatório é criada automaticamente se as configurações de e-mail tiverem sido especificadas durante a instalação do Kaspersky Security Center.

Etapa 1. Selecionar o tipo de tarefa

Na janela **Selecionar o tipo de tarefa**, na lista de tarefas, selecione **Entregar relatórios** como o tipo de tarefa.

Clique em **Avançar** para seguir para a próxima etapa.

Etapa 2. Selecionar o tipo de relatório

Na janela **Selecionar tipo de relatório**, na lista de modelos de criação de tarefa, selecione o tipo de relatório.

Clique em **Avançar** para seguir para a próxima etapa.

Etapa 3. Ações em um relatório

Na janela **Ação a ser aplicada aos relatórios**, especifique as seguintes configurações:

- **Enviar relatórios por e-mail**

  Se esta opção estiver ativada, o aplicativo envia os relatórios gerados por e-mail.

  É possível configurar o envio do relatório por e-mail clicando no link **Configurações de notificação por e-mail**. O link está disponível se esta opção estiver ativada.

  Se esta opção estiver desativada, o aplicativo salva os relatórios na pasta especificada para armazená-los.

  Por padrão, esta opção está desativada.

- **Salvar os relatórios na pasta compartilhada**

  Se esta opção estiver ativada, o aplicativo salva o relatório na pasta, que estiver especificada no campo sob a caixa de seleção. Para salvar os relatórios em uma pasta compartilhada, especifique o caminho UNC à pasta. Neste caso, na janela **Selecionar uma conta para executar a tarefa**, você deve especificar a conta do usuário e senha para acessar esta pasta.

  Se esta opção estiver desativada, o aplicativo não salva os relatórios na pasta e os envia por e-mail.

  Por padrão, esta opção está desativada.

- **Substituir relatórios antigos do mesmo tipo**

  Se esta opção estiver ativada, o novo arquivo de relatório a cada inicialização de tarefa substitui o arquivo anteriormente salvo na pasta de relatórios na inicialização de tarefas.

  Se esta opção estiver desativada, os arquivos de relatórios não serão substituídos. Um novo arquivo de relatório será armazenado na pasta de relatórios a cada execução da tarefa.

  A caixa de seleção fica disponível se **Salvar relatório na pasta** estiver selecionado.

  Por padrão, esta opção está desativada.

- **Especificar uma conta para acessar a pasta compartilhada**

  Se esta opção estiver ativada, você poderá especificar uma conta sob a qual o relatório será salvo na pasta. Se um caminho UNC a uma pasta compartilhada for especificado como a configuração **Salvar relatório na pasta** na janela **Ação a ser aplicada ao relatório**, você deve especificar a conta de usuário e senha para acessar esta pasta.

  Se esta opção estiver desativada, o relatório será salvo na pasta sob a conta do Servidor de Administração.

  A caixa de seleção fica disponível se **Salvar relatório na pasta** estiver selecionado.

  Por padrão, esta opção está desativada.

Ao salvar ou enviar um relatório como um arquivo XLS, todas as imagens relacionadas, como o logotipo e o datagrama, serão salvas como arquivos separados.

Clique em **Avançar** para seguir para a próxima etapa.

Etapa 4. Selecionar a conta para iniciar a tarefa

Na janela **Selecionar uma conta para executar a tarefa**, você pode especificar qual conta usar ao executar a tarefa. Selecione uma das seguintes opções:

- **Conta padrão**

  A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

  Por padrão, esta opção está selecionada.

- **Especificar conta**

  Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

  - **Conta**

    Conta sob a qual a tarefa é executada.

  - **Senha**

    Senha da conta sob a qual a tarefa será executada.

Clique em **Avançar** para seguir para a próxima etapa.

Etapa 5. Configurar um agendamento da tarefa

Na página **Configurar agendamento da tarefa** do Assistente, você pode criar um agendamento para o início da tarefa. Caso seja necessário, defina as seguintes configurações:

- **Início agendado:**

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - **A cada N horas**

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - **A cada N dias**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - **A cada N semanas**

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - **A cada N minutos**

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - **Diariamente (não é compatível com horário de verão)**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - **Semanalmente**

    A tarefa é executada toda semana, no dia e na hora especificados.

  - **Por dias da semana**

A tarefa é executada regularmente, nos dias da semana e no horário especificados.

Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

Etapa 6. Definir o nome da tarefa

Na janela **Definir o nome da tarefa**, especifique o nome para a tarefa que você está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (`"*<>?\:|`).

Clique em **Avançar** para seguir para a próxima etapa.

Etapa 7. Concluir a criação da tarefa

Na janela **Concluir a criação da tarefa**, clique no botão **Concluir** para concluir o assistente.

Se você desejar que tarefa de inicie assim que o Assistente seja concluído, selecione a caixa de seleção **Executar tarefa após a conclusão do assistente**.

Gerenciar estatísticas

As informações estatísticas sobre a proteção do sistema e dos dispositivos gerenciados são exibidas na forma de painéis de informações que podem ser personalizados. As estatísticas são mostradas na área de trabalho do nó do **Servidor de Administração**, na guia **Estatísticas**. A guia contém algumas guias de segundo nível (páginas). Cada página com guias exibe painéis de informações com estatísticas, assim como links para notícias corporativas e outros materiais da Kaspersky. As informações estatísticas são exibidas em painéis de informação como uma tabela ou gráfico (setorial ou barras). Os dados nos painéis de informação são atualizados durante a execução do aplicativo, refletindo a condição atual do aplicativo de proteção.

Você pode alterar as guias de segundo nível na guia **Estatísticas**, o número dos painéis de informações em cada página com guias e o modo de exibição dos dados nos painéis de informações.

*Para adicionar uma nova guia de segundo nível com painéis de informações na guia **Estatísticas**:*

1. Clique no botão **Personalizar visualização** no canto superior direito da guia **Estatísticas**.

   A janela de propriedades das estatísticas é exibida. Esta janela contém a lista de páginas com guias que são atualmente exibidas na guia **Estatísticas**. esta janela, você pode alterar a ordem de exibição para as páginas na guia, adicionar e remover páginas e seguir para a configuração de propriedades da página ao clicar no botão **Propriedades**.

2. Clique no botão **Adicionar**.

   Isso abre a janela Propriedades de uma nova página.

3. Configurar a nova página:

   - Na seção **Geral**, especifique o nome da página.
   - Na seção **Painéis de informações**, clique no botão **Adicionar** para adicionar painéis de informações que devem ser exibidos na página.

     Clique no botão **Propriedades** na seção **Painéis de informações** para configurar as propriedades dos painéis de informação que foram adicionados: nome, tipo e aparência do gráfico no painel, assim como os dados necessários para plotar o gráfico.

4. Clique em **OK**.

A página com guias com os painéis de informações que você adicionou aparece na guia **Estatísticas**. Clique no ícone Configurações (⚙) para prosseguir imediatamente à configuração da página ou a um painel de informações selecionado naquela página.

Configurar a notificação de evento

O Kaspersky Security Center lhe permite configurar o método de notificação ao administrador sobre os eventos que ocorrem em dispositivos cliente e para configurar a notificação:

- E-mail. Sempre que ocorre um evento, o aplicativo envia uma notificação para os endereços de e-mail especificados. Você pode editar o texto da notificação.
- SMS. Sempre que ocorre um evento, o aplicativo envia uma notificação para os números de telefone especificados. Você pode configurar o envio de notificações SMS através do gateway de correio.
- Arquivo executável. Sempre que ocorre um evento em um dispositivo, o arquivo executável é iniciado na estação de trabalho do administrador. Usando o arquivo executável, o administrador pode receber os parâmetros de qualquer evento tiver ocorrido.

Para configurar a notificação de eventos que ocorrem em dispositivos cliente:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Clique no link **Configurar notificações e exportação de eventos** e selecione o valor **Configurar notificações** na lista suspensa.

   Isso abre a janela **Propriedades: Eventos**.

4. Na seção **Notificação**, selecione um método de notificação (por e-mail, SMS ou a executar um arquivo executável) e defina as configurações da notificação:

   - **E-mail**

A guia **E-mail** permite configurar notificações de e-mail para eventos.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome da rede Windows (nome NetBIOS) do dispositivo
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Se você ativar a opção **Usar consulta de DNS MX**, pode usar vários registros MX dos endereços IP para o mesmo nome DNS do servidor SMTP. O mesmo nome DNS pode ter vários registros de MX com valores diferentes de prioridade de recebimento de mensagens de e-mail. O Servidor de Administração tenta enviar notificações por e-mail ao servidor SMTP em ordem crescente de prioridade dos registros MX. Por padrão, esta opção está desativada.

Se você ativar **Usar consulta de DNS MX** e não ativar o uso de configurações TLS, recomendamos que use as configurações DNSSEC em seu dispositivo de servidor como uma medida adicional de proteção para o envio de notificações por e-mail.

Clique no link **Configurações** para definir configurações de notificação adicionais:

- Nome do assunto (nome do assunto de uma mensagem de e-mail)
- Endereço de e-mail do remetente
- Configurações de autenticação ESMTP

Você deve especificar uma conta para autenticação em um servidor SMTP se a opção de autenticação ESMTP estiver ativada para o servidor SMTP.

- Configurações TLS para servidor SMTP:
  - **Não usar TLS**

    Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.
  - **Usar TLS se compatível com servidor SMTP**

    Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.
  - **Sempre usar TLS, verificar a validade do certificado do servidor**

    Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se escolher o valor **Sempre usar TLS, verificar a validade do certificado do servidor**, poderá especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar as configurações de TLS para um servidor SMTP:

- Procurar por um arquivo de certificado do servidor SMTP:

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

- Procurar um arquivo de certificado de cliente:

Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer autoridade de certificação confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

- Certificado X-509:

Você deve especificar um arquivo com o certificado e um arquivo com a chave privada. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Quando os dois arquivos são carregados, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- Contêiner pkcs12:

Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

O campo **Mensagem da notificação** contém o texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto inclui parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio. Você pode editar o texto da mensagem adicionando outros parâmetros substitutos com detalhes mais relevantes sobre o evento. A lista de parâmetros substitutos está disponível ao clicar no botão à direita do campo.

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clique no link **Configurar limite numérico de notificações** para especificar a quantidade máxima de notificações que o aplicativo pode enviar ao longo do intervalo de tempo especificado.

Clique no botão **Enviar mensagem de teste** para verificar se você configurou as notificações corretamente. O aplicativo deve enviar uma notificação de teste aos endereços de e-mail especificados.

- SMS

A guia **SMS** permite configurar a transmissão de notificações por SMS de vários eventos para um telefone celular. As mensagens SMS são enviadas por meio de um gateway de correio.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula. As notificações serão entregues aos números de telefone associados aos endereços de e-mail especificados.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome da rede Windows (nome NetBIOS) do dispositivo
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Clique no link **Configurações** para definir configurações de notificação adicionais:

- Nome do assunto (nome do assunto de uma mensagem de e-mail)
- Endereço de e-mail do remetente
- Configurações de autenticação ESMTP

Se necessário, você pode especificar uma conta para autenticação em um servidor SMTP se a opção de autenticação ESMTP estiver ativada para o servidor SMTP.

- Configurações TLS para um servidor SMTP

Você pode desativar o uso de TLS, usar o TLS se o servidor SMTP for compatível com este protocolo ou pode forçar o uso de TLS apenas. Se optar por usar apenas TLS, poderá especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, se optar por usar apenas TLS, poderá especificar um certificado para autenticação de cliente no servidor SMTP.

- Procurar um arquivo de certificado do servidor SMTP

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Kaspersky Security Center. O Kaspersky Security Center verifica se o certificado do servidor do sistema SIEM também é assinado por uma autoridade de certificação confiável ou não. O Kaspersky Security Center não pode se conectar ao servidor do sistema SIEM se o certificado do servidor do sistema SIEM não foi recebido de uma autoridade de certificação confiável.

Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada. O campo **Mensagem de notificação** contém texto padrão com informações sobre o evento enviado pelo aplicativo quando ocorre um evento. Este texto inclui parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio. Você pode editar o texto da mensagem adicionando outros parâmetros substitutos com detalhes mais relevantes sobre o evento. A lista de parâmetros substitutos está disponível ao clicar no botão à direita do campo.

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clique no link **Configurar limite numérico de notificações** para especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

Clique no botão **Enviar mensagem de teste** para verificar se as notificações foram configuradas corretamente. O aplicativo deve enviar uma notificação de teste aos destinatários especificados.

- Arquivo executável a ser executado

  Se este método de notificação estiver selecionado, no campo de entrada, você pode especificar o aplicativo que será iniciado quando ocorre um evento.

  Clicar no link **Configurar limite numérico de notificações** permite especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

  Clicar no botão **Enviar mensagem de teste** permite verificar se você configurou as notificações apropriadamente: o aplicativo envia uma notificação de teste aos endereços de e-mail que você especificou.

5. No campo **Mensagem de notificação**, insira o texto que o aplicativo enviará quando um evento ocorrer.

   Você pode usar a lista suspensa à direita do campo de texto para adicionar configurações de substituição com detalhes de evento (por exemplo, descrição de evento ou a hora da ocorrência).

   Se o texto de notificação contiver uma porcentagem (%), você deve especificá-lo duas vezes seguidas para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

6. Clique no botão **Enviar mensagem de teste** para verificar se a notificação foi configurada corretamente.

   O aplicativo envia uma notificação de teste ao usuário especificado.

7. Clique em **OK** para salvar as alterações.

As configurações de notificação reajustadas serão aplicadas à todos os eventos que ocorrem em dispositivos cliente.

Você pode ignorar as configurações de notificação de determinados eventos na seção **Configuração de eventos** das configurações do Servidor de Administração, das configurações de uma política ou das configurações de um aplicativo.

Criar um certificado para um servidor SMTP

Para criar um certificado para um servidor SMTP:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Clique no link **Configurar notificações e exportação de eventos** e selecione o valor **Configurar notificações** na lista suspensa.

   A janela Propriedades de evento é aberta.
4. Na guia **E-mail**, clique no link **Configurações** para abrir a janela **Configurações**.
5. Na janela **Configurações**, clique no link **Especificar o certificado** para abrir a janela **Certificado para efetuar o login**.
6. Na janela **Certificado para efetuar o login**, clique no botão **Procurar**.

   A janela **Certificado** se abre.

7. Na lista suspensa **Tipo de certificado**, selecione o tipo de certificado público ou privado:

   - Se o tipo privado do certificado (**Contêiner PKCS#12**) for selecionado, especifique o arquivo e senha do certificado.
   - Se o tipo público do certificado (**Certificado X.509**) for selecionado:

     a. Especifique um arquivo de chave privada (um com a extensão *.prk ou *.pem).

     b. Especifique a senha da chave privada.

     c. Especifique o arquivo de chave pública (com a extensão *.cer).

8. Clique em **OK**.

O certificado do servidor SMTP será emitido.

Seleções de eventos

As informações sobre os eventos na operação do Kaspersky Security Center e nos aplicativos gerenciados são salvas no banco de dados do Servidor de Administração e no registro do sistema Microsoft Windows. Você pode visualizar as informações do banco de dados do Servidor de Administração no espaço de trabalho do nó **Servidor de Administração**, na guia **Eventos**.

As informações na guia **Eventos** são representadas como uma lista de seleções de eventos. Cada seleção inclui eventos de somente um tipo específico. Por exemplo, a seleção "O status do dispositivo é Crítico" somente contém registros sobre as alterações do status do dispositivo para "Crítico". Após a instalação do aplicativo, a guia **Eventos** contém algumas seleções padrão de evento. Você pode criar seleções (personalizadas) de eventos adicionais ou exportar informações de eventos para um arquivo.

Visualização de uma seleção de eventos

Para visualizar a seleção de eventos:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Na lista suspensa **Seleções de eventos**, selecione a seleção de eventos relevante.

   Caso deseje que os eventos desta seleção sejam exibidos constantemente no espaço de trabalho, clique no ícone Estrela (☆) ao lado da seleção.

   O espaço de trabalho exibirá uma lista de eventos, armazenados no Servidor de Administração, do tipo selecionado.

Você pode ordenar as informações na lista de eventos na ordem ascendente ou descendente em qualquer coluna.

Personalização de uma seleção de eventos

Para personalizar uma seleção de eventos:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Abra a seleção de eventos relevante na guia **Eventos**.
4. Clique no botão **Propriedades da seleção**.

Na janela de propriedades da seleção de eventos que abre, você pode configurar a seleção de eventos.

Criar uma seleção de eventos

Para criar uma seleção de eventos:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Clique no botão **Criar a seleção**.
4. Na janela **Nova seleção de eventos** que se abre, insira o nome da nova seleção e clique em **OK**.

Uma seleção com o nome que você especificou é criada na lista suspensa **Seleções de eventos**.

Por padrão, uma seleção de eventos criada contém todos os eventos armazenados no Servidor de Administração. Para fazer que a uma seleção somente exiba os eventos você desejar, deverá personalizar a seleção.

Exportação de uma seleção de eventos para um arquivo de texto

Para exportar uma seleção de eventos para um arquivo de texto:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Clique no botão **Importar/Exportar**.
4. Na lista suspensa, selecione **Exportar eventos para arquivo**.

O Assistente de exportação de eventos é iniciado. Siga as instruções do Assistente.

Exclusão de eventos da uma seleção

Para excluir eventos de uma seleção:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração relevante.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Selecione os eventos que pretende excluir usando o mouse, a tecla **Shift** ou **Ctrl**.
4. Exclua os eventos selecionados através de uma das seguintes formas:
   - Selecionando **Excluir** no menu de contexto de qualquer dos eventos selecionados.

     Se você selecionar o item **Excluir todos** no menu de contexto, todos os eventos exibidos serão removidos da seleção, independentemente de sua seleção de eventos para exclusão.
   - Clicando no link **Excluir evento** (se um evento estiver selecionado) ou **Excluir eventos** (se diversos eventos estiverem selecionados) na caixa de informações para esses eventos.

Os eventos selecionados são excluídos.

Adicionar aplicativos a exclusões por solicitação do usuário

Ao receber pedidos de usuário para desbloquear aplicativos bloqueados por engano, você pode criar uma exclusão para esses aplicativos a partir das regras de Segurança Adaptativa. Consequentemente, os aplicativos não mais ficarão bloqueados nos dispositivos dos usuários. Você pode rastrear o número de solicitações dos usuários na guia **Monitoramento** do Servidor de Administração.

Para adicionar aplicativos bloqueados pelo Kaspersky Endpoint Security às exclusões por solicitação do usuário:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Eventos**.
3. Na lista suspensa **Seleções de eventos**, selecione **Pedidos de usuário**.
4. Clique com o botão direito na solicitação do usuário (ou em várias solicitações) contendo os aplicativos que você deseja adicionar às exclusões e selecione **Adicionar exclusão**.

   Isso inicia o Assistente para adicionar exclusão. Siga as instruções.

Os aplicativos selecionados serão excluídos da lista **Acionamento de regras no estado de Treinamento inteligente** (em **Repositórios**, na árvore do console) após a próxima sincronização do dispositivo cliente com o Servidor de Administração e não serão mais exibidos na lista.

Seleções de dispositivos

As informações sobre o status do dispositivos são exibidas na pasta **Seleções de dispositivos** na árvore do console.

As informações na pasta **Seleções de dispositivos** são exibidas como uma lista de seleções de dispositivo. Cada seleção contém dispositivos que atendem condições específicas. Por exemplo, a seleção **Dispositivos com status Crítico** somente contém dispositivos com o status *Crítico*. Após a instalação do aplicativo, a pasta **Seleções de dispositivos** contém algumas seleções padrão. Você pode criar seleções de dispositivos adicionais (personalizada), exportar configurações de seleção para um arquivo ou criar seleções com configurações importadas de outro arquivo.

Exibir uma seleção de dispositivos

Para visualizar uma seleção de dispositivos:

1. Na árvore do console, selecione a pasta **Seleções de dispositivos**.
2. No espaço de trabalho da pasta, na lista de **Dispositivos nesta seleção**, selecione a seleção de dispositivos relevante.
3. Clique no botão **Executar seleção**.
4. Clique na guia **Resultados da seleção**.

O espaço de trabalho exibirá a lista de dispositivos que atendem o critério de seleção.

É possível ordenar as informações na lista de dispositivos em ordem ascendente ou descendente em qualquer coluna.

Configurar uma seleção de dispositivos

Para configurar uma seleção de dispositivo:

1. Na árvore do console, selecione a pasta **Seleções de dispositivos**.
2. No espaço de trabalho, clique na guia **Seleção** e, a seguir, clique na seleção de dispositivos relevante na lista de seleções de usuário.
3. Clique no botão **Propriedades da seleção**.
4. Na janela de propriedades que for aberta, especifique as seguintes configurações:
   - Propriedades gerais da seleção.
   - Condições que devem ser atendidas para a inclusão de dispositivos nesta seleção. Você pode configurar as condições após selecionar o nome de uma condição e clicar no botão **Propriedades**.
   - Configurações de segurança.
5. Clique em **OK**.

   As configurações são aplicadas e salvas.

Abaixo estão as descrições das condições para atribuir dispositivos a uma seleção. As condições são combinadas através da utilização do operador lógico OR: a seleção conterá dispositivos que estejam em conformidade com pelo menos uma das condições listadas.

Geral

Na seção **Geral**, você pode mudar o nome de uma condição de seleção e especificar se essa condição deve ser invertida:

Inverter condição de seleção

Por padrão, esta opção está desativada.

Se esta opção estiver ativada, a condição de seleção especificada será invertida. A seleção incluirá todos os dispositivos que não atendem a condição.

O exemplo a seguir mostra a lógica do trabalho de inversão:

- **Condição**: no seu dispositivo, há um sistema operacional com o tipo Linux e o número de compilação 00.0.000.
- **Condição invertida**: no seu dispositivo, há um sistema operacional com NOT (o tipo Linux e o número de compilação 00.0.000), que é equivalente ao seguinte:

  Existe um sistema operacional com o tipo NOT Linux OU número de compilação NOT 00.0.000.

Assim, a seleção incluirá os dispositivos com um sistema operacional, por exemplo, do tipo Windows e o número de compilação 00.0.000, ou o tipo Linux e qualquer número de compilação diferente de 00.0.000.

Rede

Na seção **Rede**, você pode especificar o critério que será usado para incluir dispositivos na seleção de acordo com seus dados na rede:

- **Nome do dispositivo ou endereço IP**

  Nome da rede Windows (nome NetBIOS) do dispositivo ou o endereço IPv4 ou IPv6.

- **Domínio do Windows**

  Exibe todos os dispositivos incluídos no domínio do Windows especificado.

- **Grupo de administração**

  Exibe os dispositivos incluídos no grupo de administração especificado.

- Descrição

  Texto na janela Propriedades do dispositivo: no campo **Descrição** da seção **Geral**.

  Para descrever texto no campo **Descrição**, é possível usar os seguintes caracteres:

  - Em uma palavra:

    - *****. Substitui qualquer sequência por qualquer número de caracteres.

    Exemplo:

    Para descrever as palavras **Servidor** ou **Servidores**, é possível inserir **Servidor***.

    - **?.** Substitui qualquer caractere único.

    Exemplo:

    Para descrever palavras como **Janela** ou **Janelas**, você pode inserir **Janel?.**

    O asterisco (*****) ou o ponto de interrogação (**?**) não pode ser usado como o primeiro caractere na consulta.

  - Para encontrar várias palavras:

    - Espaço. Exibe todos os dispositivos cujas descrições contêm qualquer uma das palavras listadas.

    Exemplo:

    Para localizar uma frase que contenha as palavras **Secundário** ou **Virtual**, você pode incluir a linha **Secundário Virtual** na consulta.

    - **+**. Quando o sinal de mais antecede uma palavra, todos os resultados de pesquisa contêm essa palavra.

    Exemplo:

    Para encontrar uma frase que contenha as palavras **Secundário** e **Virtual**, insira **+Secundário+Virtual** na consulta.

    - **-**. Quando um sinal de menos antecede uma palavra, nenhum dos resultados de pesquisa contém essa palavra.

    Exemplo:

    Para encontrar uma frase que contenha **Secundário**, mas que não contenha **Virtual**, insira **+Secundário-Virtual** na consulta.

    - **"<algum texto>"**. O texto dentro de aspas deve estar no texto.

    Exemplo:

    Para encontrar uma expressão que contenha a combinação de palavras **Servidor Secundário**, você pode inserir **"Servidor Secundário"** na consulta.

- Intervalo de IPs

  Se esta opção estiver ativada, você poderá inserir os endereços IP inicial e final do conjunto de IPs no qual os dispositivos relevantes devem ser incluídos.

  Por padrão, esta opção está desativada.

Tags

Na seção **Tags**, você pode configurar o critério para pesquisar por dispositivos com base em palavras-chave (tags) adicionadas anteriormente às descrições dos dispositivos gerenciados:

- **Aplicar se pelo menos uma tag especificada corresponder**

  Se esta opção estiver ativada, o resultado da pesquisa mostrará os dispositivos com descrições que contêm ao menos uma das tags selecionadas.

  Se esta opção estiver ativada, o resultado da pesquisa irá mostrar os dispositivos com descrições que não contêm todos as tags selecionadas.

  Por padrão, esta opção está desativada.

- **A tag deve ser incluída**

  Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

  Por padrão, esta opção está selecionada.

- **A tag deve ser excluída**

  Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições não contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

Active Directory

Na seção **Active Directory**, você pode configurar o critério para a inclusão de dispositivos em uma seleção com base em seus dados do Active Directory:

- **O dispositivo está em uma unidade organizacional do Active Directory**

  Se esta opção estiver ativada, a seleção inclui os dispositivos da unidade do Active Directory especificada no campo de entrada.

  Por padrão, esta opção está desativada.

- **Incluir unidades organizacionais secundárias**

  Caso esta opção esteja ativada, a seleção incluirá os dispositivos das unidades de organização secundárias da unidade organizacional do Active Directory especificada.

  Por padrão, esta opção está desativada.

- **Este dispositivo é membro de um grupo do Active Directory**

  Se esta opção estiver ativada, a seleção incluirá os dispositivos do grupo do Active Directory especificado no campo de entrada.

  Por padrão, esta opção está desativada.

Atividade de rede

Na seção **Atividade de rede**, você pode especificar o critério que será usado para incluir dispositivos na seleção de acordo com a sua atividade na rede:

- Este dispositivo é um ponto de distribuição

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. A seleção inclui dispositivos que agem como pontos de distribuição.
  - **Não**. Dispositivos que atuam como pontos de distribuição não serão incluídos na seleção.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Não desconectar do Servidor de Administração

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Ativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** está selecionada.
  - **Desativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** não está selecionada.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Perfil de conexão trocado

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. A seleção incluirá os dispositivos que se conectaram ao Servidor de Administração após o perfil de conexão ter sido alternado.
  - **Não**. A seleção não incluirá os dispositivos que se conectaram com o Servidor de Administração após o perfil de conexão ter sido alternado.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Última conexão com o Servidor de Administração

  Você pode usar essa caixa de seleção para configurar um critério para pesquisar por dispositivos pela hora da sua última conexão com o Servidor de Administração.

  Se essa caixa de seleção estiver selecionada, é possível, nos campos de entrada especificar o intervalo de tempo (data e hora) durante o qual a última conexão entre o Agente de Rede instalado no dispositivo cliente e o Servidor de Administração foi estabelecida. A seleção inclui dispositivos que estejam no intervalo especificado.

  Se essa caixa de seleção for desmarcada, o critério não é aplicado.

  Por padrão, esta caixa de seleção está desmarcada.

- Novos dispositivos detectados pela sondagem da rede

  Procura por novos dispositivos que tenham sido detectados pela sondagem da rede ao longo dos poucos últimos dias.

  Se esta opção estiver ativada, a seleção somente inclui novos dispositivos que tenham sido detectados pela descoberta de dispositivos durante a quantidade de dias especificada no campo **Período de detecção (dias)**.

  Se esta opção estiver ativada, a seleção inclui todos os dispositivos que tenham sido detectados pela descoberta de dispositivos.

  Por padrão, esta opção está desativada.

- Dispositivo visível

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos atualmente visíveis na rede.
  - **Não**. O aplicativo é incluído na seleção de dispositivos atualmente invisíveis na rede.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

Aplicativo

Na seção **Aplicativo**, você pode configurar o critério para a inclusão de dispositivos em uma seleção com base no aplicativo gerenciado selecionado:

- Nome do aplicativo

  Na lista suspensa, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome de um aplicativo da Kaspersky.

  A lista somente fornece os nomes de aplicativos com plugins de gerenciamento instalados na estação de trabalho do administrador.

  Se nenhum aplicativo for selecionado, o critério não será aplicado.

- Versão do aplicativo

  No campo de entrada, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo número da versão de um aplicativo da Kaspersky.

  Se nenhum número de versão for especificado, o critério não será aplicado.

- Nome da atualização crítica

  No campo de entrada de dados, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome do aplicativo ou pelo número do pacote de atualização.

  Se o campo for deixado em branco, o critério não será aplicado.

- Última atualização dos módulos

  Você pode usar esta opção para definir um critério para pesquisar dispositivos pela hora da última atualização dos módulos de aplicativos instalados nesses dispositivos.

  Se essa caixa de seleção estiver selecionada, nos campos de entrada você poderá especificar o intervalo de tempo (data e hora) durante o qual a última atualização de módulos de aplicativos instalados nesses dispositivos foi executada.

  Se essa caixa de seleção for desmarcada, o critério não é aplicado.

  Por padrão, esta caixa de seleção está desmarcada.

- O dispositivo é gerenciado através do Kaspersky Security Center

  Na lista suspensa, você poderá incluir nos dispositivos selecionados gerenciados através do Kaspersky Security Center:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos gerenciados através do Kaspersky Security Center.
  - **Não**. O aplicativo inclui dispositivos na seleção se eles não forem gerenciados pelo Kaspersky Security Center.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Aplicativo de segurança instalado

  Na lista suspensa, você poderá incluir na seleção todos os dispositivos com o aplicativo de segurança instalado:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos com o aplicativo de segurança instalado.
  - **Não**. O aplicativo inclui na seleção todos os dispositivos sem nenhum aplicativo de segurança instalado.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

Sistema operacional

Na seção **Sistema operacional**, você pode especificar o critério que será usado para incluir dispositivos na seleção de acordo com o seu tipo de sistema operacional.

- Versão do sistema operacional

  Se esta caixa de seleção estiver marcada, você pode selecionar um sistema operacional da lista. Os dispositivos com o sistema operacional especificado instalado são incluídos nos resultados de pesquisa.

- Tipo de bit do sistema operacional

  Na lista suspensa, você poderá selecionar a arquitetura para o sistema operacional, que determinará como a regra para mover será aplicada ao dispositivo (**Desconhecido**, **x86**, **AMD64** ou **IA64**). Por padrão, nenhuma opção é selecionada na lista para que a arquitetura do sistema operacional não fique definida.

- Versão do Service Pack do sistema operacional

  Neste campo, você pode especificar a versão do pacote do sistema operacional (no formato *X.Y*), o que determinará como a regra de migração será aplicada ao dispositivo. Por padrão, nenhum valor de versão é especificado.

- Compilação do sistema operacional

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  O número da compilação do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um número de compilação igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de compilação, exceto o especificado.

- ID da versão do sistema operacional

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  O identificador (ID) da versão do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um ID da versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de ID da versão, exceto o especificado.

Status do dispositivo

Na seção **Status do dispositivo**, você pode configurar o critério para a inclusão de dispositivos em uma seleção com base na descrição do status de dispositivos de um aplicativo gerenciado:

- Status do dispositivo

  Lista suspensa na qual você pode selecionar um dos status do dispositivo: *OK*, *Crítico* ou *Advertência*.

- Descrição do status do dispositivo

  Neste campo, você poderá selecionar caixas de seleção próximas das condições que, se atendidas, atribuem um dos seguintes status ao dispositivo: *OK, Crítico* ou *Advertência*.

- Status do dispositivo definido pelo aplicativo

  Lista suspensa na qual você pode selecionar o status da proteção em tempo real. Os dispositivos com um status da proteção em tempo real especificado serão incluídos na seleção.

Componentes de proteção

Na seção **Componentes de proteção**, você pode configurar critérios para a inclusão de dispositivos em uma seleção com base no seu status de proteção:

- **Versão dos bancos de dados**

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes por data de lançamento de versão do banco de dados antivírus. Nos campos de entrada, você pode definir o intervalo de tempo com base no qual a pesquisa é realizada.

  Por padrão, esta opção está desativada.

- **Última verificação**

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pela hora da última verificação de malwares. No campo de entrada, você poderá especificar o período de tempo no qual a última verificação de malwares foi executada.

  Por padrão, esta opção está desativada.

- **Número total de ameaças detectadas**

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pelo número de vírus detectados. Nos campos de entrada, você pode definir os valores limite inferiores e superiores pelo número de vírus encontrados.

  Por padrão, esta opção está desativada.

Registro de aplicativos

Na seção **Registro de aplicativos**, você pode definir o critério para pesquisar por dispositivos de acordo com os aplicativos neles instalados:

- **Nome do aplicativo**

  Lista suspensa na qual é possível selecionar um aplicativo. Os dispositivo nos quais o aplicativos especificado estiver instalado, serão incluídos na seleção.

- **Versão do aplicativo**

  Campo de entrada onde é possível especificar a versão do aplicativo selecionado.

- **Fornecedor**

  Lista suspensa na qual é possível selecionar o fabricante de um aplicativo instalado no dispositivo.

- **Status do aplicativo**

  Uma lista suspensa na qual é possível selecionar o status de um aplicativo (*Instalado*, *Não instalado*). Os dispositivos nos quais o aplicativo especificado está ou não instalado, dependendo do status selecionado, serão incluídos na seleção.

- **Localizar por atualização**

  Se esta opção estiver ativada, a pesquisa será executada usando os dados das atualizações para os aplicativos instalados nos dispositivos relevantes. Após selecionar a caixa de seleção, os campos **Nome do aplicativo**, **Versão do aplicativo** e **Status do aplicativo** mudam para **Nome da atualização**, **Versão da atualização** e **Status** respectivamente.

  Por padrão, esta opção está desativada.

- **Nome de aplicativo de segurança incompatível**

  Lista suspensa na qual é possível selecionar aplicativos de segurança de terceiros. Durante a pesquisa, os dispositivos nos quais está instalado o aplicativo especificado, serão incluídos na seleção.

- **Tag do aplicativo**

  Na lista suspensa, você pode selecionar a tag do aplicativo. Todos os dispositivos que instalaram aplicativos com a tag selecionada na descrição são incluídos na seleção de dispositivo.

- **Aplicar aos dispositivos sem tags especificadas**

  Se esta opção estiver ativada, o perfil da política inclui dispositivos com descrições que não contêm nenhuma das tags selecionadas.

  Se esta opção estiver desativada, o critério não é aplicado.

  Por padrão, esta opção está desativada.

Registro de hardware

Na seção **Registro de hardware**, você pode configurar o critério para a inclusão de dispositivos em uma seleção com base no seu hardware instalado:

- **Dispositivo**

  Na lista suspensa, você pode selecionar um tipo de unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

  O campo suporta a pesquisa de texto completo.

- **Fornecedor**

  Na lista suspensa, você pode selecionar o nome do fabricante da unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

  O campo suporta a pesquisa de texto completo.

- **Nome do dispositivo**

  Nome do dispositivo na rede Windows. O dispositivo com o nome especificado será incluído na seleção.

- **Descrição**

  Descrição de um dispositivo ou de uma unidade de hardware. Os dispositivos com a descrição especificada neste campo serão incluídos na seleção.

  A descrição de um dispositivo em qualquer formado pode ser inserida na janela de propriedades desse dispositivo. O campo suporta a pesquisa de texto completo.

- **Fornecedor do dispositivo**

  Nome do fabricante do dispositivo. Os dispositivos produzidos pelo fabricante especificado neste campo estão incluídos na seleção.

  Você pode inserir o nome do fabricante na janela de propriedades de um dispositivo.

- **Número de série**

  Todas as unidades hardware com número de série especificado nesse campo serão incluídas na seleção.

- **Número de inventário**

  Equipamentos com o número de inventário especificado neste campo serão incluídos na seleção.

- **Usuário**

  Todas as unidades hardware do usuário especificado nesse campo serão incluídas na seleção.

- **Localização**

  A localização do dispositivo ou unidade de hardware (por exemplo, na sede ou no escritório de uma filial). Computadores ou outros dispositivos que são implementados na localização especificada nesse campo serão incluídos na seleção.

  Você pode descrever a localização de um dispositivo em qualquer formato na janela de propriedades desse dispositivo.

- **Frequência da CPU em MHz**

  O intervalo de frequência de uma CPU. Os dispositivos com CPU's que correspondem a faixa de frequência nesses campos (inclusive) serão incluídos na seleção.

- **Núcleos de CPU virtuais**

  Faixa de número de núcleos virtuais em uma CPU. Os dispositivos com CPU's que correspondem a faixa de frequência nesses campos (inclusive) serão incluídos na seleção.

- **Volume do disco rígido, em GB**

  Faixa de valores para o tamanho do disco rígido no dispositivo. Os dispositivos com discos rígidos que correspondem a faixa nesses campos de entrada (inclusive) serão incluídos na seleção.

- **Tamanho da RAM, em MB**

  Intervalo de valores para o tamanho da RAM do dispositivo. Dispositivos com RAMs que correspondam ao intervalo nestes campos de entrada (inclusive) serão incluídos na seleção.

Máquinas virtuais

Na seção **Máquinas virtuais**, você pode definir o critério para incluir os dispositivos na seleção se estes são máquinas virtuais ou parte da Virtual Desktop Infrastructure (VDI):

- Esta é uma máquina virtual

  Na lista suspensa, você pode selecionar as seguintes opções:
  - **Irrelevante**.
  - **Não**. Localizar dispositivos que não sejam máquinas virtuais.
  - **Sim**. Localizar dispositivos que são máquinas virtuais.

- Tipo de máquina virtual

  Na lista suspensa, você pode selecionar o fabricante da máquina virtual.

  Essa lista suspensa estará disponível se o valor **Sim** ou **Irrelevante** estiver selecionado na lista suspensa **Esta é uma máquina virtual**.

- Parte da Virtual Desktop Infrastructure

  Na lista suspensa, você pode selecionar as seguintes opções:
  - **Irrelevante**.
  - **Não**. Localizar dispositivos que não fazem parte da Virtual Desktop Infrastructure.
  - **Sim**. Localizar dispositivos que fazem parte da Virtual Desktop Infrastructure (VDI).

Vulnerabilidades e atualizações

Na seção **Vulnerabilidades e atualizações**, você pode especificar o critério que será usado para incluir dispositivos na seleção de acordo com sua origem do Windows Update:

WUA foi mudado para o Servidor de Administração

Você pode selecionar uma das seguintes opções de pesquisa da lista suspensa:
- **Sim**. Se essa opção estiver selecionada, os resultados da pesquisa incluirão os dispositivos que recebem atualizações através do Windows Update do Servidor de Administração.
- **Não**. Caso essa opção esteja selecionada, os resultados incluirão os dispositivos que recebem atualizações pelo Windows Update de outras fontes.

Usuários

Na seção **Usuários**, você pode definir o critério para incluir dispositivos na seleção de acordo com as contas de usuários que efetuaram o login no sistema operacional.

- **Último usuário que fez login no sistema**

  Se esta opção estiver ativada, clique no botão **Procurar** para especificar uma conta de usuário. Os resultados da pesquisa incluem os dispositivos onde o usuário especificado efetuou o último login no sistema.

- **Usuário que fez login no sistema pelo menos uma vez**

  Se esta opção estiver ativada, clique no botão **Procurar** para especificar uma conta de usuário. Os resultados da pesquisa incluem os dispositivos nos quais o usuário especificado efetuou o login no sistema ao menos uma vez.

Problemas que afetam o status em aplicativos gerenciados

Na seção **Problemas que afetam o status em aplicativos gerenciados**, você pode especificar os critérios que serão usados para incluir os dispositivos na seleção de acordo com a lista de possíveis problemas detectados por um aplicativo gerenciado. Se pelo menos um problema que você selecionar existir em um dispositivo, o dispositivo estará incluído na seleção. Quando você seleciona um problema listado para vários aplicativos, você tem a opção de selecionar esse problema em todas das listas automaticamente.

Descrição do status do dispositivo

Você pode selecionar as caixas de seleção para descrições de status do aplicativo gerenciado; ao receber este status, os dispositivos serão incluídos na seleção. Quando você seleciona um status listado para vários aplicativos, você tem a opção de selecionar esse status em todas das listas automaticamente.

Status dos componentes em aplicativos gerenciados

Na seção **Status dos componentes em aplicativos gerenciados**, você pode configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o status dos componentes em aplicativos gerenciados:

- **Status da prevenção de vazamento de dados**

  Pesquise dispositivos pelo status da Prevenção de vazamento de dados (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

- **Status da proteção dos servidores de colaboração**

  Procure dispositivos pelo status da proteção de colaboração do servidor (*Sem dados do dispositivo*, *Parado*, *Iniciando, Pausado*, *Executando*, *Falhou*).

- **Status da proteção antivírus dos servidores de correio**

  Procure dispositivos pelo status da proteção do servidor de e-mail (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

- **Status do Endpoints Sensor**

  Procure dispositivos pelo status do componente Endpoint Sensor (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

Criptografia

Algoritmo de criptografia

Algoritmo de criptografia de bloco simétrico Advanced Encryption Standard (AES). Na lista suspensa, você pode selecionar o tamanho de chave de criptografia (de 56 bits, de 128 bits, de 192 bits ou de 256 bits).

Valores disponíveis: *AES56*, *AES128*, *AES192* e *AES256*.

Segmentos da nuvem

Na seção **Segmentos da nuvem**, você pode configurar o critério para a inclusão de dispositivos em uma seleção de acordo com os seus respetivos segmentos na nuvem:

- **O dispositivo está no segmento da nuvem**

  Se esta opção estiver ativada, você pode clicar no botão **Procurar** para especificar o segmento a ser pesquisado.

  Se a opção **Incluir objetos secundários** estiver marcada, a pesquisa é executada em todos os objetos secundários do segmento especificado.

  Os resultados da pesquisa somente incluem dispositivos do segmento selecionado.

- **Dispositivo detectado usando a API**

  Na lista suspensa, você pode selecionar se um dispositivo é detectado pelas ferramentas API:

  - **AWS**. O dispositivo é detectado usando a AWS API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do AWS.
  - **Azure**. O dispositivo é detectado usando a Azure API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do Azure.
  - **Google Cloud.** O dispositivo é descoberto usando a Google API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do Google.
  - **Não**. O dispositivo não pode ser detectado usando API do AWS, Azure ou Google, ou seja, está fora do ambiente em nuvem ou está no ambiente em nuvem, mas não pode ser detectado usando uma API.
  - **Nenhum valor**. Esta condição não se aplica.

Componentes do aplicativo

Esta seção contém a lista de componentes dos aplicativos que têm plugins de gerenciamento correspondentes instalados no Console de Administração.

Na seção **Componentes do aplicativo**, você pode especificar critérios para a inclusão de dispositivos em uma seleção segundo os status e os números da versão dos componentes que fazem referência ao aplicativo que você selecionar:

- **Status**

  Pesquise dispositivos segundo o status do componente enviado por um aplicativo ao Servidor de Administração. Você pode selecionar um dos seguintes status: *Nenhum dado do dispositivo*, *Interrompido*, *Iniciando*, *Pausado*, *Executando*, *Mau funcionamento*, ou *Não instalado*. Se o componente selecionado do aplicativo instalado em um dispositivo gerenciado tiver o status especificado, o dispositivo será incluído na seleção de dispositivos.

  Status enviados pelos aplicativos:

  - *Iniciando* – O componente está atualmente em processo de inicialização.
  - *Executando* – O componente está ativado e funcionando corretamente.
  - *Pausado* – O componente está suspenso, por exemplo, depois que o usuário pausou a proteção no aplicativo gerenciado.
  - *Mau funcionamento* – Um erro ocorreu durante a operação do componente.
  - *Interrompido* – O componente está desativado e não está funcionando no momento atual.
  - *Não instalado* – O usuário não selecionou o componente para instalação ao configurar a instalação personalizada do aplicativo.

  Diferentemente de outros status, o status *Nenhum dado do dispositivo* não é enviado pelos aplicativos. Esta opção mostra que os aplicativos não têm nenhuma informação sobre o status do componente selecionado. Por exemplo, isto pode acontecer quando o componente selecionado não pertence a nenhum dos aplicativos instalados no dispositivo, ou quando o dispositivo está desligado.

- **Versão**

  Pesquise dispositivos segundo o número da versão do componente que você selecionar na lista. Você pode digitar um número de versão, por exemplo `3.4.1.0`, e especificar se o componente selecionado deve ter uma versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todas as versões, exceto a especificada.

Exportar as configurações de uma seleção de dispositivos para um arquivo

Para exportar as configurações de uma seleção de dispositivos para um arquivo de texto:

1. Na árvore do console, selecione a pasta **Seleções de dispositivos**.
2. No espaço de trabalho, na guia **Seleção**, clique na seleção de dispositivos relevante na lista de seleções de usuário.

   As configurações podem ser exportadas apenas a partir das seleções de dispositivos criadas por um usuário.

3. Clique no botão **Executar seleção**.

4. Na guia **Resultados da seleção**, clique no botão **Exportar as configurações**.

5. Na janela **Salvar como** que é exibida, especifique um nome para o arquivo de exportação de configurações de seleção, selecione uma pasta para salvar e clique no botão **Salvar**.

As configurações da seleção de dispositivos serão salvas no arquivo especificado.

Criar uma seleção de dispositivos

Para criar uma seleção de dispositivos:

1. Na árvore do console, selecione a pasta **Seleções de dispositivos**.

2. No espaço de trabalho da pasta, clique em **Avançado** e selecione **Criar a seleção** na lista suspensa.

3. Na janela **Nova seleção de dispositivos** que se abre, insira o nome da nova seleção e clique em **OK**.

Será exibida uma nova pasta com o nome que você inseriu na árvore do console na pasta **Seleções de dispositivos**. Por padrão, a nova seleção de dispositivos contém todos os dispositivos incluídos nos grupos de administração do Servidor de Administração no qual a seleção foi criada. Para fazer com que uma seleção somente exiba os dispositivos nos quais você tem particular interesse, configure a seleção ao clicar no botão **Propriedades da seleção**.

Criar uma seleção de dispositivos de acordo com as configurações importadas

Para criar uma seleção de dispositivos de acordo com as configurações importadas:

1. Na árvore do console, selecione a pasta **Seleções de dispositivos**.

2. No espaço de trabalho da pasta, clique no botão **Avançado** e selecione **Importar seleção de arquivo** na lista suspensa.

3. Na janela que abre, especifique o caminho para o arquivo a partir do qual você pretende importar as configurações de seleção. Clique no botão **Abrir**.

Uma entrada **Nova seleção** é criada na pasta **Seleções de dispositivos**. As configurações da nova seleção são importadas do arquivo que você especificou.

Se uma seção denominada **Nova seleção** já existir na pasta **Seleções de dispositivos**, um índice no formato **(<número da próxima sequencia>)** é adicionado ao nome da seleção criada, por exemplo: **(1)**, **(2)**.

Remover os dispositivos de grupos de administração em uma seleção

Ao trabalhar com uma seleção de dispositivos, você poderá remigrar dispositivos dos grupos de administração diretamente nesta seleção, sem alternar para os grupos de administração dos quais estes dispositivos precisam ser removidos.

Para remigrar dispositivos de grupos de administração:

1. Na árvore do console, selecione a pasta **Seleções de dispositivos**.
2. Selecione os dispositivos que você desejar remover, usando as teclas **Shift** ou **Ctrl**.
3. Remova os dispositivos selecionados dos grupos de administração de uma das seguintes formas:
   - Selecione **Excluir** no menu de contexto de qualquer dos dispositivos selecionados.
   - Clique no botão **Executar a ação** e selecione **Remover do grupo** na lista suspensa.

Os dispositivos selecionados serão removidos de seus respectivos grupos de administração.

Monitoramento da instalação e desinstalação de aplicativos

Você pode monitorar a instalação e desinstalação de aplicativos específicos em dispositivos gerenciados (por exemplo, navegador específico). Para usar esta função, você pode adicionar aplicativos do registro de aplicativos à lista de aplicativos monitorados. Quando um aplicativo monitorado é instalado ou desinstalado, o Agente de Rede publica os eventos respectivos: **O aplicativo monitorado foi instalado** ou **O aplicativo monitorado foi desinstalado**. Você pode monitorar esses eventos usando, por exemplo, seleções de eventos ou relatórios.

Você pode monitorar esses eventos apenas se eles estiverem armazenados no banco de dados do Servidor de Administração.

Para adicionar um aplicativo à lista de aplicativos monitorados:

1. Na pasta **Avançado** → **Gerenciamento de aplicativos** da árvore do console, selecione a subpasta **Registro de aplicativos**.
2. Acima da lista de aplicativos que é exibida, clique no botão **Mostrar janela de propriedades de registro de aplicativos**.
3. Na janela **Aplicativos monitorados**, que é exibida, clique no botão **Adicionar**.
4. Na janela **Selecionar o nome do aplicativo**, que é exibida, selecione os aplicativos no registro de aplicativos cuja instalação ou desinstalação você deseja monitorar.
5. Na janela **Selecionar o nome do aplicativo**, clique no botão **OK**.

Após configurar a lista de aplicativos monitorados e um aplicativo monitorado seja instalado ou desinstalado nos dispositivos gerenciados da sua organização, você poderá monitorar os respectivos eventos, por exemplo, usando a seleção de eventos Eventos recentes.

Eventos dos componentes do Kaspersky Security Center

Cada componente do Kaspersky Security Center tem o seu próprio conjunto de tipos de evento. Esta seção lista tipos de eventos que ocorrem no Servidor de Administração do Kaspersky Security Center, no Agente de Rede, no Servidor de MDM do iOS e em um Servidor de dispositivos móveis do Microsoft Exchange. Os tipos de eventos que ocorrem nos aplicativos Kaspersky não são listados nesta seção.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Estrutura de dados da descrição do tipo de evento

Para cada tipo de evento, seu nome de exibição, o identificador (ID), o código alfabético, a descrição e o termo de armazenamento padrão são fornecidos.

- **Nome de exibição do tipo de evento**. Este texto é exibido no Kaspersky Security Center quando você configura eventos e quando eles ocorrem.
- **ID do tipo de evento**. Este código numérico é usado quando você processa eventos usando ferramentas de terceiros para a análise de eventos.
- **Tipo de evento** (código alfabético). Este código é usado quando você percorre e processa eventos usando vistas públicas fornecidas no banco de dados do Kaspersky Security Center e quando os eventos são exportados para um sistema SIEM.
- **Descrição**. Este texto contém as situações nas quais um evento ocorre e o que você pode fazer nesses casos.
- **Prazo de armazenamento padrão**. É o número de dias durante os quais o evento é armazenado no banco de dados do Servidor de Administração e é exibido na lista de eventos no Servidor de Administração. Após o término desse período, o evento é excluído. Se o valor do prazo de armazenamento do evento for 0, os eventos são detectados, mas não são exibidos na lista de eventos no Servidor de Administração. Se você configurou para salvar os eventos no log de eventos do sistema operacional, poderá encontrá-los nesse local.

  Você pode alterar o prazo de armazenamento de eventos:

  - Console de Administração: configuração do termo de armazenamento de um evento
  - Kaspersky Security Center Web Console: Configurar o termo de armazenamento de um evento

Outros dados podem incluir os seguintes campos:

- **event_id**: número exclusivo do evento no banco de dados, gerado e atribuído automaticamente. Não deve ser confundido com **ID do tipo de evento**.
- **task_id**: a ID da tarefa que causou o evento (se houver)
- **severity**: um dos níveis de gravidade a seguir (na ordem crescente de gravidade):

  0) nível de gravidade inválido

  1) Informativo

  2) Aviso

  3) Erro

  4) Crítico

Eventos do Servidor de Administração

Esta seção contém informações sobre os eventos relativos ao Servidor de Administração.

Eventos críticos do Servidor de Administração

A tabela abaixo mostra os tipos de eventos do Servidor de Administração do Kaspersky Security Center que têm o nível de importância **Crítico**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Caso a porta seja especificada na janela de propriedades do Servidor de Administração no Console de Administração, o **Kaspersky Security Center publicará as métricas** e os eventos críticos a serem obtidos pelo Prometheus, um sistema para monitoramento e alerta. O Prometheus obtém as métricas e os eventos críticos e, em seguida, gera os alertas para cada 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 de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O limite da licença foi excedido	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Uma vez por dia o Kaspersky Security Center verifica se um limite de licenciamento foi excedido. Eventos deste tipo ocorrem quando Servidor de Administração detectar que alguns limites de licenciamento estão excedidos pelos aplicativos da Kaspersky instalados nos dispositivos clientes e se o número de unidades de licenciamento atualmente usadas e cobertas por uma única licença exceder 110% do número total de unidades cobertas pela licença. Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. • Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração). O Kaspersky Security Center determina as regras para gerar eventos quando um limite de licenciamento for excedido.	180 dias
Surto de vírus	26 (para Proteção Contra Ameaças ao Arquivo)	GNRL_EV_VIRUS_OUTBREAK	Eventos desse tipo ocorrem quando a quantidade de objetos maliciosos detectada em diversos dispositivos gerenciados exceder o limite dentro de um curto período. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias
Surto de vírus	27 (para Proteção Contra Ameaças ao Correio)	GNRL_EV_VIRUS_OUTBREAK	Eventos desse tipo ocorrem quando a quantidade de objetos maliciosos detectada em diversos dispositivos gerenciados exceder o limite dentro de um curto período. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Surto de vírus	28 (para Firewall)	GNRL_EV_VIRUS_OUTBREAK	Eventos desse tipo ocorrem quando a quantidade de objetos maliciosos detectada em diversos dispositivos gerenciados exceder o limite dentro de um curto período. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias
O dispositivo está sem gerenciamento	4111	KLSRV_HOST_OUT_CONTROL	Eventos deste tipo ocorrem se um dispositivo gerenciado está visível na rede, mas não se conectou ao Servidor de Administração por um período específico. Descubra o que impede o funcionamento apropriado do Agente de Rede no dispositivo. As causas possíveis incluem problemas de rede e a remoção do Agente de Rede do dispositivo.	180 dias
O status do dispositivo é Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Eventos deste tipo ocorrem quando um dispositivo gerenciado é atribuído com o status *Crítico*. Você pode configurar as condições sob as quais o status do dispositivo é alterado para *Crítico*.	180 dias
O arquivo de chave foi adicionado à lista de bloqueio	4124	KLSRV_LICENSE_BLACKLISTED	Eventos deste tipo ocorrem quando a Kaspersky tiver adicionado o código de ativação ou arquivo de chave usado por você à lista de proibição. Entre em contato com o Suporte Técnico para obter mais detalhes.	180 dias
Modo de funcionalidade limitada	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Eventos deste tipo ocorrem quando o Kaspersky Security Center inicia a operar com a funcionalidade básica, sem o Gerenciamento de Dispositivos Móveis e sem o Gerenciamento de patches e vulnerabilidades. A seguir se encontram as causas de, e as respostas apropriadas, do evento: • Termo da licença expirado. Forneça uma licença para usar a funcionalidade completa do Kaspersky Security Center (adicione um código de ativação ou um arquivo de chave válido no Servidor de Administração). • O Servidor de Administração gerencia mais dispositivos do que o especificado pelo limite da licença. Mover dispositivos dos grupos de administração de um Servidor de Administração para aqueles de outro Servidor (se o limite da licença do outro Servidor de Administração o permitir).	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
A licença expira em breve	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Eventos desse tipo ocorrem quando a data de expiração da licença comercial está se aproximando. Uma vez ao dia, o Kaspersky Security Center verifica se a data de expiração da licença está próxima. Eventos deste tipo são publicados 30 dias, 15 dias, 5 dias e 1 dia antes da data de expiração da licença. Você não pode alterar a quantidade de dias. Se o Servidor de Administração é desativado no dia especificado antes da data de expiração da licença, o evento não será publicado até o próximo dia. Quando a licença comercial expirar, o Kaspersky Security Center fornecerá apenas a funcionalidade básica. Você pode responder ao evento nas seguintes maneiras: • Certifique-se de que uma chave reserva de licença seja adicionada ao Servidor de Administração. • Caso use uma assinatura, certifique-se de renová-la. Uma assinatura ilimitada será automaticamente renovada, caso tenha sido pré-paga ao provedor de serviços na data devida.	180 dias
O certificado expirou	4132	KLSRV_CERTIFICATE_EXPIRED	Eventos desse tipo ocorrem quando o certificado de cliente de dispositivos móveis expira.	180 dias
As atualizações dos módulos de software da Kaspersky foram revogadas	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Eventos deste tipo ocorrem se as atualizações racionais tenham sido revogadas (o status *Revogada* é exibido para essas atualizações) pelos especialistas técnicos da Kaspersky; por exemplo, elas precisam ser atualizadas para uma versão mais nova. Este evento é relativo aos patches do Kaspersky Security Center e não relativos aos módulos dos aplicativos Kaspersky gerenciados. O evento fornece o motivo da não instalação das atualizações racionais.	180 dias

Eventos de falha funcional do Servidor de Administração

A tabela abaixo mostra os tipos de eventos do Servidor de Administração do Kaspersky Security Center que têm o nível de importância **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Erro do tempo de execução	4125	KLSRV_RUNTIME_ERROR	Eventos deste tipo ocorrem devido a problemas desconhecidos. Mais frequentemente estes são problemas de DBMS, problemas de rede e outros problemas de software e hardware. Os detalhes do evento podem ser encontrados na descrição do evento.	180 dias
O limite de instalações foi excedido para um dos grupos de aplicativos licenciados	4126	KLSRV_INVLICPROD_EXCEDED	O Servidor de Administração gera periodicamente eventos deste tipo (a cada hora). Eventos deste tipo ocorrem se no Kaspersky Security Center você gerencia chaves de licença de aplicativos de terceiros e o número de instalações excedeu o limite definido pela chave de licença do aplicativo de terceiro. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua o aplicativo de terceiro dos dispositivos nos quais o aplicativo não está em uso. • Use uma licença de terceiro para mais dispositivos. Você pode gerenciar chaves de licença de aplicativos de terceiros usando a funcionalidade de grupos de aplicativos licenciados. Um grupo de aplicativos licenciados inclui aplicativos de terceiros que atendem os critérios definidos por você.	180 dias
Falha ao amostrar o segmento da nuvem	4143	KLSRV_KLCLOUD_SCAN_ERROR	Os eventos desse tipo ocorrem quando o Servidor de Administração falha não faz a sondagem de um segmento de rede em um ambiente de nuvem. Leia os detalhes na descrição do evento e responda de acordo.	Não armazenado
Falha ao copiar as atualizações para a pasta especificada	4123	KLSRV_UPD_REPL_FAIL	Eventos deste tipo ocorrem quando as atualizações do software são copiadas para uma pasta adicional compartilhada. Você pode responder ao evento nas seguintes maneiras: • Verifique se a conta de usuário que está sendo empregada para obter o aceso às pastas tem permissão de gravação. • Verifique se um nome de usuário e/ou senha para a(s) pasta(s) foi/está alterado. • Verifique a conexão com a internet, já que isso pode ser a causa do evento. Siga as instruções para atualizar bancos de dados e módulos do software.	180 dias
Nenhum espaço livre em disco	4107	KLSRV_DISK_FULL	Eventos deste tipo ocorrem quando o disco rígido do dispositivo onde o Servidor de Administração está instalado fica sem espaço. Libere espaço em disco no dispositivo.	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
A pasta compartilhada não está disponível	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Eventos deste tipo ocorrem se a pasta compartilhada do Servidor de Administração não estiver disponível. Você pode responder ao evento nas seguintes maneiras: • Verifique se o Servidor de Administração (onde a pasta compartilhada está localizada) está ativado e disponível. • Verifique se um nome de usuário e/ou senha para a pasta foi/está alterado. • Verifique a conexão à rede.	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O banco de dados do Servidor de Administração está indisponível	4109	KLSRV_DATABASE_UNAVAILABLE	Eventos deste tipo ocorrem se o banco de dados do Servidor de Administração s tornar indisponível. Você pode responder ao evento nas seguintes maneiras: • Verifique se o servidor remoto que tem o SQL Server instalado está disponível. • Visualize os registros do DBMS para descobrir o motivo da indisponibilidade de banco de dados do Servidor de Administração. Por exemplo, devido a uma manutenção preventiva de um servidor remoto com o SQL Server instalado possa estar indisponível.	180 dias
Espaço insuficiente no banco de dados do Servidor de Administração	4110	KLSRV_DATABASE_FULL	Eventos deste tipo ocorrem quando não houver nenhum espaço livre no banco de dados do Servidor de Administração. O Servidor de Administração não funciona quando seu banco de dados alcançou sua capacidade e quando o registro no banco de dados não for possível. A seguir estão as causas deste evento, dependendo do DBMS que você usa, e as respostas apropriadas ao evento: • Você usa o SQL Server Express Edition DBMS: Na documentação do SQL Server Express, verifique o limite de tamanho do banco de dados para a versão que estiver usando. Provavelmente, o banco de dados de seu Servidor de Administração excedeu o limite de tamanho. Limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração. No banco de dados do Servidor de Administração, há muitos eventos enviados pelo componente Controle de Aplicativos. Você pode alterar as configurações da política do Kaspersky Endpoint Security for Windows relacionadas ao armazenamento de eventos do Controle de Aplicativos no banco de dados do Servidor de Administração. • Você usa um DBMS diferente do SQL Server Express Edition: Não limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração. Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração. Revise as informações na seleção do DBMS.	180 dias

Eventos de aviso do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração do Kaspersky Security Center com o nível de importância **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Foi detectado um evento frequente de spam		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Eventos desse tipo ocorrem quando o Servidor de Administração detecta um evento frequente em um dispositivo gerenciado. Consulte a seguinte seção para obter detalhes: Bloqueio de eventos frequentes.	90 dias
O limite da licença foi excedido	4098	KLSRV_EV_LICENSE_CHECK_100_110	Uma vez por dia o Kaspersky Security Center verifica se um limite de licença foi excedido. Eventos deste tipo ocorrem quando Servidor de Administração detectar que alguns limites de licenciamento estão excedidos pelos aplicativos da Kaspersky instalados nos dispositivos clientes e se o número de unidades de licenciamento atualmente usadas e cobertas por uma única licença exceder 100% a 110% do número total de unidades cobertas pela licença. Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. • Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração). O Kaspersky Security Center determina as regras para gerar eventos quando um limite de licença é excedido.	90 dias
O dispositivo permaneceu inativo na rede por muito tempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Eventos desse tipo ocorrem quando um dispositivo gerenciado fica em inatividade por algum tempo. Na maioria das vezes, isso acontece quando um dispositivo gerenciado é desativado. Você pode responder ao evento nas seguintes maneiras: • Remova manualmente o dispositivo da lista de dispositivos gerenciados. • Especifique o intervalo de tempo após o qual o evento **O dispositivo permaneceu inativo na rede por muito tempo** é criado usando o Console de Administração ou o Kaspersky Security Center Web Console. • Especifique o intervalo de tempo após o qual o dispositivo é removido automaticamente do grupo usando o Console de Administração ou o Kaspersky Security Center Web Console.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Conflito de nomes de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Eventos desse tipo ocorrem quando o Servidor de Administração considera dois ou mais dispositivos gerenciados como um único dispositivo. Na maioria das vezes, isso acontece quando um disco rígido clonado foi usado para implantação de software em dispositivos gerenciados, sem alterar o Agente de Rede para o modo de clonagem de disco dedicado em um dispositivo de referência. Para evitar este problema, altere o Agente de Rede para o modo de clonagem de disco em um dispositivo de referência antes de clonar o disco rígido desse dispositivo.	90 dias
O status do dispositivo é Advertência	4114	KLSRV_HOST_STATUS_WARNING	Eventos deste tipo ocorrem quando à um dispositivo gerenciado for atribuído o status de *Aviso*. Você pode configurar as condições sob as quais o status do dispositivo é alterado para *Aviso*.	90 dias
O limite de instalações está prestes a ser excedido para um dos grupos de aplicativos licenciados	4127	KLSRV_INVLICPROD_FILLED	Eventos deste tipo ocorrem quando o número de instalações de aplicativos de terceiros incluídos em um grupo de aplicativos licenciados atinge 90% do valor máximo permitido especificado nas propriedades da chave de licença. Você pode responder ao evento nas seguintes maneiras: • Se o aplicativo de terceiros não estiver em uso em alguns dos dispositivos gerenciados, exclua o aplicativo desses dispositivos. • Se você espera que o número de instalações do aplicativo de terceiros ultrapasse o máximo permitido em um futuro próximo, considere obter uma licença de terceiros para um número maior de dispositivos com antecedência. Você pode gerenciar chaves de licença de aplicativos de terceiros usando a funcionalidade de grupos de aplicativos licenciados.	90 dias
O certificado foi solicitado	4133	KLSRV_CERTIFICATE_REQUESTED	Eventos deste tipo ocorrem quando um certificado para Gerenciamento de Dispositivos Móveis não é reemitido automaticamente. Seguem abaixo as possíveis causas e as respostas apropriadas para o evento: • A reemissão automática foi iniciada para um certificado para o qual a opção **Reemitir o certificado automaticamente se possível** está desativada. Isso pode ser devido a um erro ocorrido durante a criação do certificado. Pode ser necessária a reemissão manual do certificado. • Se você usar uma integração com uma infraestrutura de chave pública, a causa pode ser a ausência de um atributo SAM-Account-Name na conta usada para integração com PKI e para emissão do certificado. Revise as propriedades da conta.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O certificado foi removido	4134	KLSRV_CERTIFICATE_REMOVED	Eventos deste tipo ocorrem quando um administrador remove qualquer tipo de certificado (Geral, Correio, VPN) para Gerenciamento de Dispositivos Móveis. Depois de remover um certificado, os dispositivos móveis conectados por meio deste certificado não conseguirão se conectar ao Servidor de Administração. Este evento pode ser útil ao investigar falhas associadas ao gerenciamento de dispositivos móveis.	90 dias
O certificado vai expirar	6128	ServerCertificateExpiresSoon	Eventos deste tipo ocorrem quando os certificados do Servidor de Administração para dispositivos móveis e dispositivos com UEFI expiram. Você precisa atualizar o certificado expirado.	90 dias
O certificado de APNs expirou	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Eventos deste tipo ocorrem quando um certificado de APNs expira. Você precisa renovar manualmente o certificado de APNs e instalá-lo em um servidor de MDM do iOS.	Não armazenado
O certificado de APNs expira em breve	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Eventos deste tipo ocorrem quando faltam menos de 14 dias para a expiração do certificado de APNs. Quando o certificado de APNs expirar, você precisará renová-lo manualmente e instalá-lo em um servidor de MDM do iOS. Recomendamos que você agende a renovação do certificado de APNs antes da data de expiração.	Não armazenado
Falha ao enviar a mensagem FCM para o dispositivo móvel	4138	KLSRV_GCM_DEVICE_ERROR	Eventos desse tipo ocorrem quando o Gerenciamento de Dispositivos Móveis está configurado para usar o Firebase Cloud Messaging (FCM) para se conectar a dispositivos móveis gerenciados com um sistema operacional Android e o Servidor FCM não consegue processar algumas das solicitações recebidas do Servidor de Administração. Isso significa que alguns dos dispositivos móveis gerenciados não receberão uma notificação push. Leia o código HTTP nos detalhes da descrição do evento e responda de acordo. Para obter mais informações sobre os códigos HTTP recebidos do Servidor FCM e erros relacionados, consulte a documentação do serviço Firebase (em especial, o capítulo "Códigos de resposta de erro de mensagens downstream").	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Ocorreu um erro de HTTP ao enviar a mensagem FCM para o servidor FCM	4139	KLSRV_GCM_HTTP_ERROR	Eventos desse tipo ocorrem quando o Gerenciamento de Dispositivos Móveis está configurado para usar o Firebase Cloud Messaging (FCM) para se conectar a dispositivos móveis gerenciados com sistema operacional Android e o Servidor FCM responde à solicitação do Servidor de Administração com um código HTTP diferente de 200 (OK). Seguem abaixo as possíveis causas e as respostas apropriadas para o evento: • Problemas no lado do servidor FCM. Leia o código HTTP nos detalhes da descrição do evento e responda de acordo. Para obter mais informações sobre os códigos HTTP recebidos do Servidor FCM e erros relacionados, consulte a documentação do serviço Firebase (em especial, o capítulo "Códigos de resposta de erro de mensagens downstream"). • Problemas no lado do servidor proxy (se estiver usando servidor proxy). Leia o código HTTP nos detalhes da descrição do evento e responda de acordo.	90 dias
Falha ao enviar a mensagem FCM para o servidor FCM	4140	KLSRV_GCM_GENERAL_ERROR	Eventos desse tipo ocorrem devido a erros inesperados no Servidor de Administração ao trabalhar com o protocolo HTTP do Firebase Cloud Messaging. Leia os detalhes na descrição do evento e responda de acordo. Se você não conseguir solucionar o problema sozinho, é recomendável entrar em contato com o Suporte Técnico da Kaspersky.	90 dias
Pouco espaço livre no disco rígido	4105	KLSRV_NO_SPACE_ON_VOLUMES	Eventos deste tipo ocorrem quando o disco rígido do dispositivo onde o Servidor de Administração está instalado fica praticamente sem espaço livre. Libere espaço em disco no dispositivo.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Resta pouco espaço livre no banco de dados do Servidor de Administração	4106	KLSRV_NO_SPACE_IN_DATABASE	Eventos deste tipo ocorrem se o espaço no banco de dados do Servidor de Administração for muito limitado. Se você não remediar a situação, em breve o banco de dados do Servidor de Administração alcançará sua capacidade e o Servidor de Administração não funcionará. A seguir estão as causas deste evento, dependendo do DBMS que estiver usando, e as respostas apropriadas ao evento. Você usa o SQL Server Express Edition DBMS: • Na documentação do SQL Server Express, verifique o limite de tamanho do banco de dados para a versão que estiver usando. Provavelmente, o banco de dados de seu Servidor de Administração está por alcançar seu limite de tamanho. • Limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração. • No banco de dados do Servidor de Administração, há muitos eventos enviados pelo componente Controle de Aplicativos. Você pode alterar as configurações da política do Kaspersky Endpoint Security for Windows relacionadas ao armazenamento de eventos do Controle de Aplicativos no banco de dados do Servidor de Administração. Você usa um DBMS diferente do SQL Server Express Edition: • Não limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração Revise as informações na seleção do DBMS.	90 dias
A conexão com o Servidor de Administração secundário foi interrompida	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Eventos deste tipo ocorrem quando uma conexão com o Servidor de Administração secundário é interrompida. Leia o Log de eventos Kaspersky no dispositivo onde o Servidor de Administração primário está instalado e responda de acordo.	90 dias
A conexão com o Servidor de Administração principal foi interrompida	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Eventos deste tipo ocorrem quando uma conexão com o Servidor de Administração primário é interrompida. Leia o Log de eventos Kaspersky no dispositivo onde o Servidor de Administração primário está instalado e responda de acordo.	90 dias
Novas atualizações para os módulos de software da Kaspersky foram registradas	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Eventos deste tipo ocorrem quando o Servidor de Administração registra novas atualizações para o software Kaspersky instalado em dispositivos gerenciados que requerem aprovação para instalação. Aprove ou recuse as atualizações usando o Console de Administração ou o Kaspersky Security Center Web Console.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O limite de eventos no banco de dados foi excedido. A exclusão dos eventos foi iniciada	4145	KLSRV_EVP_DB_TRUNCATING	Eventos deste tipo ocorrem quando a exclusão de eventos antigos do banco de dados do Servidor de Administração começou após a capacidade do banco de dados do Servidor de Administração ter sido alcançada. Você pode responder ao evento nas seguintes maneiras: • Alterar o número máximo de eventos armazenados no banco de dados do Servidor de Administração • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração	Não armazenado
O limite de eventos no banco de dados foi excedido. Os eventos foram excluídos	4146	KLSRV_EVP_DB_TRUNCATED	Eventos deste tipo ocorrem quando a exclusão de eventos antigos do banco de dados do Servidor de Administração começou após a capacidade do banco de dados do Servidor de Administração ter sido alcançada. Você pode responder ao evento nas seguintes maneiras: • Altere o número máximo de eventos armazenados permitidos no banco de dados do Servidor de Administração • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração	Não armazenado
Falha na emissão automática do certificado		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Esse evento ocorre em caso de erro ao criar um certificado de cliente para um dispositivo móvel (um dispositivo operando sob um protocolo móvel).	90 dias

Eventos informativos do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração do Kaspersky Security Center com o nível de importância **Informações**.

Eventos informativos do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão	Observações
Mais de 90% desta chave de licença foram utilizados	4097	KLSRV_EV_LICENSE_CHECK_90	30 dias	
Novo dispositivo detectado	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 dias	
O dispositivo foi adicionado automaticamente ao grupo	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 dias	
O dispositivo foi removido do grupo: inativo na rede por muito tempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 dias	

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão	Observações
O limite de instalações está prestes a ser excedido (mais de 95% já foram utilizados) para um dos grupos de aplicativos licenciados	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 dias	
Foram encontrados arquivos para enviar para a Kaspersky para análise	4131	KLSRV_APS_FILE_APPEARED	30 dias	
O ID da Instância FCM foi alterado neste dispositivo móvel	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 dias	
As atualizações foram copiadas com êxito para a pasta especificada	4122	KLSRV_UPD_REPL_OK	30 dias	
A conexão com o Servidor de Administração secundário foi estabelecida	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 dias	
A conexão com o Servidor de Administração principal foi estabelecida	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 dias	
Os bancos de dados foram atualizados	4144	KLSRV_UPD_BASES_UPDATED	30 dias	
Auditoria: a conexão com o Servidor de Administração foi estabelecida	4147	KLAUD_EV_SERVERCONNECT	30 dias	
Auditoria: o objeto foi modificado	4148	KLAUD_EV_OBJECTMODIFY	30 dias	Este evento acompanha mudanças nos seguintes objetos: • Grupo de administração • Grupo de segurança • Usuário • Pacote • Tarefa • Política • Servidor • Servidor virtual
Auditoria: o status do objeto foi alterado	4150	KLAUD_EV_TASK_STATE_CHANGED	30 dias	Por exemplo, este evento ocorre quando uma tarefa falha com um erro.
Auditoria: as configurações do grupo foram modificadas	4149	KLAUD_EV_ADMGROUP_CHANGED	30 dias	
Auditoria: a conexão com o Servidor de Administração foi encerrada	4151	KLAUD_EV_SERVERDISCONNECT	30 dias	

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão	Observações
Auditoria: as propriedades do objeto foram modificadas	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 dias	Este evento rastreia as mudanças nas seguintes propriedades: • Usuário • Licença • Servidor • Servidor virtual
Auditoria: as permissões do usuário foram modificadas	4153	KLAUD_EV_OBJECTACLMODIFIED	30 dias	
Auditoria: as chaves de criptografia foram importadas ou exportadas do Servidor de Administração	5100	KLAUD_EV_DPEKEYSEXPORT	30 dias	
Emissão automática do certificado concluída		KLSRV_CERTIFICATE_AUTO_ISSUED	30 dias	Esse evento ocorre quando um certificado para um dispositivo móvel (um dispositivo operando sob um protocolo móvel) foi criado com sucesso. Este evento é gerado automaticamente pelo Servidor de Administração e só aparece no Console de Administração quando a operação correspondente é executada para certificados do Servidor de Administração, certificados de dispositivos móveis ou dispositivos UEFI.

Eventos do Agente de Rede

Esta seção contém informações sobre os eventos relativos ao Agente de Rede.

Eventos de falha funcional do Agente de Rede

A tabela abaixo mostra os tipos de eventos do Agente de Rede do Kaspersky Security Center que têm o nível de gravidade **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Erro de instalação da atualização	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Eventos deste tipo ocorrem se a atualização e correção automática para os componentes do Kaspersky Security Center não teve êxito. O evento não contém atualizações dos aplicativos gerenciados da Kaspersky. Leia a descrição do evento. Um problema do Windows no Servidor de Administração poderá ser o motivo desse evento. Se descrição mencionar qualquer problema da configuração do Windows, solucione o problema.	30 dias
Falha ao instalar a atualização de software de terceiros	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Eventos deste tipo ocorrem se os recursos de Gerenciamento de patches e vulnerabilidades e Gerenciamento de dispositivos móveis estão em uso, e se a atualização do software de terceiro não teve êxito. Verificar se o link para o software de terceiros é válido. Leia a descrição do evento.	30 dias
Falha ao instalar as atualizações do Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Eventos deste tipo ocorrem se a atualizações do Windows não tiverem êxito. Configurar as atualizações do Windows em uma política de Agente de Rede. Leia a descrição do evento. Procure o erro na Base de Dados de Conhecimento da Microsoft. Entre em contato com o Suporte Técnico da Microsoft se você não conseguir resolver o problema você mesmo.	30 dias

Eventos de aviso do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center que têm o nível de gravidade **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Uma advertência foi retornada durante a instalação da atualização dos módulos de software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 dias
A instalação da atualização do software de terceiros foi concluída com uma advertência	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 dias
A instalação da atualização do software de terceiros foi adiada	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 dias
Ocorreu um incidente	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dias
Proxy da KSN iniciado. Falha ao verificar a disponibilidade da KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 dias

Eventos informativos do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center que têm o nível de gravidade **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão
A atualização dos módulos de software foi instalada com êxito	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 dias
A instalação da atualização dos módulos de software foi iniciada	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 dias
Aplicativo instalado	7703	KLNAG_EV_INV_APP_INSTALLED	30 dias
Aplicativo desinstalado	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 dias
O aplicativo monitorado foi instalado	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 dias
O aplicativo monitorado foi desinstalado	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 dias
O aplicativo de terceiros foi instalado	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 dias
Novo dispositivo adicionado	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dias
Dispositivo removido	7709	KLNAG_EV_DEVICE_REMOVE	30 dias
Novo dispositivo detectado	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dias
O dispositivo foi autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dias
Windows Desktop Sharing: o arquivo foi lido	7712	KLUSRLOG_EV_FILE_READ	30 dias
Windows Desktop Sharing: o arquivo foi modificado	7713	KLUSRLOG_EV_FILE_MODIFIED	30 dias
Windows Desktop Sharing: aplicativo iniciado	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 dias
Windows Desktop Sharing: iniciado	7715	KLUSRLOG_EV_WDS_BEGIN	30 dias
Windows Desktop Sharing: parado	7716	KLUSRLOG_EV_WDS_END	30 dias
A atualização do software de terceiros foi instalada com êxito	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 dias
A instalação da atualização de software de terceiros foi iniciada	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 dias
Proxy da KSN iniciado. A verificação de disponibilidade da KSN foi concluída com êxito	7719	KSNPROXY_STARTED_CON_CHK_OK	30 dias
Proxy da KSN parado	7720	KSNPROXY_STOPPED	30 dias

Eventos do Servidor de MDM do iOS

Esta seção contém informações sobre os eventos relativos ao Servidor de MDM do iOS.

Eventos de falha funcional do Servidor de MDM do iOS

A tabela abaixo mostra os eventos do Servidor de MDM do iOS do Kaspersky Security Center com o nível de gravidade **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Servidor de MDM do iOS

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Falha ao solicitar a lista de perfis	PROFILELIST_COMMAND_FAILED	30 dias
Falha ao instalar o perfil	INSTALLPROFILE_COMMAND_FAILED	30 dias
Falha ao remover o perfil	REMOVEPROFILE_COMMAND_FAILED	30 dias
Falha ao solicitar a lista de perfis de provisionamento	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 dias
Falha ao instalar o perfil de provisionamento	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 dias
Falha ao remover o perfil de provisionamento	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 dias
Falha ao solicitar lista de certificados digitais	CERTIFICATELIST_COMMAND_FAILED	30 dias
Falha ao solicitar a lista de aplicativos instalados	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 dias
Falha em solicitar informações gerais sobre o dispositivo móvel	DEVICEINFORMATION_COMMAND_FAILED	30 dias
Falha ao solicitar informações de segurança	SECURITYINFO_COMMAND_FAILED	30 dias
Falha em bloquear o dispositivo móvel	DEVICELOCK_COMMAND_FAILED	30 dias
Falha ao redefinir a senha	CLEARPASSCODE_COMMAND_FAILED	30 dias
Falha em limpar os dados no dispositivo móvel	ERASEDEVICE_COMMAND_FAILED	30 dias
Falha ao instalar o aplicativo	INSTALLAPPLICATION_COMMAND_FAILED	30 dias
Falha ao definir o código de resgate para o aplicativo	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 dias
Falha ao solicitar a lista de aplicativos gerenciados	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 dias
Falha ao remover o aplicativo gerenciado	REMOVEAPPLICATION_COMMAND_FAILED	30 dias
As configurações de roaming foram rejeitadas	SETROAMINGSETTINGS_COMMAND_FAILED	30 dias
Ocorreu um erro na operação do aplicativo	PRODUCT_FAILURE	30 dias
O resultado do comando contém dados inválidos	MALFORMED_COMMAND	30 dias
Falha ao enviar a notificação push	SEND_PUSH_NOTIFICATION_FAILED	30 dias
Falha em enviar o comando	SEND_COMMAND_FAILED	30 dias
Dispositivo não encontrado	DEVICE_NOT_FOUND	30 dias

Eventos de aviso do Servidor de MDM do iOS

A tabela abaixo mostra os eventos do Servidor de MDM do iOS do Kaspersky Security Center com o nível de gravidade **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Servidor de MDM do iOS

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Uma tentativa de conectar-se um dispositivo móvel bloqueado foi detectada	INACTICE_DEVICE_TRY_CONNECTED	30 dias
O perfil foi removido	MDM_PROFILE_WAS_REMOVED	30 dias
Uma tentativa de reutilizar um certificado cliente foi detectada	CLIENT_CERT_ALREADY_IN_USE	30 dias
Dispositivo inativo detectado	FOUND_INACTIVE_DEVICE	30 dias
Um código de resgate é necessário	NEED_REDEMPTION_CODE	30 dias
Perfil incluído em uma política removida do dispositivo	UMDM_PROFILE_WAS_REMOVED	30 dias

Eventos informativos do Servidor de MDM do iOS

A tabela abaixo mostra os eventos do Servidor de MDM do iOS do Kaspersky Security Center com o nível de gravidade **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Servidor de MDM do iOS

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Novo dispositivo móvel conectado	NEW_DEVICE_CONNECTED	30 dias
A lista de perfis foi solicitada com êxito	PROFILELIST_COMMAND_SUCCESSFULL	30 dias
O perfil foi instalado com êxito	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 dias
O perfil foi removido com êxito	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 dias
A lista de perfis de provisionamento foi solicitada com êxito	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 dias
O perfil de Provisionamento foi instalado com êxito	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dias
O perfil de provisionamento foi removido com êxito	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dias
A lista de certificados digitais foi solicitada com êxito	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 dias
A lista de aplicativos instalados foi solicitada com êxito	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dias
As informações gerais sobre o dispositivo móvel foram solicitadas com êxito	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 dias
As informações de segurança foram solicitadas com êxito	SECURITYINFO_COMMAND_SUCCESSFULL	30 dias
O dispositivo móvel foi bloqueado com êxito	DEVICELOCK_COMMAND_SUCCESSFULL	30 dias
A senha foi redefinida com êxito	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 dias
Os dados foram limpos do dispositivo móvel	ERASEDEVICE_COMMAND_SUCCESSFULL	30 dias
O aplicativo foi instalado com êxito	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 dias

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
O código de resgate para o aplicativo foi definido com êxito	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 dias
A lista de aplicativos gerenciados foi solicitada com êxito	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dias
O aplicativo gerenciado foi removido com êxito	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 dias
As configurações de roaming foram aplicadas com êxito	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 dias

Eventos do Servidor de dispositivos móveis Microsoft Exchange

Esta seção contém informações sobre os eventos relativos a um Servidor de dispositivos móveis do Microsoft Exchange.

Eventos de falha funcional do Servidor de dispositivos móveis Exchange

A tabela abaixo mostra os eventos do Servidor de dispositivos móveis Exchange do Kaspersky Security Center com o nível de gravidade **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Servidor de dispositivos móveis Exchange

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Falha em limpar os dados no dispositivo móvel	WIPE_FAILED	30 dias
Não foi possível excluir as informações sobre a conexão do dispositivo móvel da caixa de correio	DEVICE_REMOVE_FAILED	30 dias
Não é possível aplicar a política ActiveSync à caixa de correio	POLICY_APPLY_FAILED	30 dias
Erro de funcionamento do aplicativo	PRODUCT_FAILURE	30 dias
Falha ao modificar o estado da funcionalidade ActiveSync	CHANGE_ACTIVE_SYNC_STATE_FAILED	30 dias

Eventos informativos do Servidor de dispositivos móveis Exchange

A tabela abaixo mostra os eventos do Servidor de dispositivos móveis Exchange do Kaspersky Security Center com o nível de gravidade **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Servidor de dispositivos móveis Exchange

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Um novo dispositivo móvel foi conectado	NEW_DEVICE_CONNECTED	30 dias
Os dados foram limpos do dispositivo móvel	WIPE_SUCCESSFULL	30 dias

Bloqueio de eventos frequentes

Esta seção fornece informações sobre como gerenciar, remover o bloqueio de eventos frequentes, e sobre como exportar a lista de eventos frequentes para um arquivo.

Sobre o bloqueio de eventos frequentes

Um aplicativo gerenciado, por exemplo, Kaspersky Endpoint Security for Windows, instalado em um ou vários dispositivos gerenciados, pode enviar muitos eventos do mesmo tipo ao Servidor de Administração. Receber eventos frequentes pode sobrecarregar o banco de dados do Servidor de Administração e sobrepor-se a outros eventos. O Servidor de Administração começa a bloquear os eventos mais frequentes quando o número de todos os eventos recebidos excede o limite especificado para o banco de dados.

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes. Você não pode bloquear os eventos frequentes ou escolher quais eventos bloquear.

Caso queira saber se um evento foi bloqueado, é possível visualizar a lista de notificações ou visualizar se o evento está presente na seção **Bloqueando eventos frequentes** das propriedades do Servidor de Administração. Se o evento estiver bloqueado, você pode fazer o seguinte:

- Se deseja evitar a substituição do banco de dados, pode continuar bloqueando o recebimento desse tipo de evento.
- Se deseja, por exemplo, localizar o motivo do envio de eventos frequentes ao Servidor de Administração, pode desbloquear os eventos frequentes e continuar recebendo os eventos deste tipo de qualquer maneira.
- Se quiser continuar recebendo os eventos frequentes até que sejam bloqueados novamente, pode remover o bloqueio dos eventos frequentes.

Gerenciando o bloqueio de eventos frequentes

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes, mas você pode interromper o bloqueio para continuar a recebê-los. Você também pode bloquear o recebimento de eventos frequentes que desbloqueou anteriormente.

Para gerenciar o bloqueio de eventos frequentes:

1. Na árvore do console do Kaspersky Security Center, abra o menu contextual da pasta **Servidor de Administração** e selecione **Propriedades**.
2. Na janela Propriedades do Servidor de Administração, no painel **Seções** e selecione **Bloqueando eventos frequentes**.

3. Na seção **Bloqueando eventos frequentes**:

   - Selecione as opções **Tipo de evento** dos eventos que você deseja bloquear o recebimento.
   - Desmarque as opções **Tipo de evento** dos eventos que deseja continuar recebendo.

4. Clique no botão **Aplicar**.
5. Clique no botão **OK**.

O Servidor de Administração recebe os eventos frequentes para os quais você desmarcou a opção **Tipo de evento** e bloqueia o recebimento de eventos frequentes para os quais você selecionou a opção **Tipo de evento**.

Removendo o bloqueio de eventos frequentes

Você pode remover o bloqueio de eventos frequentes e começar a recebê-los até que o Servidor de Administração bloqueie esse tipo de evento frequente novamente.

Para remover o bloqueio de eventos frequentes:

1. Na árvore do console do Kaspersky Security Center, abra o menu contextual da pasta **Servidor de Administração** e selecione **Propriedades**.
2. Na janela Propriedades do Servidor de Administração, no painel **Seções** e selecione **Bloqueando eventos frequentes**.
3. Na seção **Bloqueando eventos frequentes**, clique na linha do evento frequente para o qual deseja remover o bloqueio.
4. Clique no botão **Excluir**.

O evento frequente é removido da lista de eventos frequentes. O Servidor de Administração receberá eventos deste tipo.

Exportando uma lista de eventos frequentes para um arquivo

Para exportar a lista de eventos frequentes para um arquivo:

1. Na árvore do console do Kaspersky Security Center, abra o menu contextual da pasta **Servidor de Administração** e selecione **Propriedades**.
2. Na janela Propriedades do Servidor de Administração, no painel **Seções** e selecione **Bloqueando eventos frequentes**.
3. Clique no botão **Exportar para arquivo**.
4. Na janela aberta **Salvar como**, especifique o caminho para o arquivo a partir do qual você deseja salvar a lista.
5. Clique no botão **Salvar**.

Todos os registros da lista de eventos frequentes são exportados para um arquivo.

Controle de alterações no status de máquinas virtuais

O Servidor de Administração armazena informações sobre o status dos dispositivos gerenciados, como o registro de hardware e a lista de aplicativos instalados e as configurações dos aplicativos gerenciados, tarefas e políticas. Se uma máquina virtual funcionar como um dispositivo gerenciado, o usuário poderá restaurar seu status a qualquer momento usando um instantâneo da máquina virtual anteriormente criado. As informações sobre o status da máquina virtual no Servidor de Administração podem se tronar desatualizadas.

Por exemplo, o administrador criou uma política de proteção no Servidor de Administração às 12h, que começou a ser executada na máquina virtual VM_1 às 12h01. Às 12h30, o usuário da máquina virtual VM_1 alterou seu status restaurando-o a partir de um instantâneo feito às 11h. A política de proteção para de ser executada na máquina virtual. No entanto, as informações desatualizadas armazenadas no Servidor de Administração indicam que a política de proteção na máquina virtual VM_1 continua.

O Kaspersky Security Center permite monitorar todas as alterações no status das máquinas virtuais.

Após cada sincronização com um dispositivo, o Servidor de Administração cria uma ID única que é armazenada no dispositivo e no Servidor de Administração. Antes de iniciar a próxima sincronização, o Servidor de Administração compara os valores destas IDs em ambos os lados. Se os valores das IDs não coincidirem, o Servidor de Administração reconhece a máquina virtual como restaurada a partir de um instantâneo. O Servidor de Administração redefine todas as configurações de políticas e tarefas que estejam ativas para a máquina virtual e envia as políticas atualizadas e a lista de tarefas de grupo.

Monitoramento do status de proteção antivírus usando informações do registro do sistema

Para monitorar o status de proteção antivírus em um dispositivo cliente usando as informações registradas pelo Agente de Rede, dependendo do sistema operacional do dispositivo:

- Nos dispositivos executando o Windows:

  1. Abra o registro do sistema de um dispositivo cliente (por exemplo, localmente, usando o comando regedit no menu **Iniciar** → **Executar**).

  2. Vá ao seguinte hive:

     - Para sistemas de 32 bits:

       HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1103\1.0.0.0\Statistics\AVState

     - Para sistemas de 64 bits:

       HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1103\1.0.0.0\Stati

     O registro do sistema exibe informações sobre o status de proteção antivírus do dispositivo cliente.

- Nos dispositivos executando o Linux:

  - As informações são colocadas em arquivos de texto separados, um para cada tipo de dado, localizados em /var/opt/kaspersky/klnagent/1103/1.0.0.0/Statistics/AVState/.

- Nos dispositivos executando o macOS:

  - As informações são colocadas em arquivos de texto separados, um para cada tipo de dado, localizados em /Library/Application Support/Kaspersky Lab/klnagent/Data/1103/1.0.0.0/Statistics/AVState/.

O status de proteção antivírus corresponde aos valores das chaves descritas na tabela abaixo.

Chaves de registro e seus possíveis valores

Chave (tipo de dados)	Valor	Descrição
`Protection_LastConnected (REG_SZ)`	DD-MM-AAAA HH-MM-SS	Data e hora (em formato UTC) da última conexão ao Servidor de Administração
`Protection_AdmServer (REG_SZ)`	IP, nome DNS ou nome NetBIOS	Nome do Servidor de Administração que gerencia o dispositivo
`Protection_NagentVersion (REG_SZ)`	abcd	Número de compilação do Agente de Rede instalado no dispositivo
`Protection_NagentFullVersion (REG_SZ)`	a.b.c.d (patch1; patch2; ...; patchN)	Número completo da versão do Agente de Rede (com patches) instalado no dispositivo
`Protection_HostId (REG_SZ)`	ID do dispositivo	ID do dispositivo
`Protection_DynamicVM (REG_DWORD)`	0 – não 1 – sim	O Agente de Rede está instalado no modo dinâmico de VDI
`Protection_AvInstalled (REG_DWORD)`	0 – não 1 – sim	Um aplicativo de segurança está instalado no dispositivo
`Protection_AvRunning (REG_DWORD)`	0 – não 1 – sim	A proteção em tempo real está ativada no dispositivo

Chave (tipo de dados)	Valor	Descrição
`Protection_HasRtp (REG_DWORD)`	0 – não 1 – sim	Um componente de proteção em tempo real está instalado
`Protection_RtpState (REG_DWORD)`	Status da proteção em tempo real:	
	0	Desconhecido
	1	Desativado
	2	Pausada
	3	Iniciando
	4	Ativado
	5	Ativado com o alto nível de proteção (proteção máxima)
	6	Ativado com baixo nível de proteção (velocidade máxima)
	7	Ativado com as configurações padrão (recomendadas)
	8	Ativado com configurações personalizadas
	9	Falha na operação
`Protection_LastFscan (REG_SZ)`	DD-MM-AAAA HH-MM-SS	Data e hora (em formato UTC) da última verificação completa
`Protection_BasesDate (REG_SZ)`	DD-MM-AAAA HH-MM-SS	Data e hora (em formato UTC) de divulgação dos bancos de dados de aplicativo

Exibir e configurar as ações quando os dispositivos mostram inatividade

Se os dispositivos clientes em um grupo estiverem inativos, você poderá receber notificações sobre isso. Você também pode excluir automaticamente esses dispositivos.

Para exibir ou configurar as ações quando os dispositivos no grupo mostrarem inatividade:

1. No árvore do console, clique com o botão direito do mouse no nome do grupo de administração necessário.
2. No menu de contexto, selecione **Propriedades**.

   A janela de propriedades do grupo de administração se abre.
3. Na janela **Propriedades**, siga até a seção **Dispositivos**.

4. Se necessário, ative ou desative as seguintes opções:

- **Notificar o administrador se o dispositivo estiver inativo por mais de (dias)**

  Se esta opção estiver ativada, o administrador receberá notificações sobre os dispositivos inativos. Você pode especificar o intervalo de tempo após o qual o evento **O dispositivo permaneceu inativo na rede por muito tempo** será criado. O intervalo de tempo predefinido é de 7 dias.

  Por padrão, esta opção está ativada.

- **Remover o dispositivo do grupo se estiver inativo por mais de (dias)**

  Se esta opção estiver selecionada, você poderá especificar o intervalo de tempo após o qual o dispositivo será automaticamente removido do grupo. O intervalo de tempo predefinido é de 60 dias.

  Por padrão, esta opção está ativada.

- **Herdar do grupo principal**

  As configurações desta seção serão herdadas do grupo principal no qual o dispositivo cliente está incluído. Se esta opção estiver ativada, as configurações sob **Atividade de dispositivos na rede** serão bloqueadas contra quaisquer alterações.

  Esta opção está disponível somente se o grupo de administração tiver um grupo principal.

  Por padrão, esta opção está ativada.

- **Forçar herança em grupos secundários**

  Os valores de configuração serão distribuídos aos grupos secundários, mas essas configurações são bloqueadas nas propriedades dos grupos secundários.

  Por padrão, esta opção está desativada.

5. Clique em **OK**.

As suas alterações serão salvas e aplicadas.

Desativando o recebimento de Novidades Kaspersky

No Kaspersky Security Center Web Console, a seção Novidades Kaspersky (**Monitoramento e relatórios → Novidades Kaspersky**) apresenta as últimas novidades sobre a sua versão do Kaspersky Security Center e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. Se não deseja receber informações de novidades sobre a Kaspersky, pode desativar este recurso.

Os informativos da Kaspersky incluem dois tipos de informações: informativos relacionados à segurança e de marketing. Você pode desativar os informativos de cada tipo separadamente.

Para desativar informativos relacionados à segurança:

1. Na árvore do console, selecione o Servidor de Administração para o qual você deseja desativar os informativos relacionados à segurança.
2. Clique com o botão direito no menu contextual exibido e selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, na seção **Novidades Kaspersky**, desative a opção **Ativar a exibição dos informativos Kaspersky no Kaspersky Security Center Web Console**.
4. Clique em **OK**.

O recebimento de novidades sobre a Kaspersky está desativado.

Informativos de marketing estão desativados por padrão. Você recebe informativos de marketing apenas se ativou a Kaspersky Security Network (KSN). Você pode desativar este tipo de informativo desativando a KSN.

Ajuste de pontos de distribuição e gateways de conexão

Uma estrutura de grupos de administração no Kaspersky Security Center executa as seguintes funções:

- Define o escopo das políticas

  Há um modo alternativo para aplicar configurações relevantes nos dispositivos, usando *perfis de política*. Neste caso, defina o escopo das políticas com tags, localizações de dispositivos nas unidades organizacionais do Active Directory ou associação nos grupos de segurança do Active Directory.

- Define o escopo da tarefas de grupo

  Há uma abordagem para definir o escopo da tarefas de grupo que não tem base em uma hierarquia de grupos de administração: uso de tarefas para seleções de dispositivos e tarefas para dispositivos específicos.

- Define os direitos de acesso aos dispositivos, Servidores de Administração virtuais e Servidores de Administração secundários

- Atribui os pontos de distribuição

Ao criar a estrutura de grupos de administração, você deve levar em conta a topologia da rede da organização para a atribuição ótima de pontos de distribuição. A distribuição ótima dos pontos de distribuição permite poupar tráfego na rede da organização.

Dependendo do esquema da organização e da topologia da rede, as seguintes configurações padrão podem ser aplicadas à estrutura de grupos de administração:

- Escritório único

- Múltiplos pequenos escritórios remotos

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Configuração padrão de pontos de distribuição: escritório único

Em uma configuração de "escritório único" padrão, todos os dispositivos estão dentro da rede da organização, portanto eles podem se "ver" mutuamente. A rede da organização pode consistir em algumas partes separadas (redes ou segmentos de rede) vinculadas por canais estreitos.

Os seguintes métodos de criar a estrutura de grupos de administração são possíveis:

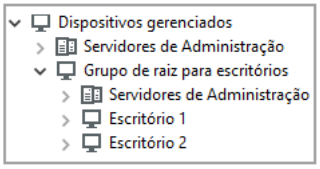
- Criar uma estrutura de grupos de administração levando em consideração a topologia da rede. A estrutura de grupos de administração pode não refletir a topologia da rede com uma precisão absoluta. Uma coincidência entre as partes separadas da rede e determinados grupos de administração seria suficiente. Você pode usar a atribuição automática de pontos de distribuição ou atribui-los manualmente.

- Criar uma estrutura de grupos de administração não levando em consideração a topologia da rede. Nesse caso, é necessário desativar a atribuição automática de pontos de distribuição e, a seguir, atribuir um ou diversos dispositivos para atuar como pontos de distribuição de um grupo de administração raiz em cada uma das partes separadas da rede, por exemplo, para o grupo **Dispositivos gerenciados**. Todos os pontos de distribuição estarão no mesmo nível e apresentarão a mesma expansão de escopo para todos os dispositivos na rede da organização. Nesse caso, cada Agente de Rede se conectará ao ponto de distribuição que tenha a rota mais curta. A rota para um ponto de distribuição pode ser traçada com o utilitário tracert.

Configuração padrão de pontos de distribuição: múltiplos pequenos escritórios remotos

Esta configuração padrão proporciona uma série de pequenos escritórios remotos, que podem se comunicar com a sede através da Internet. Cada escritório remoto é localizado além da NAT, ou seja, a conexão de um escritório remoto ao outro não é possível porque os escritórios estão isolados entre si.

A configuração deve ser refletida na estrutura de grupos de administração: um grupo de administração separado deve ser criado para cada escritório remoto (grupos **Escritório 1** e **Escritório 2** na figura abaixo).



Os escritórios remotos estão incluídos na estrutura do grupo de administração

Um ou vários pontos de distribuição devem ser atribuídos à cada grupo de administração que corresponda a um escritório. Os pontos de distribuição devem ser dispositivos nos escritórios remotos que têm espaço livre suficiente em disco. Os dispositivos implementados no grupo **Escritório 1**, por exemplo, acessarão os pontos de distribuição atribuídos ao grupo de administração **Escritório 1**.

Se alguns usuários se moverem entre escritórios fisicamente, com os seus computadores portáteis, você deve selecionar dois ou mais dispositivos (além dos pontos de distribuição existentes) em cada escritório remoto e atribui-los para atuar como pontos de distribuição para um grupo de administração de nível superior (**Grupo de raiz para escritórios** na figura acima).

Exemplo: Um computador portátil é implementado no grupo de administração **Escritório 1** e então é movido fisicamente para o escritório que corresponde ao grupo de administração **Escritório 2**. Após o computador portátil ter sido movido, o Agente de Rede tenta acessar os pontos de distribuição atribuídos ao grupo **Escritório 1**, mas aqueles pontos de distribuição estão indisponíveis. Então, O Agente de Rede começa a tentar acessar os pontos de distribuição que foram atribuídos ao **Grupo de raiz para escritórios**. Como os escritórios remotos estão isolados entre si, as tentativas de acessar os pontos de distribuição atribuídos ao grupo de administração **Grupo raiz para escritórios** somente terão êxito quando o Agente de Rede tentar acessar os pontos de distribuição no grupo **Escritório 2**. Ou seja, o computador portátil permanecerá no grupo de administração que corresponde ao escritório inicial, mas o computador portátil usará o ponto de distribuição do escritório onde estiver fisicamente localizado no momento.

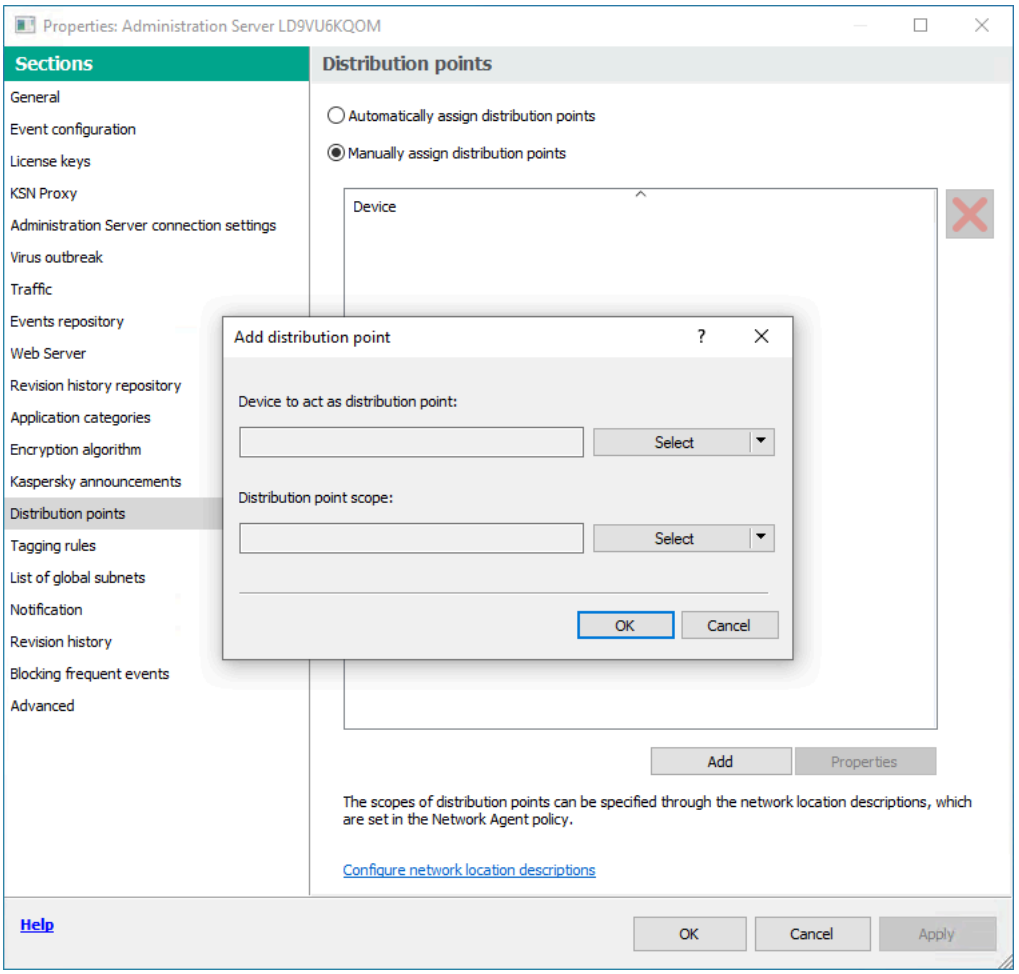
Atribuindo um dispositivo para agir como ponto de distribuição

Você pode atribuir manualmente um dispositivo para atuar como ponto de distribuição para um grupo de administração e configurá-lo como gateway de conexão no Console de Administração.

Para atribuir um dispositivo como um ponto de distribuição de um grupo de administração:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, selecione a seção **Pontos de distribuição**.
4. Na parte direita da janela, selecione a opção **Atribuir manualmente os pontos de distribuição**.

5. Clique no botão **Adicionar**.



Atribua um ponto de distribuição manualmente

Isso abre a janela **Adicionar ponto de distribuição**.

6. Na janela **Adicionar ponto de distribuição**, execute as seguintes ações:

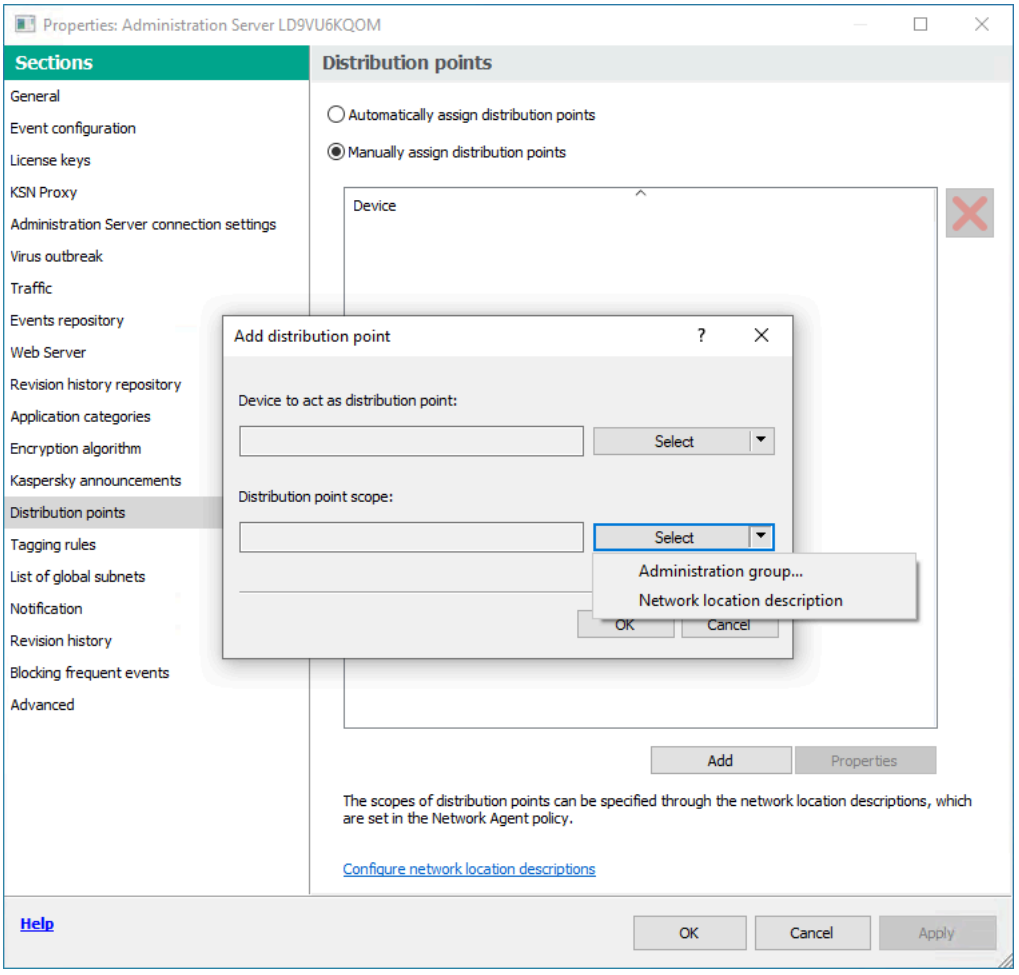
   a. Em **Dispositivo para atuar como ponto de distribuição**, clique na seta para baixo no botão **Selecionar** e selecione a opção **Adicionar dispositivo do grupo**.

   b. Na janela aberta **Selecionar dispositivos**, escolha o dispositivo para atuar como um ponto de distribuição.

   c. No **escopo do ponto de distribuição**, clique na seta para baixo no botão **Selecionar**.

   d. Indique os dispositivos específicos aos quais o ponto de distribuição distribuirá as atualizações. Você pode especificar um grupo de administração ou uma descrição da localização da rede.

e. Clique em **OK** para fechar a janela **Adicionar ponto de distribuição**.



Selecionar o escopo do ponto de distribuição

O pontos de distribuição que você adicionou será exibido na lista de pontos de distribuição na seção **Pontos de distribuição**.

O primeiro dispositivo cliente com Agente de Rede instalado que se conectar ao Servidor de Administração virtual será automaticamente atribuído para agir como o ponto de distribuição e configurado como o gateway de conexão.

Conectando um dispositivo Linux como um gateway em zona desmilitarizada

Para conectar um dispositivo Linux como gateway na zona desmilitarizada (DMZ):

1. Baixe e instale o Agente de Rede no dispositivo Linux.

2. Execute o script de pós-instalação e siga o assistente para definir a configuração do ambiente local. No prompt de comando, execute o seguinte comando:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Na etapa que solicita o modo do Agente de Rede, escolha a opção **Usar como gateway de conexão**.

4. No Console de Administração baseado em MMC, no menu de contexto do Servidor de Administração, selecione **Propriedades**.

5. Na janela de propriedades do Servidor de Administração que é exibida, selecione a seção **Pontos de distribuição**.

6. Na janela aberta **Pontos de distribuição**, à direita da janela:

   a. Selecione a opção **Atribuir manualmente os pontos de distribuição**.

   b. Clique no botão **Adicionar**.

   Isso abre a janela **Adicionar ponto de distribuição**.

7. Na janela **Adicionar ponto de distribuição**, execute as seguintes ações:

   a. Em **Dispositivo para atuar como ponto de distribuição**, clique na seta para baixo no botão **Selecionar** e selecione a opção **Adicionar o gateway de conexão no DMZ por endereço**.

   b. No **escopo do ponto de distribuição**, clique na seta para baixo no botão **Selecionar**.

   c. Indique os dispositivos específicos aos quais o ponto de distribuição distribuirá as atualizações. Você pode especificar um grupo de administração.

   d. Clique em **OK** para fechar a janela **Adicionar ponto de distribuição**.

8. O pontos de distribuição que você adicionou será exibido na lista de pontos de distribuição na seção **Pontos de distribuição**.

9. Execute o utilitário klnagchk para verificar se a conexão com o Kaspersky Security Center foi configurada com êxito. No prompt de comando, execute:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```

10. No menu principal, acesse o Kaspersky Security Center e detecte o dispositivo.

11. Na janela aberta, clique em <nome do dispositivo>.

12. Na lista suspensa, selecione o link **Mover para o grupo**.

13. Na janela aberta **Selecionar grupo**, clique no link **Pontos de distribuição**.

14. Clique em **OK**.

15. Reinicie o serviço do Agente de Rede no cliente Linux, executando o seguinte comando no prompt de comando:
    ```
    $ sudo /opt/kaspersky/klnagent64/bin/klnagchk -restart
    ```

A conexão de um dispositivo Linux como gateway na DMZ está concluída.

Depois disso, é possível conectar um dispositivo Linux ao Servidor de Administração pelo gateway de conexão configurado. Siga estes procedimentos somente após concluir o cenário de instalação principal.

Conectando um dispositivo Linux ao Servidor de Administração por meio de um gateway de conexão

Um gateway de conexão permite conectar dispositivos cliente da zona desmilitarizada (DMZ) ao Servidor de Administração. Os dispositivos baseados em Windows e em Linux podem atuar como um gateway de conexão. Depois de conectar e configurar o gateway de conexão, é possível usar esse gateway para conectar um dispositivo Linux ao Servidor de Administração. Siga o procedimento abaixo somente após concluir o cenário de instalação principal.

Para conectar um dispositivo Linux ao Servidor de Administração por meio de um gateway de conexão, execute as seguintes ações neste dispositivo:

1. Baixe e instale o Agente de Rede no dispositivo Linux.

2. Execute o script de pós-instalação do Agente de Rede executando o seguinte comando no prompt de comando:
   ```
   $ sudo /opt/kaspersky/klnagent64/lib/bin/setup/postinstall.pl
   ```

3. Na etapa que solicita o modo do Agente de Rede, escolha a opção **Conectar ao servidor usando um gateway de conexão** e insira o endereço de gateway de conexão.

4. Verifique a conexão com o Kaspersky Security Center e o gateway de conexão, usando o seguinte comando no prompt de comando:
   ```
   $ sudo /opt/kaspersky/klnagent64/bin/klnagchk
   ```
   O endereço do gateway de conexão é exibido na saída.

A conexão de um dispositivo Linux ao Servidor de Administração por meio de um gateway de conexão está concluída. Você pode usar este dispositivo para atualizar a distribuição, para instalação remota de aplicativos e para recuperar informações sobre dispositivos em rede.

Adicionando um gateway de conexão na DMZ como um ponto de distribuição

Um gateway de conexão aguarda por conexões do Servidor de Administração, em vez de estabelecer conexões com o Servidor de Administração. Isso significa que logo após um gateway de conexão ser instalado em um dispositivo na DMZ, o Servidor de Administração não lista o dispositivo entre os dispositivos gerenciados. Portanto, você precisa de um procedimento especial para garantir que o Servidor de Administração inicie uma conexão com o gateway de conexão.

Para adicionar um dispositivo com um gateway de conexão como ponto de distribuição:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.

2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.

3. Na janela de propriedades do Servidor de Administração, selecione a seção **Pontos de distribuição**.

4. Na parte direita da janela, selecione a opção **Atribuir manualmente os pontos de distribuição**.

5. Clique no botão **Adicionar**.

   Isso abre a janela **Adicionar ponto de distribuição**.

6. Na janela **Adicionar ponto de distribuição**, execute as seguintes ações:

   a. Em **Dispositivo para atuar como ponto de distribuição**, clique na seta para baixo no botão **Selecionar** e selecione a opção **Adicionar o gateway de conexão na DMZ por endereço**.

   b. Na janela **Inserir o endereço do gateway de conexão** que se abre, digite o endereço IP do gateway de conexão (ou digite o nome, se o gateway de conexão for acessível por nome).

   c. No **escopo do ponto de distribuição**, clique na seta para baixo no botão **Selecionar**.

   d. Indique os dispositivos específicos aos quais o ponto de distribuição distribuirá as atualizações. Você pode especificar um grupo de administração ou uma descrição da localização da rede.

      Recomendamos que você tenha um grupo separado para dispositivos gerenciados externos.

Após executar essas ações, a lista de pontos de distribuição contém uma nova entrada chamada **Entrada temporária para o gateway de conexão**.

O Servidor de Administração tenta, de forma quase imediata, conectar-se ao gateway de conexão no endereço especificado. Se for bem-sucedido, o nome da entrada muda para o nome do dispositivo de gateway de conexão. Esse processo leva até cinco minutos.

Enquanto a entrada temporária do gateway de conexão está sendo convertida em uma entrada nomeada, o gateway de conexão também aparece no grupo **Dispositivos não atribuídos**.

Para adicionar um gateway de conexão a uma rede configurada anteriormente, reinstale o Agente de Rede nos dispositivos que deseja conectar ao gateway de conexão recém-adicionado.

Atribuir os pontos de distribuição automaticamente

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos.

Para atribuir os pontos de distribuição automaticamente:

1. Abra a janela principal do aplicativo.

2. Na árvore do console, selecione o nó com o nome do Servidor de Administração para o qual você deseja designar pontos de distribuição automaticamente.

3. No menu de contexto do Servidor de Administração, clique **Propriedades**.

4. Na janela de propriedades do Servidor de Administração, no painel **Seções** selecione **Pontos de distribuição**.

5. Na parte direita da janela, selecione a opção **Atribuir automaticamente os pontos de distribuição**.

Se a atribuição automática dos dispositivos para agirem como pontos de distribuição estiver ativada, você não pode configurar manualmente os pontos de distribuição nem editar a lista de pontos de distribuição.

6. Clique em **OK**.

O Servidor de Administração atribui e configura automaticamente os pontos de distribuição.

Sobre a instalação local do Agente de Rede em um dispositivo selecionado como um ponto de distribuição

Para permitir que o dispositivo selecionado como ponto de distribuição se comunique diretamente com o Servidor de Administração virtual para poder atuar como um gateway de conexão, o Agente de Rede deve ser instalado localmente no dispositivo.

O procedimento de instalação local do Agente de Rede no dispositivo definido como um ponto de distribuição é igual à instalação local do Agente de Rede em qualquer dispositivo na rede.

As seguintes condições devem ser atendidas por um dispositivo selecionado como um ponto de distribuição:

- Durante a instalação local do Agente de Rede, especifique o endereço de um Servidor de Administração virtual que gerencia o dispositivo no campo **Endereço do servidor** na janela **Servidor de Administração** do Assistente de instalação. Você poderá usar o endereço IP ou o nome do dispositivo na rede Windows.

  O seguinte formato é usado para o endereço do Servidor virtual: <Endereço completo do Servidor de Administração físico ao qual o Servidor virtual está subordinado>/<Nome do Servidor de Administração virtual>.

- Para que ele possa atuar como um gateway de conexão, abra todas as portas do dispositivo que são necessárias para a comunicação com o Servidor de Administração.

Após a instalação do Agente de Rede no dispositivo com as configurações especificadas, o Kaspersky Security Center executa as seguintes ações automaticamente:

- Inclui este dispositivo no grupo **Dispositivos gerenciados** do Servidor de Administração virtual.
- Atribui este dispositivo como o ponto de distribuição do grupo **Dispositivos gerenciados** do Servidor de Administração virtual.

É necessário e suficiente instalar o Agente de Rede localmente no dispositivo atribuído para atuar como o ponto de distribuição para o grupo **Dispositivos gerenciados** na rede da organização. Você pode instalar o Agente de Rede remotamente em dispositivos que agem como pontos de distribuição nos grupos de administração aninhados. Para fazer isso, use o ponto de distribuição do grupo **Dispositivos gerenciados** como um gateway de conexão.

Sobre usar um ponto de distribuição como um gateway de conexão

Se o Servidor de Administração estiver fora da zona desmilitarizada (DMZ), os Agentes de Rede dessa zona não podem se conectar com o Servidor de Administração.

Ao conectar o Servidor de Administração com Agentes de Rede, você poderá usar um ponto de distribuição como o gateway de conexão. O ponto de distribuição abre uma porta para o Servidor de Administração para a conexão ser criada. Quando o Servidor de Administração for iniciado, ele se conecta com um ponto de distribuição e mantém essa conexão durante toda a sessão.

Após receber um sinal do Servidor de Administração, o ponto de distribuição envia um sinal UDP para os Agentes de Rede para permitir a conexão com o Servidor de Administração. Quando os Agentes de Rede recebem esse sinal, eles se conectam com o ponto de distribuição, o qual transfere a informação entre os Agentes de Rede e o Servidor de Administração. A troca de informações pode ocorrer em uma rede IPv4 ou IPv6.

Recomendamos que você use um dispositivo especialmente atribuído como o gateway de conexão e cubra um máximo de 10.000 dispositivos cliente (incluindo os dispositivos móveis) com este gateway de conexão.

Para adicionar um gateway de conexão a uma rede configurada anteriormente:

1. Instale o Agente de Rede na função de gateway de conexão.
2. Reinstale o Agente de Rede em dispositivos que deseja conectar ao gateway de conexão recém-adicionado.

Adicionar intervalos de IP na lista de intervalos sondados por um ponto de distribuição

É possível adicionar um intervalo de IP na lista de intervalos sondados por um ponto de distribuição.

Para adicionar um intervalo de IP na lista de intervalos sondados:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No menu de contexto do nó selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração que é exibida, selecione a seção **Pontos de distribuição**.
4. Na lista, selecione o ponto de distribuição necessário e clique em **Propriedades**.
5. Na janela de propriedades do ponto de distribuição aberta, no painel esquerdo **Seções**, selecione **Descoberta de dispositivos → Intervalos de IPs**.
6. Marque a caixa de seleção **Ativar a sondagem de intervalos**.
7. Clique no botão **Adicionar**.

   O botão **Adicionar** é ativado somente se você selecionar a caixa de seleção **Ativar a sondagem de intervalos**.

   A janela **Intervalo de IPs** se abre.

8. Na janela **Intervalo de IPs**, insira o nome do novo conjunto de IPs (o nome padrão é Nova faixa).
9. Clique no botão **Adicionar**.
10. Execute uma das seguintes ações:
    - Especifique o conjunto de IPs usando o endereço IP de início e fim.
    - Especifique o conjunto de IPs usando o endereço e a máscara de sub-rede.
    - Clique em **Procurar** e adicione uma sub-rede da lista global de sub-redes.
11. Clique em **OK**.
12. Clique em **OK** para adicionar a nova faixa com o nome especificado.

    O novo intervalo aparecerá na lista de intervalos sondados.

Usando um ponto de distribuição como um servidor push

No Kaspersky Security Center, um ponto de distribuição pode funcionar como um servidor push para os dispositivos gerenciados por meio do protocolo móvel e para os dispositivos gerenciados pelo Agente de Rede. Por exemplo, um servidor push deve ser ativado se você quiser forçar a sincronização dos dispositivos KasperskyOS com o Servidor de Administração. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Se você tiver vários pontos de distribuição atribuídos ao mesmo grupo de administração, poderá ativar o servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

Um servidor push suporta a carga de até 50.000 conexões simultâneas.

É possível querer usar pontos de distribuição como servidores push para garantir que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração. A conectividade contínua é necessária para algumas operações, como executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado ou criar um túnel. Caso um ponto de distribuição seja usado como servidor push, não será necessário usar a opção **Não desconecte do Servidor de Administração** nos dispositivos gerenciados ou enviar pacotes para a porta UDP do agente de rede.

Para usar um ponto de distribuição como servidor push:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No menu de contexto do nó selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração que é exibida, selecione a seção **Pontos de distribuição**.
4. Na lista, selecione o ponto de distribuição necessário e clique em **Propriedades**.
5. Na janela aberta sobre as propriedades do ponto de distribuição, na seção **Geral** à esquerda do painel **Seções**, selecione a opção **Usar este ponto de distribuição como um servidor push**.

6. Especifique o número da porta do servidor push, ou seja, a porta no ponto de distribuição que os dispositivos cliente usarão para conexão.

   Por padrão, a porta 13295 é usada.

7. Clique no botão **OK** para sair da janela de propriedades do ponto de distribuição.

8. Abra a janela de configurações de política do Agente de Rede.

9. Na seção **Conectividade**, vá para a subseção **Rede**.

10. Na subseção **Rede**, selecione a opção **Usar ponto de distribuição para forçar a conexão ao Servidor de Administração**.

11. Clique no botão **OK** para sair da janela.

O ponto de distribuição começará a atuar como um servidor push. Ele pode agora enviar notificações push para dispositivos clientes.

Caso os dispositivos sejam gerenciados com KasperskyOS instalado, ou planeja fazê-lo, é preciso usar um ponto de distribuição como servidor push. Você também pode usar um ponto de distribuição como um servidor push se quiser enviar notificações push para dispositivos cliente.

Outro trabalho de rotina

Esta seção fornece recomendações no trabalho de rotina com o Kaspersky Security Center.

Gerenciamento de Servidores de Administração

Esta seção fornece informações sobre como trabalhar com Servidores de Administração e como configurá-los.

Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário

Você pode adicionar um Servidor de Administração como um Servidor de Administração secundário, portanto, estabelecendo uma hierarquia "principal/secundário". Adicionar um Servidor de Administração secundário é possível mesmo se o Servidor de Administração que você pretende usar como secundário esteja disponível para a conexão através do Console de Administração.

Ao combinar dois Servidores de Administração em uma hierarquia, garanta que a porta 13291 esteja acessível em ambos os Servidores de Administração. A porta 13291 é necessária para receber conexões do Console de Administração ao Servidor de Administração.

Conectando um Servidor de Administração como secundário em referência ao Servidor de Administração principal

Você pode adicionar um Servidor de Administração como secundário ao conectá-lo ao Servidor de Administração principal através da porta 13000. Você precisará de um dispositivo que tenha o Console de Administração instalado e do qual as portas TCP 13291 possam ser acessadas em ambos os Servidores de Administração: suposto Servidor de Administração principal e suposto Servidor de Administração secundário.

Para adicionar como secundário um Servidor de Administração que está disponível para a conexão através do Console de Administração:

1. Assegure-se de que a porta 13000 do suposto Servidor de Administração principal esteja disponível para o recebimento de conexões de Servidores de Administração secundário.

2. Use o Console de Administração para conectar-se ao Servidor de Administração principal.

3. Selecione o grupo de administração ao qual você pretende adicionar o Servidor de Administração secundário.

4. No espaço de trabalho do nó **Servidores de Administração** do grupo selecionado, clique no link **Adicionar Servidor de Administração secundário**.

   O assistente para Adicionar Servidor de Administração secundário é iniciado.

5. Na primeira etapa do assistente (inserir o endereço do Servidor de Administração adicionado ao grupo), insira o nome da rede do suposto Servidor de Administração secundário.

6. Siga as instruções do Assistente.

A hierarquia "principal/secundário" é construída. O Servidor de Administração secundário receberá a conexão do Servidor de Administração principal.

Se você não tiver um dispositivo que tenha o Console de Administração instalado a partir do qual as portas TCP 13291 podem ser acessadas em ambos os Servidores de Administração (se, por exemplo, o suposto Servidor de Administração secundário estiver localizado em um escritório remoto e o administrador do sistema daquele escritório não pode abrir o acesso à Internet para acessar a porta 13291 para motivos de segurança), ainda será capaz de adicionar um Servidor de Administração secundário.

Para adicionar como secundário um Servidor de Administração que não está disponível para a conexão através do Console de Administração:

1. Assegure-se de que a porta 13000 do suposto Servidor de Administração principal esteja disponível para conexão a partir dos Servidores de Administração secundários.

2. Grave o arquivo do certificado do Servidor de Administração principal suporto em um dispositivo externo, tal como um flash drive, ou o envie ao administrador do sistema do escritório remoto onde o Servidor de Administração estiver localizado.

   O arquivo de certificado do Servidor de Administração está no mesmo Servidor de Administração, em %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

3. Grave o arquivo do certificado do suposto Servidor de Administração secundário em um dispositivo externo, tal como um flash drive. Se o suposto Servidor de Administração secundário estiver localizado em um escritório remoto, contate o administrador do sistema daquele escritório para solicitar-lhe que lhe envie o certificado.

   O arquivo de certificado do Servidor de Administração está no mesmo Servidor de Administração, em %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

4. Use o Console de Administração para conectar-se ao Servidor de Administração principal.

5. Selecione o grupo de administração ao qual você pretende adicionar o Servidor de Administração secundário.

6. No espaço de trabalho do nó **Servidores de Administração**, clique no link **Adicionar Servidor de Administração secundário**.

   O assistente para Adicionar Servidor de Administração secundário é iniciado.

7. Na primeira etapa do assistente (inserir o endereço), deixe o espaço do campo **Endereço do Servidor de Administração secundário (opcional)** em branco.

8. Na janela **Arquivo de certificado do Servidor de Administração secundário**, clique no botão **Procurar** e selecione o arquivo do certificado do Servidor de Administração secundário que você salvou.

9. Quando o assistente for concluído, use uma instância diferente do Console de Administração para conectar-se ao suposto Servidor de Administração secundário. Se este Servidor de Administração estiver localizado em um escritório remoto, contate o administrador do sistema do escritório para solicitar-lhe conectar-se ao suposto Servidor de Administração secundário e executar etapas além disso devidas.

10. No menu de contexto do nó do **Servidor de Administração**, selecione **Propriedades**.

11. Nas propriedades do Servidor de Administração, prossiga à seção **Avançado** e, a seguir, para a subseção **Hierarquia de Servidores de Administração**.

12. Marque a caixa de seleção **Esse Servidor de Administração é secundário na hierarquia**.

    Os campos de entrada se tornam disponíveis para a entrada e edição de dados.

13. No campo **Endereço do Servidor de Administração principal**, insira o nome da rede do Servidor de Administração principal futuro.

14. Selecione o arquivo com o certificado do suposto Servidor de Administração principal anteriormente salvo ao clicar no botão **Procurar**.

15. Clique em **OK**.

A hierarquia "principal/secundário" é construída. Você pode conectar-se ao Servidor de Administração secundário através do Console de Administração. O Servidor de Administração secundário receberá a conexão do Servidor de Administração principal.

Conectando o Servidor de Administração principal a um Servidor de Administração secundário

Você pode adicionar um novo Servidor de administração como secundário para que o Servidor de Administração principal se conecte ao Servidor de Administração secundário via porta 13000. Isto é recomendável se, por exemplo, você colocar um Servidor de Administração secundário na DMZ.

Você precisará de um dispositivo que tenha o Console de Administração instalado e do qual as portas TCP 13291 possam ser acessadas em ambos os Servidores de Administração: suposto Servidor de Administração principal e suposto Servidor de Administração secundário.

Para adicionar um novo Servidor de Administração como secundário e conectar o Servidor de Administração principal através da porta 13000:

1. Assegure-se de que a porta 13000 do suposto Servidor de Administração secundário esteja disponível para o recebimento de conexões de Servidores de Administração principal.

2. Use o Console de Administração para conectar-se ao Servidor de Administração principal.

3. Selecione o grupo de administração ao qual você pretende adicionar o Servidor de Administração secundário.

4. No espaço de trabalho do nó **Servidores de Administração** do grupo de administração relevante, clique no link **Adicionar Servidor de Administração secundário**.

   O assistente para Adicionar Servidor de Administração secundário é iniciado.

5. Na primeira etapa do assistente (inserir o endereço do Servidor de Administração sendo adicionado ao grupo), insira o nome da rede do suposto Servidor de Administração secundário e selecione a caixa de seleção **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ**.

6. Se você se conectar ao suposto Servidor de Administração secundário usando um servidor proxy, na primeira etapa do assistente, selecione a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão.

7. Siga as instruções do Assistente.

A hierarquia de Servidores de Administração é criada. O Servidor de Administração secundário receberá a conexão do Servidor de Administração principal.

Conexão a um Servidor de Administração e troca entre Servidores de Administração

Depois de o Kaspersky Security Center ser iniciado, ele tenta se conectar a um Servidor de Administração. Se vários Servidores de Administração estiverem disponíveis na rede, o aplicativo solicita aquele que estava conectado durante a sessão anterior do Kaspersky Security Center.

> Quando o aplicativo é iniciado pela primeira vez após a instalação, ele tenta se conectar com o Servidor de Administração que foi especificado durante a instalação do Kaspersky Security Center.

Após a conexão a um Servidor de Administração, a árvore de pastas desse Servidor é exibida na árvore do console.

Se vários Servidores de Administração tiverem sido adicionados à árvore do console, você pode alternar entre os mesmos.

O Console de Administração é necessário para o trabalho com cada Servidor de Administração. Antes da primeira conexão a um novo Servidor de Administração, assegure-se de que a porta 13291, que recebe conexões do Console de Administração, esteja aberta, assim como todas as portas remanescentes necessárias para a comunicação entre o Servidor de Administração e outros componentes do Kaspersky Security Center.

Para alternar para outro Servidor de Administração:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.

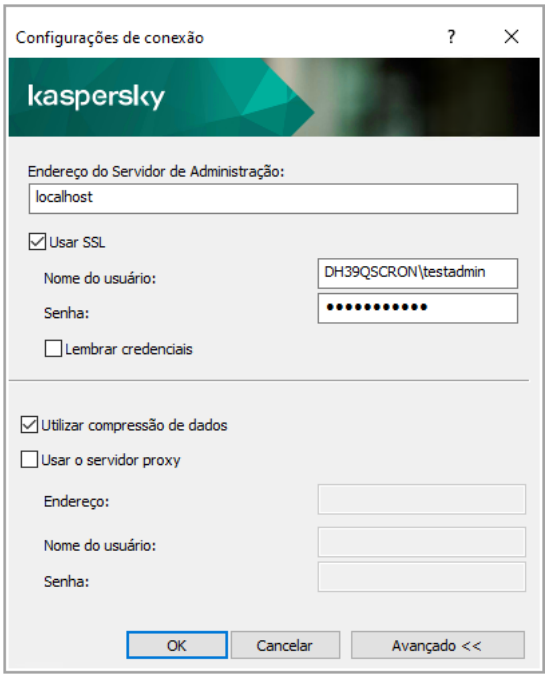
2. No menu de contexto do nó selecione **Conectar-se ao Servidor de Administração**.

3. Na janela **Configurações de conexão** que se abre, no campo **Endereço do Servidor de Administração**, especifique o nome do Servidor de Administração ao qual você deseja se conectar. Você pode especificar um endereço IP ou o nome de um dispositivo em uma rede Windows como o nome do Servidor de Administração. Você pode clicar no botão **Avançado** para configurar a conexão ao Servidor de Administração (veja a figura abaixo).

   Para se conectar-se com o Servidor de Administração através de uma porta diferente da porta padrão, insira um valor no campo **Endereço do Servidor de Administração** no formato <nome do Servidor de Administração>:<Porta>.

   Para se conectar com um Servidor de Administração virtual, insira um valor no campo **Endereço do Servidor de Administração** no formato <endereço do Servidor de Administração>/<nome do servidor virtual>.

   > Os usuários sem direitos de **Leitura** terão acesso negado ao Servidor de Administração.



Conexão ao Servidor de Administração

4. Clique no botão **OK** para concluir a troca entre Servidores.

   Depois de o Servidor de Administração estar conectado, a árvore de pastas do respectivo nó na árvore do console é atualizada.

Condições de conexão a um Servidor de Administração pela Internet

Se um Servidor de Administração estiver localizado remotamente fora de uma rede corporativa, os dispositivos cliente podem se conectar ao mesmo através da Internet.

Para os dispositivos se conectarem a um Servidor de Administração por meio da Internet, as seguintes condições precisam ser atendidas:

- O Servidor de Administração remoto deve ter um endereço IP externo e a porta de entrada 13000 deve permanecer aberta (para a conexão de Agentes de Rede). Recomendamos que você também abra a porta UDP 13000 (para receber notificações do desligamento do dispositivo).
- Os Agentes de Rede devem ser instalados nos dispositivos.

- Ao instalar o Agente de Rede em dispositivos, você deverá especificar o endereço IP externo do Servidor de Administração remoto. Se para a instalação for usado um pacote de instalação, o endereço IP externo deve ser especificado manualmente nas propriedades do pacote de instalação na seção **Configurações**.

- Para usar o Servidor de Administração para gerenciar aplicativos e tarefas para um dispositivo, na janela de propriedades desse dispositivo na seção **Geral**, selecione a caixa de seleção **Não desconectar do Servidor de Administração**. Após a caixa de seleção ter sido selecionada, aguarde até o Servidor de Administração esteja sincronizado com o dispositivo remoto. O número de dispositivos cliente mantendo uma conexão contínua com um Servidor de Administração não pode exceder 300.

Para aumentar o desempenho de tarefas iniciadas por um Servidor de Administração remoto, você pode abrir a porta 15000 em um dispositivo. Neste caso, para executar uma tarefa, o Servidor de Administração envia um pacote especial ao Agente de Rede através da porta 15000 sem esperar pela conclusão da sincronização com o dispositivo.

Conexão criptografado a um Servidor de Administração

A troca de dados entre os dispositivos cliente e o Servidor de Administração, assim como a conexão do Console de Administração ao Servidor de Administração pode ser executada usando o protocolo TLS (Transport Layer Security). O protocolo TLS permite a identificação de partes interagentes, codificação de dados que são transferidos e proteção destes contra modificação durante a transferência. O protocolo TLS usa chaves públicas para autenticar as partes que interagem e os dados criptografados.

Autenticar o Servidor de Administração quando um dispositivo for conectado

Quando um dispositivo cliente se conecta com o Servidor de Administração pela primeira vez, o Agente de Rede no dispositivo baixa uma cópia do certificado do Servidor de Administração e o armazena localmente.

> Se você instalar o Agente de Rede em um dispositivo localmente, poderá selecionar o certificado do Servidor de Administração manualmente.

A cópia baixada do certificado é usada para verificar os direitos e permissões do Servidor de Administração durante conexões subsequentes.

Durante sessões futuras, o Agente de Rede solicita o certificado do Servidor de Administração em cada conexão do dispositivo ao Servidor de Administração e o compara com a cópia local. Se as cópias não coincidirem, o dispositivo não terá a permissão para acessar o Servidor de administração.

Autenticação do Servidor de Administração durante a conexão do Console de Administração

Na primeira conexão ao Servidor de Administração, o Console de Administração solicita o certificado do Servidor de Administração e o salva localmente na estação de trabalho do administrador. Em seguida, sempre que o Console de Administração tenta se conectar a este Servidor de Administração, o Servidor de Administração é identificado com base na cópia do certificado.

Se o certificado do Servidor de Administração não corresponder à cópia armazenada na estação de trabalho do administrador, o Console de Administração solicita que você confirme a conexão ao Servidor de Administração com o nome especificado e baixar um novo certificado. Após a conexão estar estabelecida, o Console de Administração salva uma cópia do novo certificado do Servidor de Administração, a qual será usada para identificar futuramente o Servidor de Administração.

Configuração de uma lista de permissão de endereços IP para conexão ao Servidor de Administração

Por padrão, os usuários podem fazer login no Kaspersky Security Center em qualquer dispositivo onde possam abrir o Kaspersky Security Center Web Console (também chamado de Web Console) ou onde o Console de Administração baseado em MMC esteja instalado. No entanto, é possível configurar o Servidor de Administração para que os usuários possam se conectar a ele apenas a partir de dispositivos com endereços IP permitidos. Nesse caso, mesmo que um invasor roube uma conta do Kaspersky Security Center, ele não poderá fazer login no Kaspersky Security Center porque o endereço IP do dispositivo do invasor não está na lista de permissão.

O endereço IP é verificado quando um usuário faz login no Kaspersky Security Center ou executa um aplicativo que interage com o Servidor de Administração via Kaspersky Security Center OpenAPI. Neste momento, o dispositivo de um usuário tenta estabelecer uma conexão com o Servidor de Administração. Caso o endereço IP do dispositivo não esteja na lista de permissão, ocorrerá um erro de autenticação e o evento KLAUD_EV_SERVERCONNECT notifica que uma conexão com o Servidor de Administração não foi estabelecida.

Requisitos para uma lista de permissão de endereços IP

Os endereços IP são verificados apenas quando os seguintes aplicativos tentam se conectar ao Servidor de Administração:

- Web Console Server

  Se você entrar no Web Console em um dispositivo e o Web Console Server estiver instalado em outro dispositivo, você pode configurar um firewall no dispositivo em que o Web Console Server está instalado usando os meios padrão do sistema operacional. Então, se alguém tentar fazer login no Web Console, um firewall ajudará a impedir a interferência de invasores.

- Console de Administração
- Aplicativos com interação com o Servidor de Administração por meio de objetos de automação klakaut
- Aplicativos que interagem com o Servidor de Administração via OpenAPI, como Kaspersky Anti Targeted Attack Platform ou Kaspersky Security for Virtualization

Portanto, especifique os endereços dos dispositivos nos quais os aplicativos listados acima estão instalados.

É possível definir os endereços IPv4 e IPv6. Não é possível especificar os intervalos de endereços IP.

Como estabelecer uma lista de permissão de endereços IP

Caso não tenha definido uma lista de permissão anteriormente, siga as instruções abaixo.

Para estabelecer uma lista de permissão de endereços IP para fazer login no Kaspersky Security Center:

1. No dispositivo do Servidor de Administração, execute o prompt de comando do Windows em uma conta com direitos de administrador.
2. Altere o diretório atual para a pasta de instalação do Kaspersky Security Center (geralmente, <Unidade>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Digite o seguinte comando, usando direitos de administrador:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<endereços IP>" -t s`

   Especifique os endereços IP que atendem aos requisitos listados acima. Muitos endereços IP devem ser separados por um ponto e vírgula.

   Exemplo de como permitir que apenas um dispositivo se conecte ao Servidor de Administração:

   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0" -t s`

   Exemplo de como permitir que vários dispositivos se conectem ao Servidor de Administração:

   `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. Reinicie o serviço do Servidor de Administração.

É possível descobrir se a configuração da lista de permissão de endereços IP teve êxito no Log de Eventos Kaspersky do Servidor de Administração.

Como alterar uma lista de permissão de endereços IP

É possível alterar uma lista de permissão exatamente como foi feito na primeira vez. Para isso, execute o mesmo comando e especifique uma nova lista de permissão:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "<endereços IP>" -t s
```

Caso queira excluir alguns endereços IP da lista de permissão, basta reescrevê-los. Por exemplo, a lista de permissão inclui os seguintes endereços IP: 192.0.2.0; 198.51.100.0; 203.0.113.0. O usuário deseja excluir o endereço IP 198.51.100.0. Para fazer isso Digite o seguinte comando no prompt de comando:

```
klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "192.0.2.0; 203.0.113.0" -t s
```

Não se esqueça de reiniciar o serviço do Servidor de Administração.

Como redefinir uma lista de permissão de endereços IP configurada

Para redefinir uma lista de permissão de endereços IP já configurada:

1. Digite o seguinte comando no prompt de comando do Windows, usando direitos de administrador:
   `klscflag -fset -pv klserver -n KLSRV_FLAG_ALLOWED_IP_ADDRESSES_FOR_GUI -v "" -t s`

2. Reinicie o serviço do Servidor de Administração.

Depois disso, os endereços IP não serão mais verificados.

Usar o utilitário klscflag para fechar a porta 13291

A porta 13291 do Servidor de Administração é usada para receber conexões dos Consoles de Administração. Esta porta é selecionada por padrão. Se não quiser usar o Console de Administração baseado em MMC ou o utilitário klakaut, é possível fechar essa porta usando o utilitário klscflag. Este utilitário altera o valor do parâmetro KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN.

Para fechar a porta 13291:

1. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

2. Execute o seguinte comando na linha de 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. Reinicie o serviço do Servidor de Administração do Kaspersky Security Center.

   A porta 13291 é fechada.

Para verificar se a porta 13291 foi fechada com êxito:

Execute o seguinte comando na linha de comando:

```
klscflag -ssvget -pv klserver -s 87 -n KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN -svt BOOL_T -ss "|ss_type = \"SS_SETTINGS\";"
```

Este comando retorna o seguinte resultado:

```
+--- (PARAMS_T)
+---KLSRV_SP_SERVER_SSL_PORT_GUI_OPEN = (BOOL_T)false
```

O valor `false` significa que a porta está fechada. Caso contrário, o valor `true` é exibido.

Desconexão de um Servidor de Administração

Para desconectar de um Servidor de Administração:

1. Na árvore do console, selecione o nó correspondente ao Servidor de Administração que você deseja desconectar.

2. No menu de contexto do nó selecione **Desconectar do Servidor de Administração**.

Adição de um Servidor de Administração à árvore do console

Para adicionar um Servidor de Administração à árvore do console:

1. Na janela principal do Kaspersky Security Center, na árvore do console, selecione o nó **Kaspersky Security Center**.

2. No menu de contexto do nó, selecione **Novo → Servidor de Administração**.

   Um nó com o nome **Servidor de Administração - <Nome do dispositivo> (Não conectado)** será criado na árvore do console, a partir da qual você será capaz de se conectar a qualquer um dos Servidores de Administração instalados na rede.

Remoção de um Servidor de Administração da árvore do console

Para remover um Servidor de Administração da árvore do console:

1. Na árvore do console, selecione o nó correspondente ao Servidor de Administração que você deseja remover.
2. No menu de contexto do nó, selecione **Remover**.

Adição de um Servidor de Administração virtual à árvore do console

Para adicionar um Servidor de Administração virtual à árvore do console:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração para o qual você deseja criar um Servidor de Administração virtual.
2. No nó do Servidor de Administração, selecione a pasta **Servidores de Administração**.
3. No espaço de trabalho da pasta **Servidores de Administração**, clique no link **Adicionar Servidor de Administração virtual**.

   O Assistente de Assistente de novo Servidor de Administração virtual é iniciado.
4. Na janela **Nome do Servidor de Administração virtual**, especifique o nome do Servidor de Administração virtual a ser criado.

   O nome de um Servidor de Administração virtual não pode conter mais de 255 caracteres e não pode incluir nenhum caractere especial (tal como *<>?:\"|).
5. Na janela **Insira o endereço para conectar o dispositivo ao Servidor de Administração virtual**, especifique o endereço de conexão do dispositivo

   O endereço de conexão de um Servidor de Administração virtual é o endereço da rede através do qual os dispositivos se conectarão àquele Servidor. O endereço de conexão tem duas partes: o endereço da rede de um Servidor de Administração físico e o nome de um Servidor de Administração virtual, separado por uma barra. O nome do Servidor de Administração virtual será substituído automaticamente. O endereço especificado será usado no Servidor de Administração virtual como o endereço padrão em pacotes de instalação de Agente de Rede.
6. Na janela **Criar a conta do administrador do Servidor de Administração virtual**, atribua um usuário da lista para agir como um Servidor de Administração virtual ou adicione uma nova conta de administrador ao clicar no botão **Criar**.

   Você pode especificar múltiplas contas.

Um nó denominado **Servidor de Administração <Nome do Servidor de Administração virtual>** é criado na árvore do console.

Alteração de uma conta de serviço do Servidor de Administração. Utilitário klsrvswch

Se você precisa alterar a conta de serviço do Servidor de Administração que foi definida durante a instalação do Kaspersky Security Center, poderá usar um utilitário com o nome klsrvswch que é concebido para alterar a conta do Servidor de Administração.

Ao instalar o Kaspersky Security Center, o utilitário é copiado automaticamente para a pasta de instalação do aplicativo.

O número de inicializações do utilitário é, essencialmente, ilimitado.

É necessário iniciar o utilitário klsrvswch no dispositivo do Servidor de Administração com a conta com direitos administrativos que foi usada para instalar o Servidor de Administração.

O utilitário klsrvswch permite modificar o tipo de conta. Por exemplo, se você usa uma conta local, poderá modificá-la para uma conta de domínio ou para uma conta de serviço gerenciado (e vice-versa). O utilitário klsrvswch não permite alterar o tipo de conta para conta de serviço gerenciado de grupo (gMSA).

O Windows Vista e as versões posteriores do Windows não permitem o uso da LocalSystem Account para o Servidor de Administração. Nessas versões de Windows, a opção **LocalSystem Account** está inativa.

Para alterar uma conta de serviço do Servidor de Administração para uma conta de domínio:

1. Inicie o utilitário klsrvswch da pasta de instalação do Kaspersky Security Center. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Esta ação também inicia o Assistente para a modificação da conta de serviço do Servidor de Administração. Siga as instruções do Assistente.

2. A janela **Conta de serviço do Servidor de Administração**, selecione **Conta do LocalSystem**.

   Após a conclusão do Assistente, a conta do Servidor de Administração é alterada. O serviço do Servidor de Administração será iniciado com a *Conta do Local System* e usará suas credenciais.

A operação correta do Kaspersky Security Center requer que a conta usada para iniciar o serviço do Servidor de Administração tenha os direitos de administrador para o recurso onde o banco de dados do Servidor de Administração estiver hospedado.

Para alterar uma conta de serviço do Servidor de Administração para uma conta de usuário ou uma conta de serviço gerenciada:

1. Inicie o utilitário klsrvswch da pasta de instalação do Kaspersky Security Center. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   Esta ação também inicia o Assistente para a modificação da conta de serviço do Servidor de Administração. Siga as instruções do Assistente.

2. A janela **Conta de serviço do Servidor de Administração**, selecione **Conta personalizada**.

3. Clique no botão **Encontrar agora**.

   A janela **Selecionar usuário** é exibida.

4. Na janela **Selecionar usuário**, clique no botão **Tipos de objeto**.

5. Na lista de tipos de objeto, selecione **Usuários** (se você quiser uma conta de usuário) ou **Service Accounts** (se quiser uma conta de serviço gerenciada) e clique em **OK**.

6. No campo do nome do objeto, digite o nome da conta ou parte do nome, e clique em **Verificar Nomes**.

7. Na lista dos nomes correspondentes, selecione o nome necessário e clique em **OK**.

8. Se você selecionou **Contas de serviço**, na janela **Senha de conta**, deixe os campos **Senha** e **Confirmar senha** em branco. Se você selecionou **Usuários**, digite uma nova senha do usuário e confirme-a.

A conta de serviço do Servidor de Administração será alterado para a conta que você selecionou.

Quando o Microsoft SQL Server for usado em um modo que pressupõe a autenticação das contas de usuário com as ferramentas do Windows, o acesso ao banco de dados deve ser concedido. O usuário deve ter o status de proprietário do banco de dados do Kaspersky Security Center. O esquema dbo é usado por predefinição.

Alterando credenciais de DBMS

Você pode precisar alterar as credenciais do DBMS, por exemplo, para realizar a rotatividade de credenciais para fins de segurança.

Para alterar as credenciais do DBMS em um ambiente Linux usando o utilitário klsrvconfig:

1. Execute o utilitário klbackup localizado na pasta de instalação do Kaspersky Security Center. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

   É necessário iniciar o utilitário klsrvswch no dispositivo do Servidor de Administração com a conta com direitos administrativos que foi usada para instalar o Servidor de Administração.

2. Clique no botão **Avançar** do assistente até chegar na etapa **Alterar as credenciais de acesso ao DBMS**.

3. No passo **Alterar as credenciais de acesso ao DBMS** do assistente, desempenhe o seguinte:

   A etapa **Alterar as credenciais de acesso ao DBMS** do assistente será ignorada se a autenticação do Windows for usada.

   - Selecione a opção **Aplicar novas credenciais**.
   - Especifique um novo nome de conta no campo **Conta**.
   - Especifique uma nova senha para uma conta no campo **Senha**.
   - Especifique a nova senha no campo **Confirmar senha**.

   Você deve especificar as credenciais de uma conta que existe no DBMS.

4. Clique no botão **Avançar**.

Após a conclusão do assistente, as credenciais do DBMS são alteradas.

O utilitário klsrvswch só pode ser usado para alterar a senha da conta para autenticação SQL. O sistema não comporta alteração do método de autorização. Para alterar o método de autorização, reinstale o Servidor de Administração e especifique as configurações desejadas.

Resolução de problemas com nós do Servidor de Administração

A árvore do console no painel esquerdo do Console de Administração contém nós de Servidores de Administração. Você pode adicionar quantos Servidores de Administração precisar à árvore do console.

A lista de nós do Servidor de Administração na árvore do console é armazenada em uma cópia sombra de um arquivo .msc por meio do Console de Gerenciamento Microsoft. A cópia sombra desse arquivo está localizada na pasta %USERPROFILE%\AppData\Roaming\Microsoft\MMC\ no dispositivo em que o Console de Administração está instalado. Para cada nó do Servidor de Administração, o arquivo contém as seguintes informações:

- Administration Server address
- Número da porta
- Se o TLS é usado

  Este parâmetro depende do número da porta usado para conectar o Console de Administração ao Servidor de Administração.
- Nome de usuário
- Certificado do Servidor de Administração

Solução de problemas

Quando o Console de Administração é conectado ao Servidor de Administração, o certificado armazenado localmente é comparado com o certificado do Servidor de Administração. Se os certificados não corresponderem, o Console de Administração gerará um erro. Por exemplo, uma discrepância de certificado pode ocorrer quando você substitui o certificado do Servidor de Administração. Nesse caso, recrie o nó do Servidor de Administração no console.

Para recriar o nó de um Servidor de Administração:

1. Feche a janela do Console de Administração do Kaspersky Security Center.
2. Exclua o arquivo Kaspersky Security Center 14.2 em %USERPROFILE%\AppData\Roaming\Microsoft\MMC\.
3. Execute o Console de Administração do Kaspersky Security Center.

   Você será solicitado a se conectar ao Servidor de Administração e aceitar o certificado existente.
4. Execute uma das seguintes ações:

   - Aceite o certificado existente clicando no botão **Sim**.
   - Para especificar o seu certificado, clique no botão **Não** e procure arquivo do certificado a ser usado para autenticar o Servidor de Administração.

O problema do certificado está resolvido. Você pode usar o Console de Administração para conectar-se ao Servidor de Administração.

Visualização e modificação das configurações de um Servidor de Administração

Você pode ajustar as configurações de um Servidor de Administração na janela de propriedades deste Servidor.

Para abrir as Propriedades: janela Servidor de Administração,

Selecione **Propriedades** no menu de contexto do nó do Servidor de Administração na árvore do console.

Ajuste das configurações gerais de um Servidor de Administração

Você pode ajustar as configurações gerais do Servidor de Administração nas seções **Geral**, **Configurações de conexão do Servidor de Administração**, **Repositório de eventos** e **Segurança** na janela Propriedades do Servidor de Administração.

A seção **Segurança** pode não é exibida nas propriedades do Servidor de Administração se a exibição tiver sido desativada na interface do Console de Administração.

*Para ativar a exibição da seção **Segurança** no Console de Administração:*

1. Na árvore do console, selecione o nó do Servidor de Administração que você deseja.
2. No menu **Exibir** da janela principal do aplicativo, selecione **Configurar a interface**.
3. Na janela **Configurar a interface** que se abre, selecione a caixa de seleção **Exibir as seções das configurações de segurança** e clique em **OK**.
4. Na janela com a mensagem do aplicativo, clique em **OK**.

A seção **Segurança** será exibida na janela de propriedades do Servidor de Administração.

Configurações de interface do Console de Administração

Você pode ajustar as configurações da interface do Console de Administração para exibir ou ocultar os controles da interface do usuário relacionados aos seguintes recursos:

- Gerenciamento de patches e vulnerabilidades
- Criptografia e proteção de dados
- Configurações de controle de Endpoints
- Gerenciamento de Dispositivos Móveis
- Servidores de Administração secundários
- Seções de Configurações de segurança

Para definir as configurações da interface do Console de Administração:

1. Na árvore do console, selecione o nó do Servidor de Administração que você deseja.
2. No menu **Exibir** da janela principal do aplicativo, selecione **Configurar a interface**.
3. Na janela **Configurar a interface** que é aberta, marque as caixas de seleção próximas aos recursos que você deseja exibir e clique em **OK**.
4. Na janela com a mensagem do aplicativo, clique em **OK**.

Os recursos selecionados serão exibidos na interface do Console de Administração.

Processamento e armazenamento do evento no Servidor de Administração

As informações sobre eventos durante a operação do aplicativo gerenciado e de dispositivos gerenciados são salvas no banco de dados do Servidor de Administração. Cada evento é atribuído a um determinado tipo e nível de gravidade (*Evento crítico*, *Falha funcional*, *Advertência* ou *Informativo*). Dependendo das condições sob as quais um evento ocorreu, o aplicativo pode atribuir diferentes níveis de gravidade aos eventos do mesmo tipo.

Você pode visualizar os tipos e níveis de gravidade atribuídos aos eventos na seção **Configuração do evento** da janela Propriedades do Servidor de Administração. Na seção **Configuração do evento**, você também poderá configurar o processamento de cada evento pelo Servidor de Administração:

- O registro de eventos no Servidor de Administração e nos registros de evento do sistema operacional em um dispositivo cliente e no Servidor de Administração.
- Método usado para notificar o administrador sobre um evento (por exemplo, um SMS ou mensagem de e-mail).

Na seção **Repositório de eventos** da janela Propriedades do Servidor de Administração, você pode editar as configurações de armazenamento do evento no banco de dados do Servidor de Administração ao limitar o número de registros de evento ou o tempo de armazenamento do registro. Quando você especifica o número máximo de eventos, o aplicativo calcula um volume aproximado do espaço de armazenamento necessário para o número especificado. Você pode usar esse cálculo aproximado para avaliar se você tem espaço livre suficiente no disco para evitar sobrecarga do banco de dados. A capacidade padrão do banco de dados do Servidor de Administração é de 400.000 eventos. A capacidade máxima recomendada do banco de dados é de 45 milhões de eventos.

O aplicativo verifica o banco de dados a cada 10 minutos. Caso o número de eventos atinja o valor máximo especificado em mais de 10.000, o aplicativo exclui os eventos mais antigos para que apenas o número máximo de eventos especificado permaneça.

Quando o Servidor de Administração exclui eventos antigos, não pode salvar novos eventos no banco de dados. Durante esse período de tempo, as informações sobre eventos rejeitados são gravadas no Log de Eventos Kaspersky. Os novos eventos são colocados em fila e salvos no banco de dados depois que a operação de exclusão é concluída.

É possível alterar as configurações de qualquer tarefa para salvar eventos relacionados ao andamento da tarefa ou salvar apenas os resultados de execução da tarefa. Ao fazer isso, você reduzirá o número de eventos no banco de dados, aumentará a velocidade da execução dos cenários associados com a análise da tabela de eventos no banco de dados e abaixará o risco de que os eventos críticos sejam substituídos por um grande número de eventos.

Visualização do registro das conexões com o Servidor de Administração

O histórico das conexões e tentativas de conexão ao Servidor de Administração durante a operação pode ser salvo em um arquivo de registro. As informações no arquivo permitem rastrear não só as conexões na infraestrutura da rede, mas também as tentativas não autorizadas de acessar o Servidor de Administração.

Para registrar eventos da conexão ao Servidor de Administração:

1. Na árvore do console, selecione o Servidor de Administração para o qual você quer ativar o log de eventos de conexão.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades que se abre, na seção **Configurações de conexão do Servidor de Administração**, selecione a subseção **Portas de conexão**.
4. Ative a opção **Criar log de eventos de conexão do Servidor de Administração**.
5. Clique no botão **OK** para fechar a janela Propriedades do Servidor de Administração.

Todos os eventos adicionais das conexões de entrada com o Servidor de Administração, resultados de autenticação e erros de SSL serão salvos no arquivo %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Controle de ataques de vírus

O Kaspersky Security Center permite que você responda rapidamente a novas ameaças de ataque de vírus. Os riscos de ataques de vírus são avaliados através do monitoramento da atividade de vírus nos dispositivos.

Você pode configurar as regras de avaliação de ameaças de ataques de vírus e ações a serem tomadas caso surja uma ameaça; para fazer isso, use a seção **Surto de vírus** da janela propriedades do Servidor de Administração.

É possível especificar o procedimento de notificação para o evento *Ataque de vírus* na seção **Configuração de eventos** da janela Propriedades do Servidor de Administração, na janela de propriedades do evento *Ataque de vírus*.

O evento *Ataque de vírus* é gerado em caso de detecção de eventos *Objeto malicioso detectado* durante a operação de aplicativos de segurança. Portanto, você deve salvar as informações sobre todos os eventos *Objeto malicioso detectado* no Servidor de Administração para poder reconhecer ataques de vírus.

Você pode especificar as configurações para salvar informações sobre qualquer evento *Objeto malicioso detectado* nas políticas dos aplicativos de segurança.

Ao contar os eventos *Objetos maliciosos detectados*, somente as informações dos dispositivos do Servidor de Administração principal serão levadas em consideração. As informações dos Servidores de Administração secundários não são levadas em consideração. Para cada servidor secundário, as configurações do evento *Ataque de vírus* são configuradas individualmente.

Limitação de tráfego

Para reduzir volumes de tráfego dentro de uma rede, o aplicativo fornece a opção de limitar a velocidade da transferência de dados para um Servidor de Administração a partir de conjuntos de IPs e sub-redes IP especificados.

Você pode criar e configurar regras de limite de tráfego na seção **Tráfego** da janela Propriedades do Servidor de Administração.

Para criar uma regra de limitação de tráfego:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração para o qual você deseja criar uma tarefa de limitação de tráfego.

2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.

3. Na janela de propriedades do Servidor de Administração, selecione a seção **Tráfego**.

4. Clique no botão **Adicionar**.

5. Na janela **Nova regra**, especifique as seguintes configurações:

   Na seção **Intervalo de IPs para limitar o tráfego**, selecione o método que será usado para definir a sub-rede ou o conjunto para o qual a taxa de transferência de dados será limitada e, a seguir, insira os valores das configurações para o método selecionado. Selecione um dos seguintes métodos:

   - **Especificar o conjunto usando endereço e máscara de rede**

     O tráfego é limitado com base nas configurações da sub-rede. Especifique o endereço de sub-rede e a máscara de sub-rede para determinar a faixa na qual o tráfego será limitado.

     Você também pode clicar em **Procurar** para adicionar sub-redes da lista global de sub-redes.

   - **Especificar o conjunto usando os endereços inicial e final**

     O tráfego é limitado com base em uma faixa de endereços IP. Especifique a faixa de endereços IP nos campos de entrada **Inicial** e **Final**.

     Esta opção está marcada por padrão.

   Na seção **Limite de tráfego**, você pode ajustar as seguintes configurações restritivas da taxa de transferência de dados:

   - **Intervalo de tempo**

     Intervalo de tempo durante o qual a restrição de tráfego estará em vigor. Você pode especificar os limites do intervalo de tempo nos campos de entrada.

   - **Limite (KB/s)**

     O total máximo de velocidade de transferência de dados de entrada e de saída do Servidor de Administração. A restrição de tráfego somente será efetiva dentro do intervalo especificado no campo **Intervalo de tempo**.

   - **Limitar tráfego pelo restante de tempo (KB/s)**

     O tráfego será limitado não somente dentro do intervalo especificado no campo **Intervalo de tempo**, mas também em outros momentos.

     Por padrão, esta caixa de seleção está desmarcada. O valor deste campo pode não coincidir com o valor do campo **Limite (KB/s)**.

As regras de limitação de tráfego afetam principalmente a transferência de arquivos. Essas regras não são aplicadas ao tráfego gerado pela sincronização entre o Servidor de Administração e o Agente de Rede, ou entre Servidores de Administração principal e secundário.

Configuração do Servidor da Web

O Servidor da Web foi projetado para publicar pacotes de instalação independentes, perfis MDM do iOS e arquivos da pasta compartilhada.

Você pode definir as configurações para a conexão do Servidor da Web com o Servidor de Administração e configurar um certificado do Servidor da Web na seção **Servidor da Web** da janela Propriedades do Servidor de Administração.

Trabalhar com usuários internos

As contas dos *usuários internos* são destinadas ao uso com os Servidores de Administração virtuais. O Kaspersky Security Center concede direitos de usuários reais a usuários internos do aplicativo.

As contas de usuários internos só são criadas e usadas dentro do Kaspersky Security Center. Os dados sobre os usuários internos não são transferidos para o sistema operacional. O Kaspersky Security Center autentica os usuários internos.

Você pode configurar contas de usuários internos na pasta **Contas de usuário** da árvore do console.

Cópia backup e restauração das configurações do Servidor de Administração

O backup das configurações do Servidor de Administração e de seu banco de dados é executado pela tarefa de backup e com o utilitário klbackup. Uma cópia backup inclui todas as principais configurações e objetos pertencentes ao Servidor de Administração, como certificados, chaves primárias para criptografia de unidades em dispositivos gerenciados, chaves para várias licenças, estrutura de grupos de administração com todo o seu conteúdo, tarefas, políticas etc. Com uma cópia backup, é possível recuperar a operação de um Servidor de Administração o mais rápido possível, gastando de uma dúzia de minutos a algumas horas nisso.

Se nenhuma cópia backup estiver disponível, uma falha pode levar a uma perda irrevogável de certificados e de todas as configurações do Servidor de Administração. Isto exigirá reconfigurar o Kaspersky Security Center do zero e executar a implementação inicial do Agente de Rede novamente na rede da organização. Todas as chaves primárias para a criptografia das unidades em dispositivos gerenciados também serão perdidas, arriscando a perda irrevogável dos dados criptografados nos dispositivos com Kaspersky Endpoint Security. Portanto, não negligencie os backups regulares do Servidor de Administração usando a tarefa de backup padrão.

O Assistente de Início Rápido cria a tarefa de backup para as configurações do Servidor de Administração e o configura para ser executado diariamente, às 4h. As cópias de backup são salvas por padrão na pasta %ALLUSERSPROFILE%\Application Data\KasperskySC.

Se uma instância do Microsoft SQL Server instalado em outro dispositivo for usado como o DBMS, você deve modificar a tarefa de backup especificando um caminho UNC, que está disponível para gravar tanto pelo serviço Servidor de Administração como pelo serviço SQL Server, como a pasta para armazenar as cópias backup. Este requisito deriva de um recurso especial do backup no Microsoft SQL Server DBMS.

Se uma instância local do Microsoft SQL Server for usada como DBMS, também recomendamos salvar as cópias de backup em uma mídia dedicada para assegurar que elas estejam protegidas contra danos, em conjunto com o Servidor de Administração.

Como uma cópia backup contém dados importantes, a tarefa de backup e o utilitário klbackup fornecem a proteção por senha das cópias backup. Por padrão, a tarefa de backup é criada com uma senha em branco. Você deve definir uma senha nas propriedades da tarefa de backup. Negligenciar este requisito causa uma situação em que todas as chaves de certificados do Servidor de Administração, as chaves para as licenças e as chaves primárias para a criptografia de unidades em dispositivos gerenciados permanecem não criptografadas.

Além do backup regular, você também deve criar uma cópia backup antes de cada mudança significativa, incluindo a instalação de atualizações e patches do Servidor de Administração.

Se você usar o Microsoft SQL Server como DBMS, poderá minimizar o tamanho das cópias de backup. Para isso, ative a opção **Compactar o backup** nas configurações do SQL Server.

A restauração de uma cópia backup é executada com o utilitário klbackup em uma instância operável do Servidor de Administração que acaba de ser instalado e que tenha a mesma versão (ou posterior) para o qual a cópia backup foi criada.

A instância do Servidor de Administração no qual a restauração deve ser executada, deve usar um DBMS do mesmo tipo (por exemplo, o mesmo SQL Server ou MariaDB) e a mesma versão ou posterior. A versão do Servidor de Administração pode ser a mesma (com uma correção idêntica ou posterior), ou posterior.

Esta seção descreve os cenários padrão para restaurar as configurações e objetos do Servidor de Administração.

Usar um instantâneo de sistema de arquivos para reduzir a duração do backup

No Kaspersky Security Center 14.2, o tempo ocioso do Servidor de Administração durante o backup foi reduzido ao comparar com versões mais anteriores. Além disso, o recurso **Usar o instantâneo do sistema de arquivos para o backup de dados** foi adicionado às configurações da tarefa. Este recurso fornece a redução ociosa adicional usando o utilitário klbackup, que cria uma cópia sombra do disco durante o backup (isto leva alguns segundos) e simultaneamente copia o banco de dados (isto leva alguns minutos no mais tardar). Quando o klbackup cria uma cópia sombra do disco e uma cópia do banco de dados, o utilitário faz com que o Servidor de Administração esteja novamente conectável.

Você pode usar o recurso de instantâneo do sistema de arquivos somente se estas duas condições forem atendidas:

- A pasta compartilhada do Servidor de Administração e a pasta %ALLUSERSPROFILE%\KasperskyLab estão localizadas no mesmo disco lógico e estão locais em referência ao Servidor de Administração.
- A pasta %ALLUSERSPROFILE%\KasperskyLab não contém nenhum link simbólico que foi criado manualmente.

Não use o recurso se qualquer uma destas condições não puder ser atendida. Neste caso, o aplicativo retornaria uma mensagem de erro em resposta a qualquer tentativa de criar um instantâneo do sistema de arquivos.

Para usar o recurso, você deve ter uma conta à qual concedida a permissão de criar instantâneos do disco lógico que armazena a pasta %ALLUSERSPROFILE%. Observe que a conta de serviço do Servidor de Administração não tem tal permissão.

Para usar o recurso de instantâneo do sistema de arquivos para reduzir a duração do backup:

1. Na seção **Tarefas**, selecione a tarefa de backup.
2. No menu de contexto, selecione **Propriedades**.
3. Na janela de propriedades da tarefa que se abre, selecione a seção **Configurações**.
4. Selecione a caixa de seleção **Usar o instantâneo do sistema de arquivos para o backup dos dados**.

5. Nos campos **Nome de usuário** e **Senha**, insira o nome e a senha de uma conta que tenha a permissão para criar instantâneos do disco lógico que armazena a pasta %ALLUSERSPROFILE%.

6. Clique em **Aplicar**.

Em qualquer inicialização posterior da tarefa de backup, o utilitário klbackup criará instantâneos do sistema de arquivos, portanto reduzindo o tempo ocioso do Servidor de Administração durante a execução da tarefa.

Um dispositivo com o Servidor de Administração está inoperável

Se um dispositivo com o Servidor de Administração estiver inoperável devido a uma falha, você é recomendado a executar as seguintes ações:

- Ao novo Servidor de Administração deve ser atribuído o mesmo endereço: nome NetBIOS, FQDN ou IP estático (dependendo de qual deles foi definido quando os Agentes de Rede foram implementados).

- Instale o Servidor de Administração, usando um DBMS do mesmo tipo ou da mesma (ou posterior) versão. Você pode instalar a mesma versão do Servidor com a mesma (ou posterior) correção ou uma versão posterior. Após a instalação, não execute a configuração inicial por meio do assistente.

- No menu **Iniciar**, execute o utilitário klbackup e execute a restauração.

As configurações do Servidor de Administração ou o do banco de dados estão corrompidas

Se o Servidor de Administração estiver inoperável devido a configurações ou aos bancos de dados corrompidas (p. ex., após uma oscilação de corrente), você é recomendado a usar o seguinte cenário de restauração:

1. Verifique o sistema de arquivos no dispositivo danificado.

2. Desinstale a versão inoperável do Servidor de Administração.

3. Reinstale o Servidor de Administração usando um DBMS do mesmo tipo e da mesma (ou posterior) versão. Você pode instalar a mesma versão do Servidor com a mesma (ou posterior) correção ou uma versão posterior. Após a instalação, não execute a configuração inicial por meio do assistente.

4. No menu **Iniciar**, execute o utilitário klbackup e execute a restauração.

É proibido restaurar o Servidor de Administração usando qualquer outro modo que não seja através do utilitário klbackup.

Qualquer tentativa de restaurar o Servidor de Administração através de software de terceiros levará inevitavelmente a dessincronização dos dados nos nós do aplicativo Kaspersky Security Center distribuído e, consequentemente, ao funcionamento impróprio do aplicativo.

Cópia backup e restauração dos dados do Servidor de Administração

O backup de dados permite mover um Servidor de Administração de um dispositivo para outro, sem perda de dados. Usando o backup, você pode restaurar dados ao mover o banco de dados de um Servidor de Administração para outro dispositivo ou ao atualizar para uma versão mais recente do Kaspersky Security Center. Além disso, é possível usar o backup de dados para mover dados do Servidor de Administração do Kaspersky Security Center Windows sob gerenciamento do Kaspersky Security Center Linux (não há suporte para mover dados do Kaspersky Security Center Linux para o Kaspersky Security Center Windows).

Observe que não é feito backup dos plugins de gerenciamento instalados. Depois de restaurar os dados do Servidor de Administração a partir de uma cópia backup, você precisará fazer download e reinstalar plug-ins para aplicativos gerenciados.

Antes de fazer backup dos dados do Servidor de Administração, verifique se um Servidor de Administração virtual foi adicionado ao grupo de administração. Caso um Servidor de Administração virtual seja adicionado, verifique e confirme se um administrador foi atribuído para esse Servidor de Administração virtual antes do backup. Não é possível conceder ao administrador direitos de acesso ao Servidor de Administração virtual após o backup. Observe que, caso as credenciais da conta do administrador sejam perdidas, não será possível atribuir um novo administrador ao Servidor de Administração virtual.

Você pode criar uma cópia backup dos dados do Servidor de Administração em uma das seguintes formas:

- Criando e executando uma tarefa de backup de dados através do Console de Administração.
- Executando o utilitário klbackup no dispositivo que tenha o Servidor de Administração instalado. Este utilitário está incluído no kit de distribuição do Kaspersky Security Center. Após a instalação do Servidor de Administração, o utilitário estará localizado na raiz da pasta de destino especificada na instalação do aplicativo.

Os seguintes dados são salvos em uma cópia backup do Servidor de Administração:

- O banco de dados do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração).
- Detalhes da configuração da estrutura dos grupos de administração e dispositivos cliente.
- Repositório dos pacotes de distribuição de aplicativos para a instalação remota.
- Certificado do Servidor de Administração.

A recuperação dos dados do Servidor de Administração só é possível usando o utilitário klbackup.

Tarefa de backup de dados do Servidor de Administração

Criação da tarefa de backup de dados do Servidor de Administração

A tarefa de backup é uma tarefa do Servidor de Administração; ele é criado por meio do assistente de início rápido. Se uma tarefa de backup criada pelo Assistente de início rápido tiver sido excluída, você pode criar uma manualmente.

Para criar a tarefa de backup de dados do Servidor de Administração:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Inicie a criação da tarefa em uma das seguintes formas:
   - Selecionando **Novo** → **Tarefa** no menu de contexto da pasta **Tarefas** na árvore do console.
   - Clicando no botão **Criar uma tarefa** no espaço de trabalho.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente. Na janela **Selecionar o tipo de tarefa** do assistente, selecione o tipo de tarefa com nome **Backup de dados do Servidor de Administração**.

A tarefa **Backup de dados do Servidor de Administração** só pode ser criada numa única cópia. Se a tarefa de backup de dados do Servidor de Administração já tiver sido criada para o Servidor de Administração, ela não será exibida na janela de seleção de tipo de tarefa do Assistente de criação da tarefa de backup.

Configurar a tarefa Backup de dados do Servidor de Administração

Depois de criar uma tarefa de backup, é possível definir as configurações da tarefa.

Para configurar a tarefa Backup de dados do Servidor de Administração:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. No menu de contexto da tarefa **Backup de dados do Servidor de Administração**, selecione **Propriedades**.

   A janela de propriedades da tarefa *Backup de dados do Servidor de Administração* é aberta. As seguintes propriedades estão disponíveis:

- **Geral**

  Na seção **Geral**, você pode especificar o nome da tarefa, exibir a data de criação dela, a data do último comando, os status das tarefas iniciadas e os seus resultados.

- **Notificação**

  Na seção **Notificação**, você pode especificar as configurações para armazenar eventos relacionados aos resultados da execução de tarefas, bem como configurar as notificações sobre os resultados da execução da tarefa.

- **Agendamento**

  Na seção **Agendamento**, você pode especificar um agendamento para o início da tarefa.

- **Destino**

  Na seção **Destino**, é possível especificar o caminho para a pasta de armazenamento das cópias backup de dados do Servidor de Administração.

- **Configurações**

  Na seção **Configurações**, é possível definir a senha de proteção de backup e o número de cópias backup, caso seja necessário.

  Você também pode criar uma cópia de sombra do disco lógico que armazena a pasta %ALLUSERSPROFILE% e copiar o banco de dados do Servidor de Administração. Para fazer isso, é necessário ativar a opção **Usar o instantâneo do sistema de arquivo para o backup dos dados** e, em seguida, especificar o nome e a senha de uma conta que tenha permissão para criar instantâneos.

- **Segurança**

  Na seção **Segurança**, é possível conceder permissões a usuários e grupos para a execução de operações no Servidor de Administração. Caso a opção **Herdar configurações do Servidor de Administração** esteja ativada, as configurações de segurança da tarefa serão herdadas do Servidor de Administração.

  Caso esta opção esteja desativada, é possível definir as configurações de segurança para a tarefa. É possível atribuir uma função a um usuário ou grupo de usuários ou atribuir permissões a um usuário ou grupo de usuários, conforme a tarefa necessitar.

  Por padrão, a opção **Herdar configurações do Servidor de Administração** está ativada.

- **Histórico de revisões**

  Na seção **Histórico de revisões**, você pode acompanhar a modificação da tarefa. Sempre que você salva modificações feitas na tarefa, uma revisão é criada.

Utilitário de backup de dados e recuperação (klbackup)

Você copiar os dados do Servidor de Administração para backup e recuperação futura, usando o utilitário klbackup, que está incluído no kit de distribuição do Kaspersky Security Center.

O utilitário klbackup pode ser executado em qualquer um dos seguintes modos:

- Interativo
- Silencioso

Backup de dados e recuperação no modo interativo

A restauração de dados do Servidor de Administração por meio de uma cópia backup criada usando o utilitário klbackup no modo de interação pode ocorrer com um erro. Caso tenha instalado o patch 14.2.0.26967-pf5 ou 14.2.0.48079-pf5 para o Servidor de Administração e, em seguida, criado uma cópia backup usando o utilitário klbackup com a opção **Migrar banco de dados** desativada, ocorrerá um erro na restauração desta cópia (para todos os DBMSs, com exceção do MySQL e do MariaDB). Caso tenha o patch 14.2.0.26967-pf5 para o Servidor de Administração instalado e quiser criar uma cópia de backup sem migrar para outro DBMS, use uma tarefa de backup de dados ou execute o utilitário klbackup por meio da linha de comando.

Para criar uma cópia backup dos dados do Servidor de Administração no modo interativo:

1. Execute o utilitário klbackup localizado na pasta de instalação do Kaspersky Security Center.

   O Assistente de backup e restauração é iniciado.

2. Na primeira janela do assistente, selecione **Executar backup dos dados do Servidor de Administração**.

   Caso selecione a opção **Restaurar ou fazer backup somente do certificado do Servidor de Administração**, apenas uma cópia backup do certificado e chave privada do Servidor de Administração será salva. O backup do certificado e da chave privada do Servidor de Administração pode ser útil ao executar a migração do Servidor de Administração do Kaspersky Security Center Windows para o Servidor de Administração do Kaspersky Security Center Linux. Além disso, é possível migrar dispositivos gerenciados entre os Servidores de Administração do Kaspersky Security Center Windows. Para obter mais informações, consulte Uso do utilitário klbackup para mudar os dispositivos gerenciados sob gerenciamento de outro Servidor de Administração.

   Clique em **Avançar**.

3. Na janela ao lado do assistente, especifique as seguintes opções:

- **Pasta de destino do backup**
- **Migrar banco de dados**

  Ative esta opção se você atualmente armazena dados do Servidor de Administração em um banco de dados do Microsoft SQL Server e precisa migrá-los para um dos seguintes bancos de dados: MySQL ou MariaDB, PostgreSQL ou Postgres Pro, Azure SQL. Por padrão, essa opção está desativada.

  - **Migrar para o formato MySQL/MariaDB**

    Ative essa opção se você usa atualmente o SQL Server como um DBMS para o Servidor de Administração e deseja migrar os dados do SQL Server para o MySQL ou o MariaDB DBMS. O Kaspersky Security Center criará um backup compatível com o MySQL e o MariaDB. Depois disso, é possível restaurar os dados do backup para o MySQL ou o MariaDB.

  - **Migrar para o Postgres**

    Ative essa opção se você usa atualmente o SQL Server como um DBMS para o Servidor de Administração e deseja migrar os dados do SQL Server para o PostgreSQL ou o Postgres Pro DBMS. O Kaspersky Security Center criará um backup compatível com o PostgreSQL e Postgres Pro. Depois disso, é possível restaurar os dados do backup para o PostgreSQL ou Postgres Pro.

    Essa opção só ficará disponível caso você instale o patch 14.2.0.26967-pf5 para o Servidor de Administração que permita a migração para o PostgreSQL e Postgres Pro. Se você usa o Kaspersky Secure Mobility Management baseado no Kaspersky Security Center Windows 14.2, use o patch 14.2.0.48079-pf5. Entre em contato com o Suporte Técnico da Kaspersky para obter esse patch.

  - **Migrar para o formato do Azure**

    Ative essa opção se você usa atualmente o SQL Server como um DBMS para o Servidor de Administração e deseja migrar os dados do SQL Server para o Azure SQL DBMS. O Kaspersky Security Center criará um backup compatível com o Azure SQL. Depois disso, é possível restaurar os dados do backup para o Azure SQL.

- **Incluir data e hora atual no nome da pasta de destino de backup**
- **Senha para backup**

4. Clique no botão **Avançar** para iniciar o backup.

5. Se você estiver trabalhando com um banco de dados em um detecção, tal como o Amazon Web Services (AWS) ou o Microsoft Azure, na janela **Entrar no Armazenamento Online**, preencha os seguintes campos:

   - Para o AWS:

     - **Nome do bucket S3**

       O nome do S3 bucket que você criou para o Backup.

     - **ID da chave de acesso**

       Você recebeu o ID da chave (sequência de caracteres alfanuméricos) quando criou a Conta de Usuário do IAM para uso com a instância de armazenamento do S3 bucket.

       O campo está disponível se você selecionou o banco de dados RDS em um S3 bucket.

     - **Chave secreta**

       A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

       Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

       O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

   - Para o Microsoft Azure:

     - **Nome da conta de armazenamento do Azure**

       Você criou o nome da conta de armazenamento do Azure para uso com o Kaspersky Security Center.

     - **ID de assinatura do Azure**

       Você criou a assinatura no portal do Azure.

     - **Senha do Azure**

       Você recebeu a senha quando criou o ID do aplicativo.

       Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

     - **ID do aplicativo Azure**

Você criou este ID do aplicativo no portal do Azure.

É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **Nome do servidor Azure SQL**

  O nome e o grupo do recurso estão disponíveis nas propriedades do Azure SQL Server.

- **Grupo de recursos do servidor Azure SQL**

  O nome e o grupo do recurso estão disponíveis nas propriedades do Azure SQL Server.

- **Chave de acesso ao armazenamento do Azure**

  Disponível nas propriedades da conta de armazenamento, na seção Chaves de Acesso. Você pode usar qualquer uma das chaves (key1 ou key2).

Para recuperar os dados do Servidor de Administração no modo interativo:

1. Execute o utilitário klbackup localizado na pasta de instalação do Kaspersky Security Center. Inicie o utilitário na mesma conta em que você instalou o Servidor de Administração. Recomendamos que o utilitário seja executado em um Servidor de Administração recém-instalado.

   O Assistente de backup e restauração é iniciado.

2. Na primeira página do Assistente, selecione **Restaurar dados do Servidor de Administração** e clique em **Avançar**.

   Caso selecione o a opção **Restaurar ou fazer backup somente do certificado do Servidor de Administração**, apenas o certificado e a chave privada do Servidor de Administração serão recuperados.

   Ao executar o utilitário klbackup no nó do cluster de failover inativo, você será solicitado a selecionar uma das opções: especificar o certificado do Servidor de Administração ou recuperar dados automaticamente do Servidor de Administração.

3. Na janela **Restaurar configurações** do Assistente:

   - Especifique a pasta que contém uma cópia backup dos dados do Servidor de Administração.

     Se você estiver trabalhando em um ambiente de nuvem, como o AWS ou o Azure, especifique o endereço do armazenamento. Além disso, é necessário verificar e confirmar se o nome do arquivo é backup.zip.

   - Especifique a senha que foi inserida durante o backup dos dados.

     Ao restaurar dados, você deve especificar a mesma senha que foi inserida durante o backup. Se o caminho para uma pasta compartilhada for alterado após o backup, verifique a operação de tarefas que usam os dados restaurados (tarefas de restauração e tarefas de instalação remota). Se necessário, edite as configurações dessas tarefas. Enquanto os dados estão sendo restaurados de um arquivo de backup, ninguém deve acessar a pasta compartilhada do Servidor de Administração. A conta em que o utilitário klbackup é iniciado deve ter acesso completo à pasta compartilhada.

4. Clique no botão **Avançar** para restaurar os dados.

Backup de dados e recuperação no modo silencioso

Para criar uma cópia backup ou recuperar os dados do Servidor de Administração no modo silencioso,

Execute o utilitário klbackup com o conjunto de chaves a partir da linha de comando de um dispositivo que tenha o Servidor de Administração instalado.

Os sinalizadores do agente de rede não são restaurados quando o utilitário klbackup é usado. É preciso configurar manualmente os sinalizadores do agente de rede.

A sintaxe da linha de comando do utilitário:

```
klbackup -path <backup path> [-linux_path <caminho de backup do SQL Server>][-node_cert <caminho do certificado>] [-logfile <arquivo de registro>] [-use_ts]|[-restore] [-password <senha>] [-cert_only] [-online] [-migrate postgres]
```

Se nenhuma senha for especificada na linha de comando do utilitário klbackup, o utilitário solicita a inserção da senha interativamente.

Descrições das chaves:

- `-path <backup path>`. Salve as informações na pasta de backup ou utilize os dados desta pasta para fazer a recuperação (parâmetro obrigatório).

  Devem ser concedidas permissões à conta do servidor do banco de dados e ao utilitário klbackup para alterar os dados na pasta de backup.

- `-linux_path <caminho de backup do SQL Server>` Caminho local até a pasta com os dados de backup para o SQL Server no Linux.

  Devem ser concedidas permissões à conta do servidor do banco de dados e ao utilitário klbackup para alterar os dados na pasta de backup do SQL Server.

- `-node_cert <certificate path>`. Arquivo de certificado do servidor para configurar o nó do cluster de failover inativo após a recuperação. Se não estiver definido, ele será automaticamente recuperado no servidor.

  Ao executar o utilitário klbackup no nó do cluster de failover inativo, use esta chave para indicar o caminho do certificado do servidor.

- `-logfile <log file>`. Salvar um relatório sobre o backup e a recuperação de dados do Servidor de Administração.

- `-use_ts`. Ao salvar dados, copie as informações para a pasta de backup, em uma subpasta com um nome no formato `klbackup YYYY-MM-DD # HH-MM-SS`, que inclui a data atual e a hora da operação em UTC. Se nenhuma chave for especificada, as informações são salvas na raiz da pasta de backup.

  Ao tentar salvar informações em uma pasta que já armazena uma cópia backup, uma mensagem de erro será exibida. Nenhuma informação será atualizada.

  A disponibilidade da chave `-use_ts` permite manter um arquivo de dados do Servidor de Administração. Por exemplo, caso a chave `-path` indique a pasta `C:\KLBackups`, a pasta `klbackup 2022/6/19 # 11-30-18` armazenará as informações sobre o status do Servidor de Administração em 19 de junho de 2022, às 11:30:18.

- `-restore` – Recupere os dados do Servidor de Administração. A recuperação de dados é realizada com base nas informações contidas na pasta de backup. Se não houver nenhuma chave disponível, um backup dos dados será feito na pasta de backup.

- `-password <password>`. Senha para proteger os dados confidenciais.

  Uma senha esquecida não pode ser recuperada. Não há requisitos de senha. O comprimento da senha é ilimitado e também é possível um comprimento nulo (sem senha).

  Ao restaurar dados, você deve especificar a mesma senha que foi inserida durante o backup. Se o caminho para uma pasta compartilhada for alterado após o backup, verifique a operação de tarefas que usam os dados restaurados (tarefas de restauração e tarefas de instalação remota). Se necessário, edite as configurações dessas tarefas. Enquanto os dados estão sendo restaurados de um arquivo de backup, ninguém deve acessar a pasta compartilhada do Servidor de Administração. A conta em que o utilitário klbackup é iniciado deve ter acesso completo à pasta compartilhada. Recomendamos que o utilitário seja executado em um Servidor de Administração recém-instalado.

- `-online` – Backup dos dados do Servidor de Administração ao criar um instantâneo do volume para, inimizar o tempo offline do Servidor de Administração. Quando você usa o utilitário para recuperar os dados, esta opção é ignorada.

- `-migrate postgres` - Cria um backup dos dados do Servidor de Administração armazenados no banco de dados do SQL Server que são compatíveis com o PostgreSQL e Postgres Pro. É possível restaurar os dados do backup para o PostgreSQL ou Postgres Pro. Use esse sinalizador quando realizar a migração para o Kaspersky Security Center Linux usando os dados de backup do Servidor da Administração.

  Esta opção fica disponível somente se você instalar o patch 14.2.0.26967-pf5 para o Servidor de Administração que permite a migração para PostgreSQL e Postgres Pro. Se você usa o Kaspersky Secure Mobility Management baseado no Kaspersky Security Center 14.2 Windows, use o patch 14.2.0.48079-pf5. Entre em contato com o Suporte Técnico da Kaspersky para obter o patch necessário.

Uso do utilitário klbackup para alterar dispositivos gerenciados sob gerenciamento de outro Servidor de Administração

O utilitário klbackup permite alterar dispositivos gerenciados sob gerenciamento de outro Servidor de Administração. É possível alterar o Servidor de Administração do Kaspersky Security Center Windows para Kaspersky Security Center Linux usando o utilitário klbackup ao executar a migração. Além disso, é possível migrar dispositivos gerenciados entre os Servidores de Administração do Kaspersky Security Center Windows.

Para alterar dispositivos gerenciados sob gerenciamento de outro Servidor de Administração usando o utilitário klbackup:

1. No dispositivo anterior, crie uma cópia de backup do certificado e da chave privada do Servidor de Administração usando a interface do utilitário klbackup.

   Execute o utilitário klbackup localizado na pasta de instalação do Kaspersky Security Center e crie um backup usando a opção **Restaurar ou fazer backup somente do certificado do Servidor de Administração**.

2. No dispositivo anterior, desconecte o Servidor de Administração da rede.

3. Atribua o mesmo endereço ao dispositivo com outro Servidor de Administração.

   O novo Servidor de Administração pode ser atribuído ao nome NetBIOS, FQDN e endereço IP estático. Isso depende de qual endereço do Servidor de Administração foi definido no pacote de instalação do Agente de Rede quando os Agentes de Rede foram implementados. Como alternativa, é possível usar o endereço de conexão que determina o Servidor de Administração ao qual o Agente de Rede se conecta (esse endereço pode ser obtido em dispositivos gerenciados usando o utilitário klnagchk).

4. Em um dispositivo com outro Servidor de Administração, restaure o certificado do Servidor de Administração e a chave privada por meio da cópia backup.

   É possível restaurar uma cópia backup por meio de uma das seguintes formas:

   - Com o uso da interface do utilitário klbackup (somente para o Servidor de Administração do Kaspersky Security Center Windows)

     Execute o utilitário klbackup e, em seguida, restaure um backup com o uso da opção **Restaurar ou fazer backup somente do certificado do Servidor de Administração**.

   - Usando o prompt de comando (para os Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux versão 15.1 ou posterior)

     Execute o utilitário klbackup com a chave `-cert_only` na linha de comando para restaurar uma cópia de backup do certificado do Servidor de Administração e da chave privada:

     ```
     klbackup -path <caminho para a cópia backup do certificado do Servidor de Administração> -restore -cert_only
     ```

Os dispositivos gerenciados são colocados sob o gerenciamento de outro Servidor de Administração. É possível ir para o Servidor de Administração e garantir que os dispositivos gerenciados estejam visíveis na rede e se o Agente de Rede está instalado e sendo executado neles (o valor *Sim* nas colunas **Visível**, **Agente de Rede instalado** e **Agente de Rede em execução**).

Backup e restauração de dados do Servidor de Administração ao usar MySQL ou MariaDB

É possível usar um backup de dados para migrar dados do Servidor de Administração do Kaspersky Security Center Windows sob gerenciamento do Kaspersky Security Center Linux. A migração usando o backup de dados do Servidor de Administração é compatível apenas com a migração para o Kaspersky Security Center Linux 15.2 ou posterior por qualquer versão compatível do Kaspersky Security Center Windows.

> Caso queira usar o MySQL ou o MariaDB como um DBMS para o Kaspersky Security Center Windows e para o Kaspersky Security Center Linux, o parâmetro `lower_case_table_names` deve corresponder ao DBMS atual e ao novo. Caso contrário, os dados do Servidor de Administração serão migrados incorretamente.

Antes de fazer backup dos dados do Servidor de Administração no Kaspersky Security Center Windows, verifique o valor do parâmetro `lower_case_table_names`. Se você não especificar este parâmetro durante a instalação anterior do DMBS, o valor padrão do parâmetro será utilizado. O valor padrão do parâmetro `lower_case_table_names` para Windows é `1`.

Ao instalar o MySQL ou o MariaDB para o Kaspersky Security Center Linux, defina o parâmetro `lower_case_table_names` com o mesmo valor especificado para esse parâmetro para o Windows com o uso das instruções do site do MySQL. Caso esse parâmetro não seja especificado, o valor padrão do parâmetro será usado. Para sistemas operacionais baseados em Linux, o valor padrão do parâmetro `lower_case_table_names` é diferente do valor padrão para Windows.

Caso queira instalar o MySQL 8.0, especificar o parâmetro `lower_case_table_names` de acordo com esta instrução pode não funcionar. Nesse caso, primeiro é necessário instalar o MySQL 5.7, especificar o parâmetro `lower_case_table_names` usando a instrução e, em seguida, atualizar o MySQL 5.7 para o MySQL 8.0. Caso o parâmetro `lower_case_table_names` não corresponda aos DBMSs atual e novo, os dados do Servidor de Administração serão restaurados incorretamente.

Mover Servidor de Administração para outro dispositivo

Se precisar usar o Servidor de Administração em um novo dispositivo, poderá movê-lo de uma das seguintes maneiras:

- Mova o Servidor de Administração e o servidor de banco de dados para um novo dispositivo (o servidor de banco de dados pode ser instalado no novo dispositivo juntamente com o Servidor de Administração ou em outro dispositivo).
- Mantenha o servidor de banco de dados no dispositivo anterior e mova apenas o Servidor de Administração para um novo dispositivo.

Para migrar o Servidor de Administração para um novo dispositivo:

1. No dispositivo anterior, crie um backup de dados do Servidor de Administração.

   Para fazer isso, você pode executar a tarefa de backup de dados por meio do Console de Administração ou executar o utilitário klbackup.

   > Se você usa o SQL Server como um DBMS para o Servidor de Administração, é possível migrar os dados do SQL Server para o MySQL ou o MariaDB DBMS. Para fazer isso, execute o utilitário klbackup no modo interativo para criar um backup de dados. Ative a opção **Migrar para o formato MySQL/MariaDB** na janela **Configurações de backup** do Assistente de backup e restauração. O Kaspersky Security Center criará um backup compatível com o MySQL e o MariaDB. Depois disso, é possível restaurar os dados do backup para o MySQL ou o MariaDB.

   > Você também pode ativar a opção **Migrar para o formato do Azure** se você quiser migrar os dados do SQL Server para o Azure SQL DBMS.

2. No dispositivo anterior, desconecte o Servidor de Administração da rede.

3. Selecione um novo dispositivo no qual instalar o Servidor de Administração. Certifique-se de que o hardware e o software do dispositivo selecionado atendam aos requisitos para Servidor de Administração, Console de Administração e Agente de Rede. Verifique também se as portas usadas no Servidor de Administração estão disponíveis.

4. Atribua o mesmo endereço ao novo dispositivo.

   O novo Servidor de Administração pode ser atribuído ao nome NetBIOS, FQDN e endereço IP estático. Isso depende de qual endereço do Servidor de Administração foi definido no pacote de instalação do Agente de Rede quando os Agentes de Rede foram implementados. Como alternativa, é possível usar o endereço de conexão que determina o Servidor de Administração ao qual o Agente de Rede se conecta (esse endereço pode ser obtido em dispositivos gerenciados usando o utilitário klnagchk).

5. Caso necessário, em outro dispositivo, instale o sistema de gerenciamento de banco de dados (DBMS) a ser usado pelo Servidor de Administração.

   O banco de dados pode ser instalado no novo dispositivo juntamente com o Servidor de Administração ou em outro dispositivo. Verifique e confirme se este dispositivo atende aos requisitos de hardware e software. Ao selecionar um DBMS, considere o número de dispositivos cobertos pelo Servidor de Administração.

6. Execute a instalação do Servidor de Administração no novo dispositivo.

7. Durante a instalação do Servidor de Administração, defina as configurações de conexão do servidor de banco de dados.



Exemplo da janela de configurações de conexão para Microsoft SQL Server

Dependendo de onde você precisa localizar o servidor de banco de dados, siga um destes procedimentos:

- Mantenha o servidor de banco de dados no dispositivo anterior

  1. Clique no botão **Procurar** ao lado do campo **Nome da instância do SQL Server** e, em seguida, selecione o nome do dispositivo anterior na lista que aparece.

     Observe que o dispositivo anterior deve estar disponível para conexão com o novo Servidor de Administração.

  2. Digite o nome do banco de dados anterior no campo **Nome do banco de dados**.

- Mova o servidor de banco de dados para outro dispositivo

  1. Clique no botão **Procurar** ao lado do campo **Nome da instância do SQL Server** e, em seguida, selecione o novo nome do dispositivo na lista que aparece.

  2. Digite o novo nome do banco de dados no campo **Nome do banco de dados**.

     Observe que o novo nome do banco de dados deve corresponder ao nome do banco de dados do dispositivo anterior. Os nomes dos bancos de dados devem ser idênticos, para que você possa usar o backup do Servidor de Administração. O nome padrão do banco de dados é *KAV*.

8. Após a conclusão da instalação, recupere os dados do Servidor de Administração no novo dispositivo usando o utilitário klbackup.

   Se usar o SQL Server como um DBMS nos dispositivos anteriores e novos, observe que a versão do SQL Server instalada no novo dispositivo deverá ser igual ou posterior à versão do SQL Server instalada no dispositivo anterior. Caso contrário, não será possível recuperar os dados do Servidor de Administração no novo dispositivo.

9. Abra o Console de Administração e conecte-se ao Servidor de Administração.

10. Verifique se todos os dispositivos gerenciados estão conectados com o Servidor de Administração.

11. Desinstale o Servidor de Administração e o servidor de banco de dados do dispositivo anterior.

Você também pode usar o Kaspersky Security Center Web Console para mover o Servidor de Administração e um servidor de banco de dados para outro dispositivo.

Evitar conflitos entre vários Servidores de Administração

Caso haja mais de um Servidor de Administração em sua rede, eles poderão ver os mesmos dispositivos cliente. Isso pode resultar, por exemplo, no Servidor de Administração instalando um aplicativo que já foi instalado por outro Servidor de Administração, ou outros conflitos. Para evitar que um aplicativo seja instalado em um dispositivo gerenciado por outro Servidor de Administração, ative a opção **Instalar somente em dispositivos gerenciados por este Servidor de Administração** em propriedades da tarefa *Instalar o aplicativo remotamente*.

Se você ativar a opção **Instalar somente em dispositivos gerenciados por este Servidor de Administração** e, executar a tarefa *Instalar o aplicativo remotamente* em seguida, uma verificação será feita para determinar se os dispositivos são gerenciados por outro Servidor de Administração. Para dispositivos gerenciados por outro Servidor de Administração, o valor do atributo **Gerenciado por outro Servidor de Administração** será `true`. A tarefa *Instalar o aplicativo remotamente* não aplicará a esses dispositivos.

Os valores do atributo **Gerenciado por outro Servidor de Administração** são exibidos na coluna **Gerenciado por outro Servidor de Administração** na lista de dispositivos gerenciados e na lista de dispositivos não atribuídos.

Você também pode usar a propriedade **Gerenciado por outro Servidor de Administração** como um critério com os seguintes objetivos:

- Pesquisar dispositivos
- Seleções de dispositivos
- Regras de migração de dispositivos
- Regras de identificação automática

Para redefinir o atributo Gerenciado por outro Servidor de Administração:

1. No menu principal do Kaspersky Security Center Web Console, vá para **Descoberta e implementação → Dispositivos não atribuídos**.

2. Selecione o dispositivo necessário e clique no botão **Desmarcar a caixa de seleção Gerenciado por um Servidor de Administração diferente**.

O atributo **Gerenciado por outro Servidor de Administração** é redefinido.

Verificação em duas etapas

Esta seção descreve como você pode usar a verificação em duas etapas para reduzir o risco de acesso não autorizado ao Console de Administração ou ao Kaspersky Security Center Web Console.

Sobre a verificação em duas etapas

Quando a verificação em duas etapas estiver ativada para uma conta, um código de segurança de uso único é necessário, além do nome de usuário e senha, para fazer login no Console de Administração ou no Kaspersky Security Center Web Console. Com a autenticação do domínio ativada, o usuário precisa inserir apenas o código de segurança de uso único.

Para usar a verificação em duas etapas, instale um app autenticador que gere códigos de segurança de uso único no dispositivo móvel ou computador. É possível usar qualquer aplicativo compatível com o Algoritmo de Senha Avulsa por Tempo Limitado (TOTP), como:

- Autenticador do Google
- Autenticador da Microsoft
- Bitrix24 OTP
- Chave Yandex
- Autenticador da Avanpost
- Aladdin 2FA

Para verificar se o Kaspersky Security Center é compatível com o app autenticador que deseja usar, ative a verificação em duas etapas para todos os usuários ou para um usuário específico.

Uma das etapas sugere a especificação do código de segurança gerado pelo app autenticador. Em caso de êxito, o Kaspersky Security Center será compatível com o autenticador selecionado.

É altamente recomendável salvar a chave secreta ou código QR e mantê-la em um lugar seguro. Isso ajudará a restaurar o acesso ao Kaspersky Security Center Web Console, caso o dispositivo móvel seja perdido.

Para proteger o uso do Kaspersky Security Center, você pode ativar a verificação em duas etapas para sua própria conta e depois ativá-la para todos os usuários.

Você pode excluir contas da verificação em duas etapas. Isso pode ser necessário para contas de serviço que não podem receber um código de segurança para autenticação.

Regras e limitações

Para ativar a verificação em duas etapas para todos os usuários e desativar a verificação em duas etapas para usuários específicos:

- Verifique e confirme se sua conta tem o direito de modificar ACLs de objetos na área funcional **Recursos gerais: permissões do usuário**.
- Ative a verificação em duas etapas para sua conta.

Para poder desativar a verificação em duas etapas para todos os usuários:

- Verifique e confirme se sua conta tem o direito de modificar ACLs de objetos na área funcional **Recursos gerais: permissões do usuário**.
- Faça login no Kaspersky Security Center Web Console usando a verificação em duas etapas.

Caso a verificação em duas etapas esteja ativada para uma conta de usuário no Servidor de Administração do Kaspersky Security Center versão 13 ou posterior, o usuário não poderá fazer login no Kaspersky Security Center Web Console das versões 12, 12.1 ou 12.2.

Reemissão da chave secreta

Qualquer usuário pode reemitir a chave secreta usada para a verificação em duas etapas. Quando um usuário fizer login no Servidor de Administração com a chave secreta reemitida, a nova chave secreta será salva para a conta de usuário. Caso o usuário insira a nova chave secreta incorreta, a nova chave secreta não será salva e a chave secreta atual permanecerá válida.

Um código de segurança possui um identificador conhecido como *nome do emissor*. O nome do emissor do código de segurança é usado como um identificador do Servidor de Administração no app autenticador. O nome do emissor do código de segurança possui um valor padrão que é igual ao nome do Servidor de Administração. Você pode alterar o nome do emissor do código de segurança. Caso você tenha alterado o nome do emissor do código de segurança, será necessário emitir uma nova chave secreta e passá-la para o app autenticador.

Cenário: configurando a verificação em duas etapas para todos os usuários

Este cenário descreve como ativar a verificação em duas etapas para todos os usuários e como excluir contas de usuário da verificação em duas etapas. Se você não ativou a verificação em duas etapas para sua conta antes de ativá-la para outros usuários, o aplicativo abre a janela para ativando a verificação em duas etapas para sua própria conta, primeiro. Este cenário também descreve como ativar a verificação em duas etapas para a sua própria conta.

Se você ativou a verificação em duas etapas para sua conta, pode prosseguir para a ativação da verificação em duas etapas para todos os usuários.

Pré-requisitos

Antes de começar:

- Certifique-se de que sua conta de usuário tenha o direito de Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões de usuário** para modificar as configurações de segurança para contas de outros usuários.
- Verifique e confirme se os outros usuários do Servidor de Administração instalaram um app autenticador em seus dispositivos.

Fases

Ativar a verificação em duas etapas para todos os usuários é feita com os seguintes passos:

1. **Instalação de um app autenticador em um dispositivo**

   É possível instalar qualquer aplicativo compatível com o Algoritmo de Senha Avulsa por Tempo Limitado (TOTP), como:

   - Autenticador do Google
   - Autenticador da Microsoft
   - Bitrix24 OTP
   - Chave Yandex
   - Autenticador da Avanpost
   - Aladdin 2FA

   Para verificar se o Kaspersky Security Center é compatível com o app autenticador que deseja usar, ative a verificação em duas etapas para todos os usuários ou para um usuário específico.

   Uma das etapas sugere a especificação do código de segurança gerado pelo app autenticador. Em caso de êxito, o Kaspersky Security Center será compatível com o autenticador selecionado.

   > É altamente recomendável não instalar o app autenticador no mesmo dispositivo no qual a conexão com o Servidor de Administração é estabelecida.

2. **Sincronização da hora do app autenticador com a hora do dispositivo no qual o Servidor de Administração está instalado**

   Verifique e confirme se a hora no dispositivo com o app autenticador e a hora no dispositivo com o Servidor de Administração estão sincronizadas com UTC usando fontes de tempo externas. Caso contrário, falhas podem ocorrer durante a autenticação e a ativação da verificação em duas etapas.

3. **Ativando a verificação em duas etapas para sua conta e recebendo a chave secreta para sua conta**

   Instruções de como proceder:

   - Para o Console de Administração baseado em MMC: Ativando a verificação em duas etapas para sua própria conta
   - Para Kaspersky Security Center Web Console: Ativando a verificação em duas etapas para sua própria conta

Após ativar a verificação em duas etapas para sua conta, você pode fazer a verificação em duas etapas para todos os usuários.

4. **Ativando a verificação em duas etapas para todos os usuários**

   Os usuários com a verificação em duas etapas ativada devem usá-la para fazer login no Servidor de Administração.

   Instruções de como proceder:

   - Para o Console de Administração baseado em MMC: Ativando a verificação em duas etapas para todos os usuários
   - Para Kaspersky Security Center Web Console: Ativando a verificação em duas etapas para todos os usuários

5. **Editando o nome de um emissor do código de segurança**

   Se você tiver vários Servidores de Administração com nomes semelhantes, pode ser necessário alterar os nomes do emissor do código de segurança para melhor identificação de diferentes Servidores de Administração.

   Instruções de como proceder:

   - Para Console de Administração baseado em MMC: Editando o nome de um emissor de código de segurança
   - Para Kaspersky Security Center Web Console: Editando o nome de um emissor de código de segurança

6. **Excluindo contas de usuário para as quais você não precisa ativar a verificação em duas etapas**

   Caso necessário, exclua os usuários da verificação em duas etapas. Os usuários com contas excluídas não precisam usar a verificação em duas etapas para fazer login no Servidor de Administração.

   Instruções de como proceder:

   - Para Console de Administração baseado em MMC: Excluindo contas da verificação em duas etapas
   - Para Kaspersky Security Center Web Console: Excluindo contas da verificação em duas etapas

7. **Configurando a verificação em duas etapas para sua própria conta**

   Caso os usuários não sejam excluídos da verificação em duas etapas e ela ainda não tenha sido configurada para suas contas, eles precisarão configurá-la na janela aberta ao fazer login no Kaspersky Security Center. Do contrário, eles não poderão acessar o Servidor de Administração de acordo com seus direitos.

   Instruções de como proceder:

   - Para o Console de Administração baseado em MMC: configurando a verificação em duas etapas para sua própria conta
   - Para Kaspersky Security Center Web Console: configuração da verificação em duas etapas para sua própria conta

Resultados

Após a conclusão deste cenário:

- A verificação em duas etapas está ativada para a sua conta.
- A verificação em duas etapas é ativada para todas as contas de usuário do Servidor de Administração, exceto para contas de usuário excluídas.

Ativar a verificação em duas etapas para sua própria conta (baseado em MMC)

Antes de ativar a verificação em duas etapas para sua conta, verifique e confirme se um app autenticador está instalado no dispositivo móvel. Certifique-se de que a hora definida no app autenticador está sincronizada com a hora do Servidor de Administração.

Ativando a verificação em duas etapas para sua conta:

1. Na árvore do console do Kaspersky Security Center, abra o menu contextual da pasta **Servidor de Administração** e selecione **Propriedades**.
2. Na janela de propriedades do Servidor de Administração, acesse o painel **Seções**, selecione **Avançado** e **Verificação em duas etapas**.
3. Na seção **Verificação em duas etapas**, clique no botão **Configurar**.

   Caso a verificação em duas etapas já esteja ativada para sua conta, ao clicar no botão **Configurar**, a chave secreta será redefinida para que seja possível reconfigurar a verificação em duas etapas.

   Na janela aberta de propriedades da verificação em duas etapas, a chave secreta é exibida.
4. Insira a chave secreta no app autenticador para receber o código de segurança de uso único. É possível especificar a chave secreta no app autenticador manualmente ou ler o código QR do app autenticador no dispositivo móvel.
5. Especifique o código de segurança gerado pelo app autenticador e clique no botão **OK** para sair da janela de propriedades de verificação em duas etapas.
6. Clique no botão **Aplicar**.
7. Clique no botão **OK**.

A verificação em duas etapas é ativada para a sua própria conta.

Ativar a verificação em duas etapas para todos os usuários (baseado em MMC)

Você pode ativar a verificação em duas etapas para todos os usuários do Servidor de Administração se sua conta tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões do usuário** e se você fizer a autenticação usando a verificação em duas etapas.

Para ativar a verificação em duas etapas para vários usuários:

1. Na árvore do console do Kaspersky Security Center, abra o menu contextual da pasta **Servidor de Administração** e selecione **Propriedades**.
2. Na janela de propriedades do Servidor de Administração, no painel **Seções**, selecione **Avançado** e **verificação em duas etapas**.

3. Clique no botão **Definir como obrigatório** para ativar a verificação em duas etapas para todos os usuários.

4. Caso não tenha ativado a verificação em duas etapas para sua conta, o aplicativo abre a janela para ativar a verificação em duas etapas para sua própria conta.

   a. Insira a chave secreta no app autenticador para receber o código de segurança de uso único. É possível especificar a chave secreta no app autenticador manualmente ou ler o código QR do app autenticador no dispositivo móvel para receber o código de segurança de uso único.

   b. Especifique o código de segurança gerado pelo app autenticador e clique no botão **OK** para sair da janela de propriedades de verificação em duas etapas.

5. Na seção **Verificação em duas etapas**, clique no botão **Aplicar** e depois no botão **OK.**

A verificação em duas etapas está ativada para todos os usuários. A partir de agora, todos os usuários do Servidor de Administração, incluindo os usuários que foram adicionados após ativar esta opção, devem configurar a verificação em duas etapas para suas contas, exceto para os usuários cujas contas foram excluídas da verificação em duas etapas.

Desativar a verificação em duas etapas para uma conta de usuário (baseado em MMC)

Para desativar a verificação em duas etapas para uma conta de usuário:

1. Na árvore do console do Kaspersky Security Center, abra o menu contextual da pasta **Servidor de Administração** e selecione **Propriedades**.

2. Na janela de propriedades do Servidor de Administração, no painel **Seções**, selecione **Avançado** e **verificação em duas etapas**.

3. Na seção **Verificação em duas etapas**, clique no botão **Desativar**.

4. Clique no botão **Aplicar**.

5. Clique no botão **OK**.

A verificação em duas etapas é desativada para sua conta.

Você pode desativar a verificação em duas etapas para contas de outros usuários. Isso fornece proteção no caso, por exemplo, de um usuário perder ou danificar um dispositivo móvel.

> Você pode desativar a verificação em duas etapas para outra conta de usuário somente se você tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões do usuário** e se você fizer a autenticação usando a verificação em duas etapas. Seguindo os passos abaixo, você também pode desativar a verificação em duas etapas para a sua própria conta.

Para desativar a verificação em duas etapas para qualquer conta de usuário:

1. Na árvore do console, abra a pasta **Contas de usuário**.

   Por padrão, a pasta **Contas de usuário** é uma subpasta da pasta **Avançado**.

2. No espaço de trabalho, clique duas vezes na conta do usuário para a qual você deseja desativar a verificação em duas etapas.

   Para todas as contas de usuário para as quais a verificação em duas etapas está ativada, a coluna **2FA exigida** é definida como **Sim**.

3. Na janela aberta **Propriedades:<nome de usuário>**, selecione a seção **Verificação em duas etapas.**

4. Na seção **Verificação em duas etapas**, selecione as seguintes opções:

   - Se deseja ativar a verificação em duas etapas para uma conta de usuário, clique no botão **Desativar**.
   - Se deseja excluir esta conta de usuário da verificação em duas etapas, selecione a opção **Usuário pode aprovar uma autenticação usando apenas nome de usuário e senha**.

5. Clique no botão **Aplicar**.

6. Clique no botão **OK**.

A verificação em duas etapas para uma conta de usuário é desativada.

Se você quiser restaurar o acesso de um usuário que não pode fazer login no Console de Administração usando a verificação em duas etapas, desative a verificação em duas etapas para esta conta de usuário e selecione a opção **Usuário pode aprovar uma autenticação usando apenas nome de usuário e senha** na caixa **Verificação em duas etapas** como descrito acima. Depois disso, faça login no Console de Administração com a conta de usuário para a qual você desativou a verificação em duas etapas e ative a verificação novamente.

Desativar a verificação em duas etapas obrigatória para todos os usuários (baseado em MMC)

Você pode desativar a verificação em duas etapas necessária para todos os usuários do Servidor de Administração se sua conta tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões do usuário** e se você fizer a autenticação usando a verificação em duas etapas.

Para desativar a verificação em duas etapas:

1. Na árvore do console do Kaspersky Security Center, abra o menu contextual da pasta **Servidor de Administração** e selecione **Propriedades**.

2. Na janela de propriedades do Servidor de Administração, no painel **Seções**, selecione **Avançado** e **verificação em duas etapas**.

3. Clique no botão **Definir como opcional** para desativar a verificação em duas etapas para todos os usuários.

4. Clique no botão **Aplicar** na seção **Verificação em duas etapas.**

5. Clique no botão **OK** na seção **verificação em duas etapas.**

A verificação em duas etapas está desativada para todos os usuários. A desativação da verificação em duas etapas para todos os usuários não se aplica a contas específicas para as quais a verificação em duas etapas foi anteriormente ativada separadamente.

Excluir contas da verificação em duas etapas (baseado em MMC)

Você pode excluir uma conta de usuário da verificação em duas etapas se tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões de usuário**.

Se uma conta de usuário for excluída da verificação em duas etapas, esse usuário pode efetuar login no Console de Administração ou no Kaspersky Security Center Web Console sem usar a verificação em duas etapas.

A exclusão de contas da verificação em duas etapas pode ser necessária para contas de serviço que não podem passar o código de segurança durante a autenticação.

Para excluir uma conta de usuário da verificação em duas etapas:

1. Se deseja excluir uma conta do Active Directory, execute a sondagem do Active Directory para atualizar a lista de usuários do Servidor de Administração.

2. Na árvore do console, abra a pasta **Contas de usuário**.

   Por padrão, a pasta **Contas de usuário** é uma subpasta da pasta **Avançado**.

3. No espaço de trabalho, clique duas vezes na conta do usuário que deseja excluir da verificação em duas etapas

4. Na janela aberta **Propriedades:<nome de usuário>**, selecione a seção **Verificação em duas etapas.**

5. Na seção aberta, selecione a opção **Usuário pode aprovar uma autenticação usando apenas nome de usuário e senha**.

6. Na seção **Verificação em duas etapas**, clique no botão **Aplicar** e depois no botão **OK**.

Esta conta de usuário é excluída da verificação em duas etapas. Você pode marcar as contas excluídas na lista de contas de usuário.

Editar o nome de um emissor do código de segurança (baseado em MMC)

Você pode ter várias tags (chamadas de emissores) para diferentes Servidores de Administração. Você pode alterar o nome de um emissor de código de segurança no caso, por exemplo, se o Servidor de Administração já usa um nome semelhante de emissor para outro Servidor de Administração. Por padrão, o nome de um emissor de código de segurança é igual ao nome do Servidor de Administração.

Depois de alterar o nome do emissor do código de segurança, será necessário emitir novamente uma nova chave secreta e passá-la para o app autenticador.

Para especificar um novo nome de um emissor do código de segurança:

1. Na árvore do console do Kaspersky Security Center, abra o menu contextual da pasta **Servidor de Administração** e selecione **Propriedades**.
2. Na janela de propriedades do Servidor de Administração, no painel **Seções**, selecione **Avançado** e **verificação em duas etapas**.
3. Especifique um novo nome de emissor de código de segurança no campo **Emissor de código de segurança**.
4. Clique no botão **Aplicar** na seção **Verificação em duas etapas.**
5. Clique no botão **OK** na seção **verificação em duas etapas.**

Um novo nome de emissor de código de segurança é especificado para o Servidor de Administração.

Configurar a verificação em duas etapas para sua própria conta (baseado em MMC)

Na primeira vez que o usuário fizer login no Kaspersky Security Center depois que a verificação em duas etapas estiver ativada, a janela para configurar a verificação em duas etapas para sua própria conta será aberta.

Antes de ativar a verificação em duas etapas para sua conta, verifique e confirme se o aplicativo autenticador está instalado no seu dispositivo móvel. Verifique e confirme se a hora no dispositivo com o app autenticador e a hora no dispositivo com o Servidor de Administração estão sincronizadas com UTC usando fontes de tempo externas.

Para configurar a verificação em duas etapas para sua conta:

1. Gere um código de segurança de uso único usando o aplicativo autenticador em seu dispositivo móvel. Para fazer isso, execute um das seguintes ações:
   - Insira manualmente a chave secreta no app autenticador.
   - Leia o código QR usando o app autenticador.

   Um código de segurança será exibido no dispositivo móvel.
2. Na janela **Configurar a verificação em duas etapas**, especifique o código de segurança gerado pelo app autenticador e clique no botão **OK**.

A verificação em duas etapas está configurada para a sua conta. É possível acessar o Servidor de Administração de acordo com seus direitos.

Alteração da pasta compartilhada do Servidor de Administração

A pasta compartilhada do Servidor de Administração é especificada durante a sua instalação. Também é possível alterar a localização da pasta compartilhada nas propriedades do Servidor de Administração.

Para alterar a pasta compartilhada:

1. Crie uma pasta de compartilhamento de rede e configure permissões para o compartilhamento e para a estrutura de pastas para permitir direitos de controle total para o subgrupo **Todos**.
2. Na árvore do console do Kaspersky Security Center, abra o menu de contexto da pasta **Servidor de Administração** e selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, no painel **Seções**, selecione **Avançado** e, a seguir, **Pasta compartilhada do Servidor de Administração**.
4. Na seção **Pasta compartilhada do Servidor de Administração**, clique no botão **Alterar**.
5. Selecione a pasta que deseja usar como compartilhada.
6. Clique no botão **OK** para fechar a janela Propriedades do Servidor de Administração.
7. Atribua direitos de leitura para o subgrupo **Todos** para a pasta selecionada como compartilhada.

Gerenciamento de grupos de administração

Esta seção fornece informações sobre como gerenciar grupos de administração.

Você pode executar as seguintes ações nos grupos de administração:

- Adicione qualquer número de grupos aninhados de qualquer nível de hierarquia aos grupos de administração.
- Adicionar dispositivos aos grupos de administração.
- Altere a hierarquia de grupos de administração ao migrar dispositivos individuais e grupos inteiros para outros grupos.
- Remover grupos aninhados e dispositivos dos grupos de administração.
- Adicionar Servidores de Administração secundários e virtuais aos grupos de administração.
- Mover dispositivos cliente dos grupos de administração de um Servidor de Administração para aqueles de outro Servidor.
- Definir quais aplicativos Kaspersky que serão instalados automaticamente em dispositivos incluídos em um grupo.

Você pode executar essas ações somente se tiver a **permissão** Modificar na área **Gerenciamento de grupos de administração** para os grupos de administração que deseja gerenciar (ou para o Servidor de Administração ao qual esses grupos pertencem).

Criação de grupos de administração

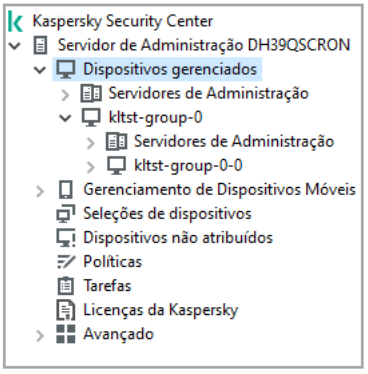
A hierarquia de grupos de administração é criada na janela principal do aplicativo Kaspersky Security Center, na pasta **Dispositivos gerenciados**. Os grupos de administração são exibidos como pastas na árvore do console (veja a figura abaixo).

Imediatamente após a instalação do Kaspersky Security Center, a pasta **Dispositivos gerenciados** contém somente uma pasta **Servidores de Administração vazia**.

As configurações de interface do usuário determinam se a pasta **Servidores de Administração** aparece na árvore do console. Para exibir esta pasta, na barra de menus, selecione **Visualizar → Configurar interface** e, na janela aberta **Configurar interface**, selecione a caixa de seleção **Exibir os Servidores de Administração secundários**.

Ao criar uma hierarquia de grupos de administração, você poderá adicionar dispositivos e máquinas virtuais à pasta **Dispositivos gerenciados**, e adicionar grupos aninhados. Você pode adicionar Servidores de Administração secundários e virtuais à pasta **Servidores de Administração**.

Assim como feito para a pasta **Dispositivos gerenciados**, cada grupo criado inicialmente, somente contém uma pasta **Servidores de Administração** vazia para uso com Servidores de Administração secundários neste grupo. Informações sobre políticas e tarefas para este grupo e informações sobre dispositivos incluídos neste grupo são exibidas nas guias com os nomes correspondentes no espaço de trabalho deste grupo.



Exibir hierarquia de grupos de administração

Para criar um grupo de administração:

1. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.
2. Se você desejar criar um subgrupo de um grupo de administração existente, na pasta **Dispositivos gerenciados**, selecione a subpasta que corresponde a esse grupo, ou seja, para incluir o novo grupo de administração.

   Se você criar um novo grupo de administração de nível superior, você pode pular esta etapa.
3. Inicie o processo de criação do grupo de administração em uma das seguintes formas:

   - Usando o comando **Novo → Grupo** no menu de contexto.
   - Ao clicar no botão **Novo grupo** localizado no espaço de trabalho da janela principal do aplicativo, na guia **Dispositivos**.
4. Na janela **Nome do grupo** que será aberta, insira um nome para o grupo e clique em **OK**.

Uma nova pasta de grupo de administração com o nome especificado aparece na árvore do console.

O aplicativo permite criar a hierarquia dos grupos de administração com base na estrutura do Active Directory ou na estrutura de domínio da rede. Você também pode criar uma estrutura de grupos a partir de um arquivo de texto.

Para criar a estrutura de grupos de administração:

1. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.
2. No menu de contexto da pasta **Dispositivos gerenciados**, selecione **Todas as tarefas → Nova estrutura de grupos**.

O Assistente de Nova Estrutura de Grupos de Administração é iniciado. Siga as instruções do Assistente.

Mover grupos de administração

Você pode mover grupos de administração alojados dentro da hierarquia dos grupos.

Um grupo de administração é migrado juntamente com todos os grupos aninhados, Servidores de Administração secundários, dispositivos, políticas de grupo e tarefas. O sistema aplicará ao grupo todas as configurações que corresponderem a sua nova posição na hierarquia dos grupos de administração.

O nome do grupo deve ser único dentro de um nível da hierarquia. Se um grupo com o mesmo nome já existir na pasta para a qual você move o grupo de administração, você deve alterar o nome do último. Se você não tiver alterado o nome do grupo movido, um índice no formato **(<próximo número de sequência>)** é automaticamente adicionado ao seu nome após ser movido, por exemplo: **(1)**, **(2)**.

Você não pode renomear o grupo **Dispositivos gerenciados** porque ele é um elemento incorporado do Console de Administração.

Para mover um grupo para outra pasta na árvore do console:

1. Selecione um grupo para mover na árvore do console.
2. Execute uma das seguintes ações:
   - Mova o grupo usando o menu de contexto:
     1. Selecione **Cortar** no menu de contexto do grupo.
     2. Selecione **Colar** no menu de contexto do grupo de administração para o qual você precisa mover o grupo selecionado.
   - Mova o grupo usando o menu principal do aplicativo:
     a. No menu principal, selecione **Ação → Cortar**.
     b. Selecione o grupo de administração para o qual você precisa mover o grupo selecionado na árvore do console.
     c. No menu principal, selecione **Ação → Colar**.
   - Mova o grupo para outro na árvore do console, usando o mouse.

Exclusão de grupos de administração

Você pode excluir um grupo de administração se o mesmo não incluir Servidores de Administração secundários, grupos aninhados ou dispositivos clientes, e caso não tenham sido criadas tarefas de grupo ou políticas para ele.

Antes de excluir um grupo de administração, você deve excluir todos os Servidores de Administração secundários, grupos aninhados e dispositivos cliente daquele grupo.

Para excluir um grupo:

1. Selecione um grupo de administração na árvore do console.
2. Execute uma das seguintes ações:
   - Selecione **Excluir** no menu de contexto do grupo.
   - No menu principal do aplicativo, selecione **Ação** → **Excluir**.
   - Pressione a tecla **DELETE**.

Criação automática de uma estrutura de grupos de administração

O Kaspersky Security Center lhe permite criar uma estrutura de grupos de administração usando o Assistente de criação de hierarquias de grupos.

O assistente cria uma estrutura de grupos de administração com base nos seguintes dados:

- Estruturas de domínios do Windows e grupos de trabalho
- Estruturas de grupos do Active Directory
- Conteúdo de um arquivo de texto criado pelo administrador manualmente

Quando o arquivo de texto for gerado, os seguintes requisitos devem ser atendidos:

- O nome de cada novo grupo deve começar com uma nova linha; o delimitador deve começar com uma quebra de linha. As linhas em branco são ignoradas.

  Exemplo:

  Escritório 1

  Escritório 2

  Escritório 3

  Três grupos do primeiro nível de hierarquia serão criados no grupo visado.

- O nome do grupo alojado deve ser inserido com uma barra (/).

  Exemplo:

  Escritório 1/Divisão 1/Departamento 1/grupo 1

  Quatro subgrupos aninhados dentro um do outro serão criados no grupo alvo.

- Para criar vários grupos alojados do mesmo nível de hierarquia, você deve especificar o "caminho completo ao grupo".

  Exemplo:

  Escritório 1/Divisão 1/Departamento 1

  Escritório 1/Divisão 2/Departamento 1

  Escritório 1/Divisão 3/Departamento 1

  Escritório 1/Divisão 4/Departamento 1

  Um grupo do primeiro nível de hierarquia Escritório 1 será criado no grupo de destino; esse grupo incluirá quatro grupos alojados do mesmo nível de hierarquia: "Divisão 1", "Divisão 2", "Divisão 3" e "Divisão 4". Cada um desses grupos incluirá o grupo "Departamento 1".

Criar a hierarquia de grupos de administração através do assistente não afeta a integridade da rede: em vez de grupos existentes sendo substituídos, novos grupos são adicionados. Um dispositivo cliente não pode estar incluído em um grupo de administração uma segunda vez porque o dispositivo é removido do grupo **Dispositivos não atribuídos** quando ele for movido para o grupo de administração.

Se, durante a criação da estrutura do grupo de administração, um dispositivo não foi incluído no grupo **Dispositivos não atribuídos** por algum motivo (foi desligado ou desconectado da rede), ele não será automaticamente movido para o grupo de administração. Você pode adicionar dispositivos manualmente aos grupos de administração após o assistente concluir sua operação.

Para iniciar a criação automática de uma estrutura de grupos de administração:

1. Selecione a pasta **Dispositivos gerenciados** na árvore do console.
2. No menu de contexto da pasta **Dispositivos gerenciados**, selecione **Todas as tarefas → Nova estrutura de grupos**.

   O Assistente de Nova Estrutura de Grupos de Administração é iniciado. Siga as instruções do Assistente.

Instalação automática de aplicativos nos dispositivos em um grupo de administração

É possível especificar quais pacotes de instalação devem ser usados para a instalação remota automática de aplicativos da Kaspersky em dispositivos clientes em um grupo de administração.

Para configurar a instalação automática de aplicativos em dispositivos em um grupo de administração:

1. Na árvore do console, selecione um grupo de administração desejado.
2. Abra a janela de propriedades do grupo de administração.
3. No painel **Seções**, selecione **Instalação automática** e, no espaço de trabalho, selecione os pacotes de instalação dos aplicativos a serem instalados em novos dispositivos.
4. Clique em **OK**.

As tarefas de grupo são criadas. Estas tarefas são executadas nos dispositivos cliente imediatamente após serem adicionadas ao grupo de administração.

Se alguns pacotes de instalação de um aplicativo são selecionados para instalação automática, a tarefa de instalação é criada apenas para a versão do aplicativo mais recente.

Gerenciamento de dispositivos cliente

Esta seção contém informações como trabalhar com dispositivos cliente.

Conectar dispositivos cliente ao Servidor de Administração

A conexão do dispositivo cliente ao Servidor de Administração é estabelecida através do Agente de Rede instalado no dispositivo cliente.

Quando um dispositivo cliente se conecta ao Servidor de Administração, as seguintes operações são executadas:

- Sincronização automática de dados:
  - A sincronização da lista de aplicativos instalados no dispositivo cliente.
  - Sincronização das políticas, configurações do aplicativo, tarefas e configurações de tarefa.
- Resgate de informações atualizadas sobre a condição de aplicativos, execução de tarefas e estatísticas da operação de aplicativos pelo Servidor de Administração.
- Entrega das informações do evento ao Servidor de Administração para o processamento.

A sincronização automática de dados é executada regularmente de acordo com as configurações do Agente de Rede (por exemplo, a cada 15 minutos). Você pode especificar o intervalo de conexão manualmente.

As informações sobre um evento são enviadas ao Servidor de Administração assim que ocorram.

Se um Servidor de Administração estiver localizado remotamente fora de uma rede corporativa, os dispositivos cliente podem se conectar ao mesmo através da Internet.

Para os dispositivos se conectarem a um Servidor de Administração por meio da Internet, as seguintes condições precisam ser atendidas:

- O Servidor de Administração remoto deve ter um endereço IP externo e a porta de entrada 13000 deve permanecer aberta (para a conexão de Agentes de Rede). Recomendamos que você também abra a porta UDP 13000 (para receber notificações do desligamento do dispositivo).
- Os Agentes de Rede devem ser instalados nos dispositivos.
- Ao instalar o Agente de Rede em dispositivos, você deverá especificar o endereço IP externo do Servidor de Administração remoto. Se para a instalação for usado um pacote de instalação, o endereço IP externo deve ser especificado manualmente nas propriedades do pacote de instalação na seção **Configurações**.
- Para usar o Servidor de Administração para gerenciar aplicativos e tarefas para um dispositivo, na janela de propriedades desse dispositivo na seção **Geral**, selecione a caixa de seleção **Não desconectar do Servidor de Administração**. Após a caixa de seleção ter sido selecionada, aguarde até o Servidor de Administração esteja sincronizado com o dispositivo remoto. O número de dispositivos cliente mantendo uma conexão contínua com um Servidor de Administração não pode exceder 300.

Para aumentar o desempenho de tarefas iniciadas por um Servidor de Administração remoto, você pode abrir a porta 15000 em um dispositivo. Neste caso, para executar uma tarefa, o Servidor de Administração envia um pacote especial ao Agente de Rede através da porta 15000 sem esperar pela conclusão da sincronização com o dispositivo.

O Kaspersky Security Center permite configurar a conexão entre um dispositivo cliente e o Servidor de Administração, para que a conexão permaneça ativa após a conclusão de todas as operações. Uma conexão ininterrupta é necessária nos casos quando o monitoramento em tempo real de status do aplicativo seja necessário e o Servidor de Administração não é capaz de estabelecer uma conexão ao cliente por algum motivo (por exemplo, a conexão é protegida por um firewall, a abertura de portas no dispositivo cliente não é permitida, o endereço IP do cliente é desconhecido). Você pode estabelecer uma conexão ininterrupta entre um dispositivo cliente e o Servidor de Administração na janela Propriedades do dispositivo na seção **Geral**.

Nós recomendamos que você estabeleça uma conexão ininterrupta com os dispositivos cliente mais importantes. O número total de conexões simultaneamente mantidas pelo Servidor de Administração é limitado a 300.

Durante a sincronização manual, o sistema usa um método de conexão auxiliar que permite a conexão iniciada pelo Servidor de Administração. Antes de estabelecer a conexão em um dispositivo cliente, você deve abrir a porta UDP. O Servidor de Administração envia uma solicitação de conexão para a porta UDP do dispositivo cliente. Em resposta, o certificado do Servidor de Administração é verificado. Se o certificado do Servidor de Administração coincidir com a cópia do certificado armazenada no dispositivo cliente, a conexão será estabelecida.

O início manual da sincronização também é usado para obter informações atualizadas sobre a condição de aplicativos, execução de tarefas e estatísticas da operação de aplicativos.

Conecte manualmente um dispositivo cliente ao Servidor de administração. Utilitário klmover

Se você precisar conectar manualmente um dispositivo cliente ao Servidor de Administração, poderá usar o utilitário klmover no dispositivo cliente.

Ao instalar o Agente de Rede em um dispositivo cliente, o utilitário é copiado automaticamente para a pasta de instalação do Agente de Rede.

Para conectar manualmente um dispositivo cliente ao Servidor de Administração usando o utilitário klmover:

No dispositivo, inicie o utilitário klmover a partir da linha de comando.

Quando iniciado a partir da linha de comando, o utilitário klmover pode executar as seguintes ações (dependendo das chaves que estiverem em uso):

- Conecta o Agente de Rede ao Servidor de Administração com as configurações especificadas;
- Grava os resultados de operação no arquivo de log de eventos ou exibe os mesmos na tela.

Você não pode usar o utilitário klmover para dispositivos clientes conectados ao Servidor de Administração por meio de gateways de conexão. Para esses dispositivos, é necessário reconfigurar o Agente de Rede ou reinstalar o Agente de Rede e especificar o gateway de conexão.

A sintaxe da linha de comando do utilitário:

```
klmover [-logfile <nome do arquivo>] [-address <endereço do servidor>] [-pn <número da porta>] [-ps <número da porta SSL>] [-nossl] [-cert <caminho para o arquivo de certificado>] [-silent] [-dupfix] [-virtserv] [-cloningmode]
```

Os direitos de administrador são necessários para executar o utilitário.

Descrições das chaves:

- `-logfile <nome do arquivo>`: Registra os resultados da execução do utilitário em um arquivo de log.

  Por predefinição, as informações são salvas na transmissão de saída predefinido (stdout). Se a chave não estiver sendo usada, os resultados e as mensagens de erro são exibidos na tela.

- `-address <endereço do servidor>`: Endereço do Servidor de Administração para conexão.

  Você pode especificar um endereço IP, o nome NetBIOS ou o nome DNS de um dispositivo como seu endereço.

- `-pn <número da porta>`: Número da porta pela qual a conexão não criptografada com o Servidor de Administração é estabelecida.

  O número da porta padrão é 14000.

- `-ps <número da porta SSL>`: Número da porta SSL pela qual a conexão criptografada com o Servidor de Administração é estabelecida usando SSL.

  O número da porta padrão é 13000.

- `-nossl` – usa a conexão não criptografada ao Servidor de Administração.

  Se a chave não estiver sendo usada, o Agente de Rede é conectado ao Servidor de Administração através do protocolo SSL codificado.

- `-cert <caminho para o arquivo de certificado>`: Use o arquivo de certificado especificado para fazer a autenticação de acesso ao Servidor de Administração.

  Se a chave não estiver sendo usada, o Agente de Rede recebe um certificado na primeira conexão ao Servidor de Administração.

- `-silent` – Executa o utilitário no modo silencioso.

  Usar a chave poderá ser útil se, por exemplo, o utilitário for iniciado a partir do script de login no momento do registro do usuário.

- `-dupfix` – A chave é usada se o Agente de Rede tiver sido instalado usando um método diferente do que é habitual (com o pacote de distribuição) – por exemplo, recuperando a partir de uma imagem de disco ISO.

- `-virtserv` – nome do Servidor de Administração virtual.

- `-cloningmode` – modo de clonagem do disco do Agente de Rede.

  Use um dos seguintes parâmetros para configurar o modo de clonagem de disco:

  - `-cloningmode` – Solicita o status do modo de clonagem de disco.

  - `-cloningmode 1` – Ativa o modo de clonagem de disco.

  - `-cloningmode 0` – Desativa o modo de clonagem de disco.

- `-nauninstpwd <senha>`: A chave é usada para especificar a senha de desinstalação do Agente de Rede.

  A chave não é obrigatória.

Por exemplo, para conectar o Agente de Rede ao Servidor de Administração, execute o seguinte comando:

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

Conexão em túnel entre um dispositivo cliente e o Servidor de Administração

O Kaspersky Security Center permite o tunelamento de conexões de TCP, do Console de Administração via Servidor de Administração, e então via Agente de Rede a uma porta especificada em um dispositivo gerenciado. O tunelamento é projetado para conectar um aplicativo cliente em um dispositivo com o Console de Administração instalado à uma porta TCP em um dispositivo gerenciado – se nenhuma conexão direta for possível entre o Console de Administração e o dispositivo alvo.

Por exemplo, o tunelamento é usado para conexões a uma área de trabalho remota, para conectar-se a uma sessão existente e para criar uma nova sessão remota.

O tunelamento também pode ser ativado usando ferramentas externas. Por exemplo, o administrador pode executar o utilitário putty, o cliente VNC e outras ferramentas desta forma.

A conexão em túnel entre um dispositivo cliente remoto e Servidor de Administração é necessária se a porta usada para a conexão ao Servidor de Administração não estiver disponível no dispositivo. A porta no dispositivo poderá estar indisponível nos seguintes casos:

- O dispositivo remoto é conectado à uma rede local que usa o mecanismo NAT.

- Um dispositivo remoto é parte da rede local, do Servidor de Administração, mas sua porta está fechada por um firewall.

Para criar uma conexão em túnel entre um dispositivo cliente e o Servidor de Administração:

1. Na árvore do console, selecione a pasta do grupo de administração que contém o dispositivo cliente.
2. Na guia **Dispositivos**, selecione o dispositivo.
3. No menu de contexto do dispositivo, selecione **Todas as tarefas → Conexão em túnel**.
4. Na janela **Conexão em túnel** que for aberta, crie um túnel.

Conexão remota à Área de trabalho de um dispositivo cliente

O administrador pode obter o acesso remoto à área de trabalho de um dispositivo cliente através de um Agente de Rede instalado no dispositivo.

A conexão remota a um dispositivo por meio do Agente de Rede é possível mesmo que as portas TCP e UDP do dispositivo cliente estejam fechadas. Ao estabelecer a conexão com o dispositivo, o administrador obtém o acesso completo às informações armazenadas nesse dispositivo, para que possa gerenciar os aplicativos nele instalados.

Esta seção descreve como estabelecer uma conexão com um dispositivo cliente Windows e um dispositivo cliente macOS por meio do Agente de Rede.

Conectar-se a dispositivos clientes Windows

A conexão remota com um dispositivo cliente Windows pode ser estabelecida em uma das seguintes formas:

- Usando um componente padrão do Microsoft Windows nomeado Conexão com a área de trabalho remota.

  A conexão com uma área de trabalho remota é estabelecida através do utilitário Windows padrão mstsc.exe, de acordo com as configurações do utilitário.

- Usando a tecnologia de Compartilhamento da área de trabalho do Windows.

Conectando-se ao dispositivo cliente Windows usando a conexão de desktop remoto

A conexão com a sessão de área de trabalho remota atual do usuário é estabelecida sem o conhecimento do usuário. Após o administrador se conectar com a sessão, o usuário do dispositivo será desconectado da sessão sem uma notificação antecipada.

Para conectar-se com a área de trabalho de um de dispositivo cliente através do componente Conexão de área de trabalho remota:

1. Na árvore do Console de Administração, selecione um dispositivo ao qual você precisa obter acesso.
2. No menu de contexto do dispositivo, selecione **Todas as tarefas → Conectar-se ao dispositivo → Nova sessão RDP**.

   O utilitário padrão do Windows, mstsc.exe, é iniciado, o que ajuda a estabelecer conexão com a área de trabalho remota.

3. Siga as instruções exibidas nas caixas de diálogo do utilitário.

Quando a conexão com o dispositivo for estabelecida, a área de trabalho ficará disponível na janela Conexão remota do Microsoft Windows.

Conectar-se ao dispositivo cliente Windows usando o Compartilhamento da área de trabalho do Windows

Ao conectar-se a uma sessão da área de trabalho remota existente, o usuário da sessão no dispositivo recebe uma solicitação para a conexão do administrador. Nenhuma informação sobre a atividade remota no dispositivo e seus resultados será salva em relatórios criados pelo Kaspersky Security Center.

O administrador pode conectar-se a uma sessão existente em um dispositivo cliente sem desconectar o usuário a sessão. Nesse caso, o administrador e o usuário da sessão no dispositivo compartilham o acesso à área de trabalho.

O administrador pode configurar uma auditoria da atividade do usuário em um dispositivo cliente remoto. Durante a auditoria, o aplicativo salva as informações sobre arquivos no dispositivo cliente que tenham sido abertos e/ou modificados pelo administrador.

Para conectar-se com a área de trabalho de um dispositivo cliente por meio do Compartilhamento da área de trabalho do Windows, as seguintes condições devem ser satisfeitas:

- Microsoft Windows Vista ou mais recente instalado na estação de trabalho do administrador. O tipo de sistema operacional do dispositivo que hospeda o Servidor de Administração não impõe restrições à conexão através do Compartilhamento da área de trabalho do Windows.

  Para verificar se o recurso Compartilhamento da área de trabalho do Windows está incluído na sua edição do Windows, verifique se há a chave CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} no registro do Windows.

- O Microsoft Windows Vista ou mais recente está instalado no dispositivo cliente.

- O Kaspersky Security Center usa uma licença para Gerenciamento de patches e vulnerabilidades.

Para conectar-se com a área de trabalho de um de dispositivo cliente através da tecnologia de Compartilhamento da área de trabalho do Windows:

1. Na árvore do Console de Administração, selecione um dispositivo ao qual você precisa obter acesso.

2. No menu de contexto do dispositivo, selecione **Todas as tarefas → Conectar-se ao dispositivo → Windows Desktop Sharing**.

3. Na janela **Selecionar sessão de área de trabalho remota** que for aberta, selecione a sessão no dispositivo ao qual você deseja se conectar.

   Se a conexão com o dispositivo cliente for estabelecida com êxito, a área de trabalho do dispositivo ficará disponível na janela **Visualizador da sessão do Kaspersky Remote Desktop**.

4. Para começar a interagir com o dispositivo, no menu principal da janela **Visualizador da sessão do Kaspersky Remote Desktop**, selecione **Ações → Modo interativo**.

O utilitário **Visualizador da sessão do Kaspersky Remote Desktop** requer uma licença comercial.

Conectar-se a dispositivos clientes macOS

O administrador pode usar o sistema Virtual Network Computing (VNC) para se conectar a dispositivos macOS.

A conexão com um desktop remoto é estabelecida por meio de um cliente VNC instalado no dispositivo do Servidor de Administração. O cliente VNC alterna o controle de teclado e mouse do dispositivo cliente para o administrador.

Quando o administrador se conecta ao desktop remoto, o usuário não recebe notificações ou solicitações de conexão do administrador. O administrador conecta-se a uma sessão existente em um dispositivo cliente sem desconectar o usuário da sessão.

Para conectar-se com a área de trabalho de um dispositivo cliente macOS por meio do cliente VNC, as seguintes condições devem ser satisfeitas:

- O cliente VNC está instalado no dispositivo do Servidor de Administração.
- Login remoto e gerenciamento remoto são permitidos no dispositivo cliente.
- O usuário permitiu o acesso de administrador ao dispositivo cliente nas configurações de **Compartilhamento** do sistema operacional macOS.

Para conectar-se com a área de trabalho de um de dispositivo cliente por meio do sistema de Virtual Network Computing:

1. Na árvore do Console de Administração, selecione um dispositivo ao qual você precisa obter acesso.
2. No menu de contexto do dispositivo, selecione **Todas as tarefas** → **Conexão em túnel**.
3. Na janela **Conexão em túnel** que se abre, execute a seguinte ação:
    a. Na seção **1. Porta de rede**, especifique o número da porta de rede do dispositivo ao qual você precisa se conectar.

    Por padrão, a porta 5900 é usada.

    b. Na seção **2. Tunelamento**, clique no botão **Criar tunelamento**.

    c. Na seção **3. Configurações de rede**, clique no botão **Copiar**.
4. Abra o cliente VNC e cole os atributos de rede copiados no campo de texto. Pressione **`Enter`**.
5. Na janela que for aberta, visualize os detalhes do certificado. Se você concorda em usar o certificado, clique no botão **Sim**.
6. Na janela **Autenticação**, especifique as credenciais do dispositivo cliente e clique em **OK**.

Conexão com dispositivos cliente através do Windows Desktop Sharing

Para conectar-se a um dispositivo através do Compartilhamento da área de trabalho do Windows:

1. No árvore do console, na guia **Dispositivos**, selecione a pasta **Dispositivos gerenciados**.

   O espaço de trabalho desta pasta exibe uma lista de dispositivos.

2. No menu de contexto do dispositivo ao qual você deseja se conectar, selecione **Conectar-se ao dispositivo → Windows Desktop Sharing**.

   A janela **Selecionar sessão de área de trabalho remota** se abre.

3. Na janela **Selecionar sessão de área de trabalho remota**, selecione uma sessão de área de trabalho para usar para conexão ao dispositivo.

4. Clique em **OK**.

O dispositivo é conectado.

Configurar o reinício de um dispositivo cliente

Usando, instalando ou removendo o Kaspersky Security Center, você deveria reiniciar o dispositivo. Você pode especificar as configurações de reinicialização somente para dispositivos que executam o Windows.

Para configurar o reinício de um de dispositivo cliente:

1. Na árvore do console, selecione o grupo de administração para o qual você deve configurar o reinício.

2. No espaço de trabalho do grupo, selecione a guia **Políticas**.

3. No espaço de trabalho, selecione uma política do Agente de Rede do Kaspersky Security Center na lista de políticas e, em seguida, selecione **Propriedades** no menu de contexto da política.

4. Na janela de propriedades da política, selecione a seção **Gerenciamento de reinício**.

5. Selecione a ação que deve ser executada se uma reinicialização do dispositivo for necessária:

   - Selecione **Não reiniciar o sistema operacional** para bloquear a reinicialização automática.
   - Selecione **Reiniciar o sistema operacional automaticamente se necessário** para permitir o reinício automático.
   - Selecione **Perguntar ao usuário o que fazer** para perguntar ao usuário se ele permite o reinício.

   Você pode especificar a frequência das solicitações de reinicialização e ativar a reinicialização e o fechamento forçados dos aplicativos em sessões bloqueadas no dispositivo, marcando as caixas de seleção e as configurações de hora correspondentes nas caixas de rotação.

6. Clique em **OK** para salvar as alterações e fechar a janela Propriedades da política.

O reinicio do dispositivo será configurado agora.

Auditar ações em um dispositivo cliente remoto

O aplicativo permite a realização de auditoria das ações do administrador em dispositivos cliente remotos executando o Windows. Durante a auditoria, o aplicativo salva as informações sobre arquivos no dispositivo cliente que tenham sido abertos e/ou modificados pelo administrador. A auditoria das ações do administrador está disponível quando as seguintes condições são observadas:

- A licença de Gerenciamento de Patches e Vulnerabilidades está em uso.
- O administrador tem o direito de iniciar o acesso compartilhado à área de trabalho do dispositivo remoto.

Para ativar a auditoria de ações em um de dispositivo cliente remoto:

1. Na árvore do console, selecione o grupo de administração para o qual a auditoria das ações do administrador deve ser configurada.
2. No espaço de trabalho do grupo, selecione a guia **Políticas**.
3. Selecione uma política do Agente de Rede do Kaspersky Security Center e, a seguir, selecione **Propriedades** no menu de contexto da política.
4. Na janela de propriedades da política, selecione a seção **Windows Desktop Sharing**.
5. Marque a caixa de seleção **Ativar auditoria**.
6. Nas listas **Máscaras de arquivos para monitorar quando lidos** e **Máscaras de arquivos para monitorar quando modificados**, adicione máscaras de arquivo nas quais o aplicativo deve monitorar ações durante a auditoria.

   Por padrão, o aplicativo monitora ações em arquivos com as extensões .txt, .rtf, .doc, .xls, .docx, .xlsx, .odt e .pdf.
7. Clique em **OK** para salvar as alterações e fechar a janela Propriedades da política.

Isso resulta na configuração da auditoria das ações do administrador no de dispositivo remoto do usuário com acesso à área de trabalho compartilhado.

Os registros de ações do administrador no dispositivo remoto são registrados:

- No log de eventos no dispositivo remoto.
- Em um arquivo com extensão syslog localizado na pasta do Agente de Rede em um dispositivo remoto (por exemplo, C:\ProgramData\KasperskyLab\adminkit\1103\logs).
- No banco de dados de eventos do Kaspersky Security Center.

Verificar a conexão entre um dispositivo cliente e o Servidor de Administração

O Kaspersky Security Center lhe permite verificar as conexões entre um dispositivo cliente e o Servidor de Administração de forma automática ou manual.

A verificação automática da conexão é realizada no Servidor de Administração. A verificação manual da conexão é executada no dispositivo.

Verificar automaticamente a conexão entre um dispositivo cliente e o Servidor de Administração

Para iniciar uma verificação automática da conexão entre um dispositivo cliente e o Servidor de Administração:

1. Na árvore do console, selecione o grupo de administração que inclui o dispositivo.
2. No espaço de trabalho do grupo de administração, na guia **Dispositivos**, selecione o dispositivo.
3. No menu de contexto do dispositivo, selecione **Verificar a acessibilidade do dispositivo**.

Isto abre uma janela que contém informações sobre a acessibilidade do dispositivo.

Verificar manualmente a conexão entre um dispositivo cliente e o Servidor de Administração. Utilitário klnagchk

Você pode verificar a conexão e obter informações detalhadas sobre as configurações da conexão entre um dispositivo cliente e o Servidor de Administração usando o utilitário klnagchk. O utilitário klnagchk está localizado na pasta Instalação do Agente de Rede.

Quando iniciado a partir da linha de comando, o utilitário klnagchk pode executar as seguintes ações (dependendo das chaves que estiverem em uso):

- Exibe na tela ou registra em log os valores das configurações usadas para conectar o Agente de Rede instalado no dispositivo ao Servidor de Administração.
- Grava em um arquivo de log de eventos as estatísticas do Agente de Rede (desde a última inicialização) e os resultados de operação do utilitário ou exibe as informações na tela.
- Tenta estabelecer uma conexão entre o Agente de Rede e o Servidor de Administração.

  Se a tentativa de conexão falhar, o utilitário envia um pacote ICMP para verificar o status do dispositivo no qual o Servidor de Administração está instalado.

Para verificar a conexão entre um dispositivo cliente e o Servidor de Administração usando o utilitário klnagchk.

No dispositivo com o Agente de Rede instalado, inicie o utilitário klnagchk por meio da linha de comando em uma conta de administrador local.

A sintaxe da linha de comando do utilitário:

```
klnagchk [-logfile <nome do arquivo>] [-sp] [-savecert <caminho para o arquivo de certificado>] [-restart][-sendhb]
```

Descrições das chaves:

- `-logfile <nome do arquivo>` – Registra os valores das configurações de conexão entre o Agente de Rede e o Servidor de Administração, assim como os resultados da operação do utilitário em um arquivo de log.

  Por predefinição, as informações são salvas na transmissão de saída predefinido (stdout). Se a chave não estiver sendo usada, as configurações, os resultados e as mensagens de erro são exibidos na tela.

- `-sp` – Mostra a senha para a autenticação do usuário no servidor proxy.

  A chave está em uso se a conexão ao Servidor de Administração for estabelecida por meio de um servidor proxy.

- `-savecert <nome do arquivo>` – Salva o certificado usado para acessar o Servidor de Administração em um arquivo especificado.

- `-restart` – Inicia o Agente de Rede após a conclusão do utilitário.

- `-sendhb` – Inicia a sincronização do Agente de Rede com o Servidor de Administração.

Após a inicialização, o utilitário klnagchk acessa os arquivos de configuração do Agente de Rede e exibe os parâmetros de conexão. Esses parâmetros são especificados durante a instalação do Agente de Rede e nas configurações da política do Agente de Rede:

- `Dispositivo atual` – Nome de rede Windows do dispositivo cliente.

- `Versão do Agente de Rede` – Número completo da versão do Agente de Rede (com patches) instalado no dispositivo.

- `Endereço do Servidor de Administração` – O endereço do Servidor de Administração.

- `Usar SSL` – Parâmetro que indica se uma conexão segura é usada ao conectar-se ao Servidor de Administração.

  Valores possíveis:

  - 0 – A conexão segura não é usada.

  - 1 – A conexão segura é usada.

- `Compactar o tráfego` – Parâmetro que indica se o tráfego entre o dispositivo cliente e o Servidor de Administração é compactado.

- `Números das portas SSL do Servidor de Administração` – Números de portas válidas para comunicação com o Servidor de Administração ao usar uma conexão segura.

- `Números das portas do Servidor de Administração` – Números das portas válidas para comunicação com o Servidor de Administração ao usar uma conexão comum.

- `Usar servidor proxy` – Parâmetro que indica se um servidor proxy é usado.

  Valores possíveis:

  - 0 – O servidor proxy não é usado.

  - 1 – O servidor proxy é usado.

- `Endereço` – Endereço e porta do servidor proxy separados por dois pontos. Esse parâmetro é exibido somente se um servidor proxy for usado.
- `Nome de usuário` – Nome de usuário para acessar o servidor proxy. Esse parâmetro é exibido somente se um servidor proxy for usado.
- `Senha` – Senha para acessar o servidor proxy. Esse parâmetro é exibido somente se um servidor proxy for usado. Para mostrar a senha do servidor proxy, é necessário usar a chave `sp` no comando.
- `Certificado do Servidor de Administração` – Parâmetro que indica se o dispositivo cliente tem um certificado do Servidor de Administração. Um certificado pode não existir, por exemplo, se o Agente de Rede nunca tiver se conectado com êxito ao Servidor de Administração.

  Valores possíveis:

  - `não instalado` – O dispositivo cliente não tem um certificado do Servidor de Administração.
  - `disponível` – O dispositivo cliente tem um certificado do Servidor de Administração.
- `Abrir porta UDP` – Parâmetro que indica se o Agente de Rede usa a porta UDP para receber solicitações de sincronização do Servidor de Administração.

  Valores possíveis:

  - 0 – A porta UDP está fechada para receber as solicitações de sincronização do Servidor de Administração.
  - 1 – A porta UDP está aberta para receber as solicitações de sincronização do Servidor de Administração.
- `Números das portas UDP` – Números das portas UDP que podem ser usadas pelo Agente de Rede.
- `Nome do local` – Localização da rede do dispositivo.
- `Estado da localização da rede` – Parâmetro que indica se o dispositivo cliente pode ser alternado de um perfil de conexão do Servidor de Administração para outro.

  Valores possíveis:

  - `Ativado` – O perfil de conexão do Servidor de Administração pode ser trocado para o dispositivo cliente.
  - `Desativado` – O perfil de conexão do Servidor de Administração não pode ser trocado para o dispositivo cliente.
- `Perfil a ser usado` – Perfil de conexão para o Servidor de Administração.
- `Condição` – Endereço IP e máscara de sub-rede da rede à qual o dispositivo cliente está conectado.
- `Intervalo de sincronização (min)` – Intervalo padrão entre sincronizações.
- `Tempo limite da conexão (em segundos)` – Tempo limite da conexão.
- `Tempo limite de envio/recebimento (em segundos)` – Tempo limite da conexão das operações de leitura/gravação.
- `ID do dispositivo` – Identificador do dispositivo na rede. A `ID do dispositivo` é exclusiva entre os dispositivos clientes gerenciados por um Servidor de Administração específico.

- `Locais dos gateways de conexão` – Parâmetros para conectar o dispositivo cliente ao Servidor de Administração por meio do gateway de conexão.

- `Localização dos pontos de distribuição` – Parâmetros para conectar o dispositivo cliente ao Servidor de Administração por meio do ponto de distribuição.

- `Conexão com o servidor` – Parâmetro que indica se o gateway de conexão tem uma conexão contínua com o Servidor de Administração. O parâmetro é exibido somente se o dispositivo cliente atuar como um gateway de conexão.

  Valores possíveis:

  - `ativo` – O gateway de conexão tem uma conexão contínua com o Servidor de Administração.

  - `inativo` – O gateway de conexão não tem uma conexão contínua com o Servidor de Administração.

- `Conexão com o servidor pelo gateway de conexão` – Parâmetro que indica se a conexão ao Servidor de Administração por meio de um gateway de conexão foi estabelecida corretamente. O parâmetro é exibido somente se o dispositivo cliente atuar como um gateway de conexão.

  Valores possíveis:

  - `ativo` – A conexão com o Servidor de Administração por meio de um gateway de conexão foi estabelecida corretamente.

  - `inativo` – A conexão com o Servidor de Administração por meio de um gateway de conexão foi estabelecida incorretamente.

Além disso, a saída do utilitário klnagchk pode conter uma das seguintes linhas:

- `O Servidor de Administração está instalado neste dispositivo` – O utilitário klnagchk é executado no dispositivo do Servidor de Administração.

- `Este dispositivo foi atribuído a um gateway de conexão, mas ainda não está registrado no Servidor de Administração` – O utilitário klnagchk é executado no dispositivo no qual o Agente de Rede está instalado, no modo de gateway de conexão. O gateway de conexão configurado está aguardando uma conexão do Servidor de Administração, mas o Servidor de Administração não lista o dispositivo entre os dispositivos gerenciados. Você precisa garantir que o Servidor de Administração inicie uma conexão com o gateway de conexão.

- `Este dispositivo é um gateway de conexão` – O utilitário klnagchk é executado no dispositivo que atua como um gateway de conexão.

- `Atua como um ponto de distribuição` – O utilitário klnagchk é executado no dispositivo que atua como um ponto de distribuição.

O utilitário klnagchk verifica o status do serviço do Agente de Rede. Se o serviço não estiver em execução, o utilitário será interrompido. Se o serviço estiver em execução, o utilitário exibirá as seguintes estatísticas de conexão:

- `Número total de solicitações de sincronização` – Número de tentativas para conectar o dispositivo cliente ao Servidor de Administração.

- `O número de solicitações de sincronização bem-sucedidas` – Número de tentativas bem-sucedidas de conectar o dispositivo cliente ao Servidor de Administração.

- `Número total de sincronizações` – Número de tentativas para sincronizar as configurações do dispositivo cliente com as configurações do Servidor de Administração.

- `O número de sincronizações bem-sucedidas` – Número de tentativas bem-sucedidas de sincronizar as configurações do dispositivo cliente ao Servidor de Administração.

- `Data/hora da última solicitação de sincronização` – Data e hora da última conexão.

Você precisa usar os parâmetros `Número total de solicitações de sincronização` e `Número de solicitações de sincronização bem-sucedidas` ao analisar a conexão entre o Servidor de Administração e o Agente de Rede. As configurações do dispositivo cliente só serão sincronizadas com as configurações do Servidor de Administração se as configurações do Servidor de Administração forem alteradas (por exemplo, se novas tarefas forem adicionadas ou as configurações de política forem modificadas). Caso contrário, os valores dos parâmetros `Número total de sincronizações` e `Número de sincronizações bem-sucedidas` permanecerão inalterados.

Para obter mais informações sobre como solucionar problemas ao conectar o Agente de Rede ao Servidor de Administração, consulte as perguntas frequentes do Kaspersky Security Center.

Sobre verificar o tempo de conexão entre um dispositivo e o Servidor de Administração

Para desligar um dispositivo, o Agente de Rede notifica o Servidor de Administração sobre este evento. No Console de Administração, esse dispositivo é exibido como desligado. No entanto, o Agente de Rede não pode notificar o Servidor de Administração sobre todos tais eventos. O Servidor de Administração, portanto, periodicamente analisa o atributo **Conectado ao Servidor de Administração** (o valor deste atributo é exibido no Console de Administração, nas propriedades do dispositivo, na seção **Geral**) para cada dispositivo e compara-o com o intervalo de sincronização a partir das configurações atuais do Agente de Rede. Se um dispositivo não tiver respondido ao longo de mais de três intervalos de sincronização sucessivos, aquele dispositivo é marcado como desligado.

Identificação de dispositivos cliente no Servidor de Administração

Os dispositivos cliente são identificados com base em seus nomes. Um nome de dispositivo cliente é único entre todos os nomes de dispositivos conectados ao Servidor de Administração.

O nome de um dispositivo é encaminhado ao Servidor de Administração quando a rede Windows for amostrada e um novo dispositivo for descoberto nela, ou durante a primeira conexão do Agente de Rede instalado em um dispositivo cliente ao Servidor de Administração. Por padrão, o nome corresponde ao nome do dispositivo na rede Windows (nome NetBIOS). Se um dispositivo com esse nome já estiver registrado no Servidor de Administração, será adicionado um índice com o próximo número de sequência ao nome do novo dispositivo, por exemplo: **<Nome>-1**, **<Nome>-2**. Sob este nome, o dispositivo é adicionado ao grupo de administração.

Mover dispositivos para um grupo de administração

Você pode migrar dispositivos de um grupo de administração para outro somente se tiver a permissão **Modificar** na área **Gerenciamento de grupos de administração** para grupos de administração de origem e de destino (ou para o Servidor de Administração ao qual esses grupos pertencem).

Para incluir um ou diversos dispositivos em um grupo de administração selecionado:

1. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.
2. Na pasta **Dispositivos gerenciados**, selecione subpasta que corresponde ao grupo no qual os dispositivos cliente serão incluídos.

   Se você desejar incluir os dispositivos cliente no grupo **Dispositivos gerenciados**, poderá ignorar esta etapa.
3. No espaço de trabalho do grupo de administração selecionado, na guia **Dispositivos**, inicie o processo de incluir os dispositivos no grupo usando uma das seguintes formas:

   - Adicionando os dispositivos ao grupo, clicando no botão **Migrar dispositivos para o grupo**, na caixa de informações para a lista de dispositivos
   - Selecionando **Criar** → **Dispositivo** no menu de contexto da lista de dispositivos

   O Assistente para Mover Dispositivos é iniciado. Seguindo suas instruções, selecione um método para mover os dispositivos ao grupo e crie uma lista de dispositivos para incluir no grupo.

   Se você criar a lista de dispositivos manualmente, poderá usar um endereço IP (ou um conjunto de IPs), um nome NetBIOS ou um nome DNS como endereço de um dispositivo. Você pode mover manualmente à lista somente os dispositivos para os quais as informações já foram adicionadas no banco de dados do Servidor de Administração ao conectar o dispositivo ou após descoberta de dispositivos.

   Para importar a lista de dispositivos a partir de um arquivo, especifique um arquivo TXT com uma lista de endereços de dispositivos a serem adicionados. Cada endereço deve ser especificado em uma linha em separado.

Após o Assistente concluir a sua operação, os dispositivos selecionados serão incluídos no grupo de administração e exibidos na lista de dispositivos sob os nomes gerados pelo Servidor de Administração.

Você pode mover um dispositivo cliente ao grupo de administração arrastando-o da pasta **Dispositivos não atribuídos** para a pasta do grupo de administração.

Alterar o Servidor de Administração para dispositivos clientes

É possível alterar o Servidor de Administração que gerencia os dispositivos cliente por outro, usando a tarefa *Alterar o Servidor de Administração*.

Para alterar o Servidor de Administração que gerencia dispositivos cliente para outro servidor:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. No espaço de trabalho da pasta, clique no botão **Nova tarefa**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na etapa **Selecionar o tipo de tarefa** do assistente, selecione o nó **Servidor de Administração do Kaspersky Security Center**, expanda a pasta **Avançado** e selecione a tarefa **Alterar o Servidor de Administração**.
4. Na janela que é aberta, clique no botão **OK** para confirmar que concorda com os termos de alteração do Servidor de Administração para dispositivos clientes.

5. Na etapa **Configurações** do assistente, selecione o Servidor de Administração que deseja usar para gerenciar os dispositivos selecionados:

- Mudar para outro Servidor de Administração principal

  Para mover dispositivos cliente para outro Servidor de Administração principal, especifique as seguintes configurações de conexão do Servidor de Administração:

  1. No campo **Servidor de Administração**, especifique o endereço do novo Servidor de Administração principal.
  2. No campo **Porta**, especifique o número da porta para se conectar ao Servidor de Administração.

     O número da porta padrão é 14000.
  3. No campo **Porta SSL**, especifique o número da porta SSL no Servidor de Administração principal.

     O número da porta padrão é 13000.
  4. Se necessário, marque a caixa de seleção **Usar o servidor proxy**.

     Se essa caixa de seleção estiver desmarcada, a conexão direta será usada para conectar o dispositivo ao Servidor de Administração.

     Se essa caixa de seleção estiver selecionada, especifique os parâmetros do servidor proxy:

     - **Endereço do servidor proxy**
     - **Porta do servidor proxy**

     Se o servidor proxy exigir autenticação, nos campos **Nome do usuário** e **Senha**, especifique as credenciais da conta sob a qual a conexão com o servidor proxy será estabelecida. Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.
  5. Se necessário, carregue um novo certificado do Servidor de Administração.

- Mudar para outro Servidor de Administração virtual neste Servidor principal

  Selecione essa opção para mover dispositivos cliente para o Servidor de Administração virtual no Servidor de Administração principal atual. Para fazer isso, no campo **Nome do Servidor de Administração virtual**, especifique o nome do Servidor de Administração virtual necessário.

Se necessário, especifique o tempo de espera antes de reiniciar o Agente de Rede.

6. Nesta etapa do assistente, faça as seleções de dispositivos aos quais a tarefa será atribuída:

- **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**. Neste caso, a tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

- **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**. Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

- **Atribuir a tarefa a uma seleção de dispositivos**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em uma seleção anteriormente criada. É possível especificar a seleção predefinida ou uma personalizada criada por você.

- **Atribuir tarefa a um grupo de administração**. Neste caso, a tarefa é atribuída aos dispositivos incluídos no grupo de administração criado anteriormente.

7. Na etapa **Selecionar uma conta para executar a tarefa**, especifique as configurações da conta:

- Conta padrão

  A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

  Por padrão, esta opção está selecionada.

- Especificar conta

  Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

  - Conta

    Conta sob a qual a tarefa é executada.

  - Senha

    Senha da conta sob a qual a tarefa será executada.

8. Na etapa **Configurar agendamento da tarefa** do assistente, você pode criar um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- Início agendado:

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - Diariamente (não é compatível com horário de verão)

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

  - Por dias da semana

    A tarefa é executada regularmente, nos dias da semana e no horário especificados.

    Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

  - Mensalmente

    A tarefa é executada regularmente, no dia do mês e na hora especificados.

    Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

    Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

  - Uma vez

    A tarefa é executada uma vez, na data e hora especificadas (por padrão, no dia em que a tarefa foi criada).

  - Manualmente

    A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

    Por padrão, esta opção está selecionada.

  - Imediatamente

    A tarefa é executada imediatamente após o dispositivo se tornar visível na rede ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

- Executar tarefas ignoradas

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

9. Nesta etapa do assistente, especifique o nome da tarefa que você está criando.

10. Na etapa **Concluir a criação da tarefa** do assistente, clique no botão **Concluir** para fechar o assistente.

    Se deseja que a tarefa inicie assim que o assistente for concluído, marque a caixa de seleção **Executar tarefa após a conclusão do assistente**.

Após a conclusão da tarefa, os dispositivos cliente, para os quais a mesma foi criada, são colocados sob gerenciamento pelo Servidor de Administração especificado nas configurações da tarefa.

Caso o Servidor de Administração seja compatível com a criptografia e a proteção dos dados e o usuário esteja criando uma tarefa *Alterar o Servidor de Administração*, uma advertência é exibida. O aviso indica que se quaisquer dados criptografados forem armazenados nos dispositivos, após o novo servidor começar a gerenciar os dispositivos, os usuários somente serão capazes de acessar os dados criptografados com os quais eles anteriormente trabalharam. Em outros casos, nenhum acesso a dados criptografados será fornecido. Para obter descrições detalhadas de cenários nos quais o acesso aos dados criptografados não é fornecido, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

Migração de dispositivos conectados com o Servidor de Administração por meio de gateways de conexão para outro Servidor de Administração

É possível migrar os dispositivos conectados com o Servidor de Administração por meio de gateways de conexão para outro Servidor de Administração. Por exemplo, esse procedimento pode ser necessário se você instalar outra versão do Servidor de Administração e não quiser reinstalar o Agente de Rede nos dispositivos, pois isso pode levar muito tempo.

Os comandos descritos na instrução devem ser executados em dispositivos clientes em uma conta com direitos de administrador.

Para migrar um dispositivo conectado por meio do gateway de conexão para outro Servidor de Administração:

1. Execute o utilitário klmover com o parâmetro `-address <endereço do servidor>` para mudar para o novo Servidor de Administração.
2. Execute o comando `klnagchk -nagwait -tl 4`.
3. Execute os seguintes comandos para definir um novo gateway de conexão:
   - `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 "<gateway_ip_or_name>" -svt STRING_T -ss "|ss_type = \"SS_SETTINGS\";"`

     Aqui `gateway_ip_or_name` é o endereço do gateway de conexão acessível pela Internet.
   - `klscflag -ssvset -pv klnagent -s FileTransfer -n ft_gateway_ssl_port -sv 13000 -svt INT_T -ss "|ss_type = \"SS_SETTINGS\";"`

     `13000` é o número da porta TCP que o gateway de conexão está escutando.
4. Execute o comando `klnagchk -restart -tl 4` para iniciar o serviço do Agente de Rede.

O dispositivo é migrado e conectado com o novo Servidor de Administração por meio do novo gateway conectado.

Grupamentos e matrizes de servidores

O Kaspersky Security Center suporta a tecnologia de grupamento. Se o Agente de Rede enviar uma informação ao Servidor de Administração confirmando que o aplicativo instalado no dispositivo cliente faz parte de uma matriz de servidor, este dispositivo cliente torna-se um nó de cluster. O cluster será adicionado como um objeto individual na pasta **Dispositivos gerenciados** na árvore do console com o ícone Servidores ().

Alguns recursos típicos de um grupamento podem ser distinguidos:

- Um grupamento e qualquer um de seus nós estão sempre no mesmo grupo de administração.
- Se o administrador tentar mover um nó de grupamento, o nó voltará para sua localização original.
- Se o administrador tentar mover um cluster para um grupo diferente, todos os seus nós serão movidos com ele.

Ativar, desativar e reiniciar remotamente dispositivos clientes

O Kaspersky Security Center lhe permite gerenciar dispositivos cliente remotamente ao ligá-los, desligá-los ou reiniciando-os.

Para gerenciar remotamente os dispositivos cliente:

1. Conecte-se ao Servidor de Administração que gerencia os dispositivos.
2. Crie uma tarefa de gerenciamento de dispositivo usando uma das seguintes formas:
   - Se você precisar ligar, desligar ou reiniciar os dispositivos incluídos no grupo de administração selecionado, crie uma tarefa para o grupo selecionado.
   - Se você deve ligar, desligar ou reiniciar os dispositivos incluídos em vários grupos de administração ou que não pertençam a nenhum deles, crie uma tarefa para dispositivos específicos.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente. Na janela **Selecionar o tipo de tarefa** do Assistente para novas tarefas, selecione o nó **Kaspersky Security Center**, abra a pasta **Avançado** e selecione a tarefa **Gerenciar dispositivos**.
3. Execute a tarefa criada.

   Após a conclusão da tarefa, o comando (ativar, desativar ou reiniciar) será executado nos dispositivos selecionados.

Sobre o uso da conexão contínua entre um dispositivo gerenciado e o Servidor de Administração

Por padrão, o Kaspersky Security Center não apresenta a conectividade contínua entre os dispositivos gerenciados e o Servidor de Administração. Os Agentes de Rede em dispositivos gerenciados periodicamente estabelecem conexões e sincronizam com o Servidor de Administração. O intervalo entre essas sessões de sincronização é definido em uma política do Agente de Rede e é, por padrão, 15 minutos. Se for necessária uma sincronização antecipada (por exemplo, para forçar a aplicação de uma política), o Servidor de Administração envia um pacote de rede assinado para o Agente de Rede na porta UDP 15000. (O Servidor de Administração pode enviar este pacote por uma rede IPv4 ou IPv6.) Se nenhuma conexão por UDP for possível entre o Servidor de Administração e um dispositivo gerenciado por qualquer motivo, a sincronização será executada na próxima conexão de rotina entre o Agente de Rede e o Servidor de Administração dentro do intervalo de sincronização.

No entanto, algumas operações não podem ser realizadas sem uma conexão antecipada entre o Agente de Rede e o Servidor de Administração. Essas operações incluem executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado e criar um túnel. Para tornar essas operações possíveis, você deve ativar a opção **Não desconectar do Servidor de Administração** no dispositivo gerenciado.

Sobre a sincronização forçada

Embora o Kaspersky Security Center automaticamente sincronize o status, configurações, tarefas e políticas para dispositivos gerenciados, em alguns casos o administrador precisa saber exatamente se a sincronização já foi executada para um dispositivo especificado no presente momento.

No menu de contexto dos dispositivos gerenciados no Console de Administração, o item de menu **Todas as tarefas** contém o comando **Forçar a sincronização**. Quando o Kaspersky Security Center 14.2 executa este comando, o Servidor de Administração tenta se conectar ao dispositivo. Se esta tentativa for bem sucedida, a sincronização forçada será executada. Caso contrário, a sincronização será forçada somente após a próxima conexão entre o Agente de Rede e o Servidor de Administração.

Sobre o agendador de conexão

Na janela de propriedades do Agente de Rede, na seção **Conectividade**, na subseção **Agendador de conexão**, você poderá especificar intervalos de tempo durante os quais o Agente de Rede transmitirá dados ao Servidor de Administração.

Conectar quando necessário. Se esta opção estiver selecionada, a conexão é estabelecida quando o Agente de Rede tem de enviar dados para o Servidor de Administração.

Conectar-se nos intervalos de tempo especificados. Se esta opção estiver selecionada, o Agente de Rede se conecta ao Servidor de Administração numa hora específica. Você pode adicionar vários períodos de tempo de conexão.

Enviar mensagens aos usuários de dispositivos

Para enviar uma mensagem aos usuários de dispositivos:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. Crie uma mensagem enviando a tarefa para os usuários de dispositivo em uma das seguinte formas:
   - Se você desejar enviar um mensagem aos usuários de dispositivos cliente que pertençam ao grupo de administração selecionado, crie uma tarefa para o grupo selecionado.
   - Se você desejar enviar mensagem aos usuários de dispositivos que pertençam a diferentes grupos de administração ou que não pertençam a nenhum grupo de administração, crie uma tarefa para dispositivos específicos.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.
3. Na janela de tipo de tarefa do assistente para novas tarefas, selecione o nó do **Servidor de Administração do Kaspersky Security Center**, abra a pasta **Avançado** e selecione a tarefa **Enviar mensagem ao usuário**. A tarefa Enviar mensagens ao usuário está disponível apenas para dispositivos que executam o Windows. Você também pode enviar mensagens no menu de contexto do usuário, na pasta **Contas de usuário**.
4. Execute a tarefa criada.

   Após a conclusão da tarefa, a mensagem criada será enviada aos usuários dos dispositivos selecionados. A tarefa Enviar mensagens ao usuário está disponível apenas para dispositivos que executam o Windows. Você também pode enviar mensagens no menu de contexto do usuário, na pasta **Contas de usuário**.

Gerenciar o Kaspersky Security for Virtualization

O Kaspersky Security Center oferece suporte à opção de conexão de máquinas virtuais ao Servidor de Administração. As máquinas virtuais são protegidas pelo Kaspersky Security for Virtualization. Para obter mais detalhes, consulte a documentação deste aplicativo.

Configurar a alternância dos status do dispositivo

Você pode alterar as condições para atribuir o status *Crítico* ou *Advertência* para um dispositivo.

Para ativar a alteração do status do dispositivo para Crítico:

1. Abra a janela Propriedades em uma das seguintes formas:
   - Na pasta **Políticas** no menu de contexto de uma política de Servidor de Administração, selecione **Propriedades**.
   - Selecione **Propriedades** no menu de contexto de um grupo de administração.
2. Na janela de **Propriedades** que se abre, no painel **Seções**, selecione **Status do dispositivo**.

3. No painel direito, na seção **Se especificados, definir como Crítico**, selecione a caixa de seleção ao lado de uma condição na lista.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

4. Clique duas vezes no nome da condição selecionada e, na janela que será aberta, defina o valor necessário para a condição.

   Não é possível definir valores para as seguintes condições: O aplicativo de segurança não está instalado, Aplicativos incompatíveis estão instalados, Foram detectadas vulnerabilidades de software, As configurações do dispositivo móvel não estão em conformidade com a política, Incidentes não processados detectados, Status do dispositivo definido pelo aplicativo, O dispositivo está sem gerenciamento, O aplicativo de segurança não está em execução, A licença expirou.

   Para a condição **A reinicialização é necessária**, é possível especificar os motivos da reinicialização. Recomendamos marcar as caixas de seleção ao lado de todos os motivos da lista.

5. Clique em **OK**.

Quando condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Crítico*.

Para ativar a alteração do status do dispositivo para Advertência:

1. Abra a janela Propriedades em uma das seguintes formas:

   - Na pasta **Políticas**, no menu de contexto da política de Servidor de Administração, selecione **Propriedades**.
   - Selecione **Propriedades** no menu de contexto do grupo de administração.

2. Na janela de **propriedades** que se abre, no painel **Seções**, selecione **Status do dispositivo**.

3. No painel direito, na seção **Se especificados, definir como Advertência**, selecione a caixa de seleção ao lado de uma condição na lista.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

4. Clique duas vezes no nome da condição selecionada e, na janela que será aberta, defina o valor necessário para a condição.

   Não é possível definir valores para as seguintes condições: O aplicativo de segurança não está instalado, Aplicativos incompatíveis estão instalados, Foram detectadas vulnerabilidades de software, As configurações do dispositivo móvel não estão em conformidade com a política, Incidentes não processados detectados, Status do dispositivo definido pelo aplicativo, O dispositivo está sem gerenciamento, O aplicativo de segurança não está em execução, A licença expirou.

   Para a condição **A reinicialização é necessária**, é possível especificar os motivos da reinicialização. Recomendamos marcar as caixas de seleção ao lado de todos os motivos da lista.

5. Clique em **OK**.

Quando as condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Advertência*.

Atribuindo tags a dispositivos e visualizando tags atribuídas

O Kaspersky Security Center permite atribuir tags a dispositivos. Uma *tag* é a ID de um dispositivo que pode ser usada para agrupar, descrever ou encontrar dispositivos. As tags atribuídas aos dispositivos podem ser usadas para criar seleções, para encontrar dispositivos, e para distribuir dispositivos entre grupos de administração.

Você pode identificar os dispositivos manualmente ou automaticamente. Identificar um dispositivo manualmente nas propriedades de dispositivo; você pode usar a identificação manual quando tiver que identificar um dispositivo individual. A atribuição automática de tags é executada pelo Servidor de Administração de acordo com as regras de identificação especificadas.

Nas propriedades de um Servidor de Administração, você pode atribuir tags automaticamente a dispositivos gerenciados por este Servidor de Administração. Os dispositivos são identificados automaticamente quando as regras especificadas são atendidas. Uma regra individual corresponde a cada tag. As regras são aplicadas às propriedades da rede do dispositivo, sistema operacional, aplicativos instalados no dispositivo e outras propriedades de dispositivo. Por exemplo, você pode definir uma regra que atribuirá a tag *Win* à todos os dispositivos que executam o Windows. Então, você pode usar esta tag ao criar uma seleção de dispositivo; isto ajudará a classificar todos os dispositivos que executam o Windows e atribuir-lhes uma tarefa.

Você também pode usar tags como as condições da ativação do perfil da política em um dispositivo gerenciado para poder aplicar perfis de política específicos somente em dispositivos com tags específicas. Por exemplo, se um dispositivo identificado como *Correio* aparecer no grupo de administração *de Usuários* e se a ativação do perfil da política correspondente pela tag *Correio* tiver sido ativada, então a política criada para o grupo *Usuários* não será aplicada a este dispositivo – mas o perfil do perfil da política será aplicado. O perfil da política pode permitir que este dispositivo inicie alguns aplicativos que foram bloqueados de ser executados pela política.

Você pode criar múltiplas regras de identificação. A um dispositivo único pode ser atribuído múltiplas regras de identificação e se as respetivas condições destas regras forem atendidas simultaneamente. Você pode ver a lista de todos as tags atribuídas nas propriedades do dispositivo. Cada regra de identificação pode ser ativada ou desativada. Se uma regra for ativada, ela é aplicada aos dispositivos gerenciados pelo Servidor de Administração. Se você não estiver usando uma regra atualmente mas puder precisar dela no futuro, não terá que removê-la; basta simplesmente desmarcar a caixa de seleção **Ativar regra**. Neste caso, a regra é desativada; ela não será executada até que a caixa de seleção **Ativar regra** seja novamente selecionada. Você poderá precisar desativar uma regra sem removê-lo se tiver de excluir a regra da lista de regras de identificação temporariamente e logo inclui-la novamente.

Identificação automática do dispositivo

Você pode criar e editar as regras de identificação automática na janela Propriedades do Servidor de Administração.

Para identificar dispositivos automaticamente:

1. No árvore do console, selecione o nó com o nome do Servidor de Administração para o qual você tem de especificar regras de identificação.

2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.

3. Na janela de propriedades do Servidor de Administração, selecione a seção **Regras de aplicação de tags**.

4. Na seção **Regras de aplicação de tags**, clique no botão **Adicionar**.

   A janela **Nova regra** se abre.

5. Na janela **Nova regra**, configure as propriedades gerais da regra:

   - Especifique o nome da regra.

     O nome de regra não pode conter mais de 255 caracteres e não pode incluir nenhum caractere especial (tal como `"*<>?\:|`).

   - Ative ou desative a regra usando a caixa de seleção **Ativar regra**.

     Por padrão, esta caixa de seleção **Ativar regra** está selecionada.

   - No campo **Tag**, insira um nome de tag.

     O nome da tag não pode conter mais de 255 caracteres e não pode incluir nenhum caractere especial (tal como `"*<>?\:|`).

6. Na seção **Condições**, clique no botão **Adicionar** para adicionar uma nova condição, ou clique no botão **Propriedades** para editar uma condição existente.

   A janela do Assistente de nova condição de regra e identificação automática se abre.

7. Na janela **Condição de atribuição da tag**, selecione as caixas de seleção para as condições que devem afetar a identificação. Você pode selecionar múltiplas condições.

8. Dependendo de quais condições de identificação você selecionou, o assistente exibe as janelas para a configuração das condições correspondentes. Defina o acionamento da regra de acordo com as seguintes condições:

   - **Uso ou associação do dispositivo com uma rede específica** – Propriedades da rede do dispositivo, tal como um nome de dispositivo na rede Windows, e a inclusão do dispositivo em um domínio ou em uma sub-rede IP.

     > Caso o agrupamento com distinção entre maiúsculas e minúsculas seja definido para o banco de dados usado para o Kaspersky Security Center, mantenha maiúsculas e minúsculas ao especificar um nome DNS de dispositivo. Caso contrário, a regra de marcação automática não funcionará.

   - **Uso do Active Directory** – Presença do dispositivo em uma unidade organizacional do Active Directory e a associação do dispositivo em um grupo do Active Directory.

   - **Aplicativos específicos** – Presença do Agente de Rede no dispositivo, tipo de sistema operacional, versão e arquitetura.

   - **Máquinas virtuais** – Inclusão do dispositivo em um tipo específico de máquinas virtuais.

   - **Aplicativo do registro de aplicativos instalado** – Presença de aplicativos de diferentes fornecedores no dispositivo.

9. Após a configuração da condição, insira um nome para ela, e então feche o assistente.

   Se necessário, você pode definir múltiplas condições para única regra. Neste caso, a tag será atribuída um dispositivo se atender ao menos uma condição. As condições adicionadas serão exibidas na janela de propriedades da regra.

10. Clique em **OK** na janela **Nova regra** e clique em **OK** na janela de propriedades do Servidor de Administração.

As regras recentemente criadas têm o cumprimento exigido nos dispositivos gerenciados pelo Servidor de Administração selecionado. Se as configurações de um dispositivo atenderem as condições da regra, ao dispositivo é atribuído à tag.

Exibir e configurar tags atribuídas a um dispositivo

Você pode exibir a lista de todas as tags que foram atribuídas a um dispositivo, assim como seguir para a configuração de regras de identificação automáticas na janela Propriedades do dispositivo.

Para exibir e para configurar as tags que foram atribuídas a um dispositivo:

1. Na árvore do console, abra a pasta **Dispositivos gerenciados**.
2. No espaço de trabalho da pasta **Dispositivos gerenciados**, selecione o dispositivo para o qual você quer visualizar as tags atribuídas.
3. No menu de contexto do dispositivo móvel, selecione **Propriedades**.
4. Na janela de propriedades do dispositivo, selecione a seção **Identificadores**.

   Uma lista de tags atribuídas ao dispositivo selecionado é exibida, assim como o caminho em qual cada uma dos tags foram atribuídas: manualmente ou segundo uma regra.
5. Se necessário, execute uma das seguintes ações:
   - Para prosseguir para a configuração de regras de identificação, clique no link **Configurar as regras de identificação automática** (somente para Windows).
   - Para renomear uma tag, selecione uma e clique no botão **Renomear**.
   - Para remover uma tag, selecione uma e clique no botão **Remover**.
   - Para adicionar uma tag manualmente, insira uma no campo na parte inferior da seção **Tags** e clique no botão **Adicionar**.
6. Clique no botão **Aplicar**, se você tiver feito modificações na seção **Identificadores**, para as suas modificações tenham efeito.
7. Clique em **OK**.

Se você removeu ou renomeou uma tag nas Propriedades do dispositivo, esta modificação não afetará as regras de identificação que foram definidas nas Propriedades do Servidor de Administração. A modificação somente será aplicada ao dispositivo à cujas propriedades ela foi feita.

Diagnóstico remoto de dispositivos cliente. Utilitário de diagnóstico remoto do Kaspersky Security Center

O utilitário para diagnóstico remoto do Kaspersky Security Center (aqui referido como o utilitário de diagnóstico remoto) é concebido para a execução remota das seguintes operações em dispositivos cliente:

- Ativar e desativar o rastreio, alterar o nível de rastreio, baixar o arquivo de rastreio.
- Download de informações do sistema e de configurações do aplicativo.
- Download de registros de eventos.

- Gerar um arquivo de dump para um aplicativo.
- Início do diagnóstico e download de seus relatórios.
- Iniciar e parar aplicativos.

Você pode usar registros de eventos e relatórios de diagnóstico baixados de um dispositivo cliente para resolver problemas. Além disso, um especialista de Suporte Técnico da Kaspersky pode pedir que você faça download de arquivos de rastreio, de arquivos de dump, de registros de evento e de relatórios de diagnóstico de um dispositivo cliente para análise adicional na Kaspersky.

O utilitário de diagnóstico remoto é instalado automaticamente no dispositivo junto com o Console de Administração.

Conexão do utilitário de diagnóstico remoto com dispositivo cliente

Para conectar o utilitário de diagnóstico remoto a um dispositivo cliente:

1. Selecione um grupo de administração na árvore do console.
2. No espaço de trabalho, na guia **Dispositivos**, no menu de contexto de qualquer dispositivo, selecione **Ferramentas personalizadas → Diagnóstico remoto**.

   A janela principal do utilitário de diagnóstico remoto se abre.
3. No primeiro campo da janela principal do utilitário de diagnóstico remoto, especifique as ferramentas que você pretende usar para se conectar ao dispositivo cliente:
   - **Acesso usando a rede do Microsoft Windows**.
   - **Acesso usando o Servidor de Administração**.
4. Se você selecionou **Acesso usando a rede do Microsoft Windows** no primeiro campo da janela principal do utilitário, execute as seguintes ações:
   - No campo **Dispositivo**, especifique o endereço do dispositivo ao qual você precisa conectar-se

     Você pode usar um endereço IP, nome de NetBIOS ou nome do DNS como o endereço do dispositivo.

     O valor padrão é o endereço do dispositivo no menu de contexto no qual o utilitário foi iniciado.
   - Especifique uma conta para se conectar ao dispositivo:
     - **Conecte como usuário atual** (selecionado por padrão). Conectar-se usando a conta do usuário atual.
     - **Use o nome de usuário e senha fornecidos para conexão**. Conectar-se usando uma conta do usuário fornecida. Especifique o **Nome de usuário** e **Senha** da conta desejada.

     A conexão a um dispositivo cliente somente é possível sob a conta do administrador local do dispositivo cliente.

5. Se você selecionou **Acesso usando o Servidor de Administração** no primeiro campo da janela principal do utilitário, execute as seguintes ações:

   - No campo **Servidor de Administração**, especifique o endereço do Servidor de Administração a partir do qual você pretende se conectar ao dispositivo.

     Você pode usar um endereço IP, nome de NetBIOS ou nome do DNS como o endereço do servidor.

     O valor predefinido é o endereço do Servidor de Administração a partir do qual o utilitário tem sido executado.

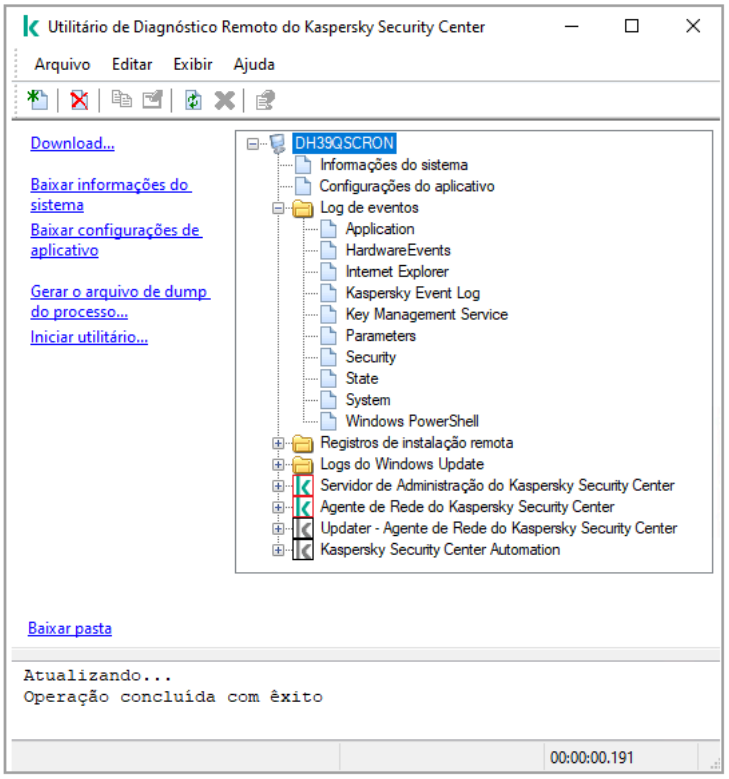
   - Se necessário, selecione as caixas de seleção **Usar SSL**, **Compactar o tráfego** e **O dispositivo pertence ao Servidor de Administração secundário**.

     Se a caixa de seleção **O dispositivo pertence ao Servidor de Administração secundário** estiver marcada, você pode preencher o campo **O dispositivo pertence ao Servidor de Administração secundário** com o nome do Servidor de Administração secundário que gerencia o dispositivo ao clicar no botão **Procurar**.

6. Para se conectar-se ao dispositivo, clique no botão **Login**.

Você tem que autorizar usando a verificação em duas etapas se este recurso estiver ativado para sua conta.

Isso abre a janela elaborada para o diagnóstico remoto do dispositivo (consulte a figura abaixo). A parte esquerda da janela contém links para operações de diagnóstico do dispositivo. A parte direita da janela contém a árvore de objetos do dispositivo com o qual o utilitário pode operar. A parte inferior da janela exibe o andamento das operações do utilitário.



Utilitário de diagnóstico remoto. Janela Diagnóstico de dispositivo remoto

O utilitário de diagnóstico remoto salva os arquivos baixados de dispositivos cliente no espaço de trabalho do dispositivo que o iniciou.

Gerar um arquivo de dump para um aplicativo

Um arquivo de despejo de aplicativo permite visualizar os parâmetros do aplicativo em execução em um dispositivo cliente em um determinado momento. Esse arquivo também contém informações sobre os módulos que foram carregados para um aplicativo.

A obtenção de despejos de dispositivos baseados em Linux não é compatível.

Para obter despejos por meio do diagnóstico remoto, o utilitário kldumper é usado. Esse utilitário foi desenvolvido para obter os despejos de processos dos aplicativos da Kaspersky mediante solicitação de especialistas do suporte técnico. Informações detalhadas sobre os requisitos para usar o utilitário kldumper são fornecidas na base de conhecimento do Kaspersky Security Center.

Para criar um arquivo de despejo para um aplicativo:

1. No espaço de trabalho da pasta **Dispositivos gerenciados**, na guia **Dispositivos**, abra o menu de contexto do dispositivo necessário e selecione **Ferramentas personalizadas → Diagnóstico remoto**.

   A janela **Utilitário de Diagnóstico Remoto do Kaspersky Security Center** é aberta.

2. Conexão do utilitário de diagnóstico remoto com um dispositivo cliente.

   Isso abre a janela elaborada para o diagnóstico remoto do dispositivo.

3. Na parte esquerda da janela, clique no link **Gerar o arquivo de dump do processo**

4. Na janela **Gerando o arquivo de dump do processo** aberta, especifique o arquivo executável do aplicativo para o qual deseja gerar um arquivo de despejo.

5. Clique no botão **OK**.

   Um arquivo comprimido com o arquivo de despejo para o aplicativo especificado é baixado.

   Caso o aplicativo especificado não esteja em execução no dispositivo cliente, a pasta "resultado" contida no arquivo comprimido baixado estará vazia.

   Caso o aplicativo especificado esteja em execução, mas o download falhe com um erro ou a pasta "result" (resultado) contida no arquivo comprimido baixado esteja vazia, consulte a Base de Dados de Conhecimento do Kaspersky Security Center.

Ativação e desativação de rastreio, download de arquivos de rastreio

Para ativar o rastreio em um dispositivo remoto:

1. Execute o utilitário de diagnóstico remoto e conecte-se ao dispositivo necessário.
2. Na árvore de objetos do dispositivo, selecione o aplicativo para o qual deseja ativar o rastreio.

   O rastreio somente pode ser ativado ou desativado para aplicativos com autodefesa se o dispositivo estiver conectado usando ferramentas do Servidor de Administração.

   Se quiser ativar o rastreio para o Agente de Rede, também pode fazê-lo ao criar a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades. Nesse caso, o Agente de Rede gravará as informações mesmo se o rastreio estiver desativado para o Agente de Rede no utilitário de diagnóstico remoto.

3. Para ativar o rastreio:

   a. Na parte esquerda da janela do utilitário de diagnóstico remoto, clique em **Ativar rastreamento**.

   b. Na janela **Selecionar nível de rastreamento** que se abre, recomendamos que você mantenha os valores padrões das configurações. Quando necessário, um especialista de Suporte Técnico orientará você através do processo de configuração. Estão disponíveis as seguintes configurações:

   - **Nível de rastreamento**

     O nível de rastreamento define o volume de detalhes que o arquivo de rastreamento contém.

   - **Rastreamento baseado em rotatividade** (disponível apenas para o Kaspersky Endpoint Security)

     O aplicativo sobrescreve as informações de rastreamento para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o número máximo de arquivos a serem usados para armazenar as informações de rastreamento e o tamanho máximo de cada arquivo. Se o número máximo de arquivos de rastreamento com o tamanho máximo estiver gravado, o arquivo de rastreamento mais antigo será excluído para que um novo arquivo possa ser gravado.

   c. Clique em **OK**.

4. Para o Kaspersky Endpoint Security, um especialista de Suporte Técnico pode solicitar que você ative o rastreamento do Xperf para obter informações sobre o desempenho do sistema.

   Para ativar o rastreio do Xperf:

   a. Na parte esquerda da janela do utilitário de diagnóstico remoto, clique em **Ativar rastreamento Xperf**.

   b. Na janela **Selecionar nível de rastreamento** que se abre, dependendo da solicitação do especialista de Suporte Técnico, selecione um dos seguintes níveis de rastreio:

   - **Nível leve**

     Um arquivo de rastreamento deste tipo contém a quantidade mínima de informações sobre o sistema.

     Por padrão, esta opção está selecionada.

   - **Nível profundo**

     Um arquivo de rastreamento deste tipo contém informações mais detalhadas do que as dos arquivos de rastreamento do tipo *Superficial* e podem ser solicitadas pelos especialistas de Suporte Técnico quando um arquivo de rastreamento do tipo *Superficial* não for suficiente para a avaliação de desempenho. Um arquivo de rastreamento *Profundo* contém informações técnicas sobre o sistema, como as informações sobre hardware, sistema operacional, lista de processos e aplicativos iniciados e concluídos, eventos usados para avaliação de desempenho e eventos da Ferramenta de Avaliação de Sistema do Windows.

   c. Selecione um dos seguintes tipos de rastreio:

   - **Tipo básico**

As informações de rastreamento são recebidas durante a operação do aplicativo Kaspersky Endpoint Security.

Por padrão, esta opção está selecionada.

- Tipo na reinicialização

  As informações de rastreamento são recebidas quando o sistema operacional é iniciado no dispositivo gerenciado. Esse tipo de rastreamento é eficaz quando o problema que afeta o desempenho do sistema ocorre depois que o dispositivo é ligado e antes da inicialização do Kaspersky Endpoint Security.

d. Você também pode receber a solicitação de ativar a opção **Rastreamento baseado em rotatividade** para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o tamanho máximo do arquivo de rastreamento. Quando o arquivo atingir o tamanho máximo, as informações de rastreamento mais antigas serão substituídas por novas informações.

e. Clique em **OK**.

Em alguns casos, um aplicativo de segurança e sua tarefa devem ser reiniciados para que seja possível ativar o rastreamento.

O utilitário de diagnóstico remoto ativa o rastreio do aplicativo selecionado.

Para fazer download do arquivo de rastreamento de um aplicativo:

1. Execute o utilitário de diagnóstico remoto e conecte-o ao dispositivo necessário, como descrito em "Conexão do utilitário de diagnóstico remoto com dispositivo cliente".
2. No nó do aplicativo, na pasta **Arquivos de rastreamento**, selecione o arquivo necessário.
3. Na parte esquerda da janela do utilitário de diagnóstico remoto, clique em **Baixar todo o arquivo**.

   Para os arquivos grandes, as partes do rastreio mais recentes podem ser baixadas.

   Você pode excluir o arquivo de rastreio destacado. O arquivo pode ser excluído depois de o rastreio estar desabilitado.

O arquivo selecionado será baixado no local especificado na parte inferior da janela.

Para desativar o rastreio no dispositivo remoto:

1. Execute o utilitário de diagnóstico remoto e conecte-o ao dispositivo necessário, como descrito em "Conexão do utilitário de diagnóstico remoto com dispositivo cliente".
2. Na árvore de objetos do dispositivo, selecione o aplicativo para o qual deseja desativar o rastreio.

   O rastreio somente pode ser ativado ou desativado para aplicativos com autodefesa se o dispositivo estiver conectado usando ferramentas do Servidor de Administração.

3. Na parte esquerda da janela do utilitário de diagnóstico remoto, clique em **Desabilitar rastreamento**.

O utilitário de diagnóstico remoto desativa o rastreio do aplicativo selecionado.

Download das configurações do aplicativo

Para baixar as configurações do aplicativo a partir de um dispositivo remoto:

1. Execute o utilitário de diagnóstico remoto e conecte-o ao dispositivo necessário, como descrito em "Conexão do utilitário de diagnóstico remoto com dispositivo cliente".
2. Na árvore de objetos da janela do utilitário de diagnóstico remoto, selecione o nó superior com o nome do dispositivo.
3. Na parte esquerda da janela do utilitário de diagnóstico remoto, selecione a ação necessária entre as seguintes opções:
   - **Baixar informações do sistema**
   - **Baixar configurações de aplicativo**
   - **Gerar o arquivo de dump do processo**

     Na janela que se abre depois que você clicar neste link, especifique o arquivo executável do aplicativo para o qual você precisa gerar um arquivo de dump de memória.
   - **Iniciar utilitário**

     Na janela que se abre depois que você clicar neste link, especifique o arquivo executável do utilitário que deseja iniciar e suas configurações de execução.

O utilitário selecionado é baixado e baixado e iniciado no dispositivo.

Download de registros de eventos

Para baixar um log de eventos a partir de um dispositivo remoto:

1. Execute o utilitário de diagnóstico remoto e conecte-o ao dispositivo necessário, como descrito em "Conexão do utilitário de diagnóstico remoto com dispositivo cliente".
2. Na pasta **Log de eventos do sistema** da árvore do objeto de dispositivo, selecione o registro relevante.
3. Baixe o registro selecionado clicando no link **Baixar log de eventos <Nome do log de eventos>** na parte esquerda da janela do utilitário de diagnóstico remoto.

O log de eventos selecionado será baixado no local especificado no painel inferior.

Download de múltiplos itens de informações de diagnóstico

O utilitário de diagnóstico remoto do Kaspersky Security Center permite que você baixe vários itens de informações de diagnóstico, incluindo registros de eventos, informações do sistema, arquivos de rastreio e arquivos de dump.

Para baixar as configurações de diagnóstico a partir de um dispositivo remoto:

1. Execute o utilitário de diagnóstico remoto e conecte-o ao dispositivo necessário, como descrito em "Conexão do utilitário de diagnóstico remoto com dispositivo cliente".
2. Na parte esquerda da janela do utilitário de diagnóstico remoto, clique em **Download**.
3. Marque as caixas de seleção ao lado dos itens que você deseja baixar.
4. Clique em **Iniciar**.

Cada item selecionado será baixado no local especificado no painel inferior.

Início do diagnóstico e download dos resultados

Para iniciar o diagnóstico para um aplicativo em um dispositivo remoto e baixar os resultados:

1. Execute o utilitário de diagnóstico remoto e conecte-o ao dispositivo necessário, como descrito em "Conexão do utilitário de diagnóstico remoto com dispositivo cliente".
2. Selecione o aplicativo necessário na árvore de objetos do dispositivo.
3. Inicie o diagnóstico clicando no link **Executar diagnósticos** na parte esquerda da janela do utilitário de diagnóstico remoto.

   Um relatório de diagnóstico aparece no nó do aplicativo selecionado na árvore de objetos.
4. Selecione o relatório de diagnóstico recentemente gerado na árvore de objetos e baixe o mesmo clicando no link **Baixar pasta**.

O relatório selecionado será baixado no local especificado no painel inferior.

Início, interrupção e reinício de aplicativos

Você somente pode iniciar, parar e reiniciar aplicativos se tiver conectado o dispositivo usando as ferramentas do Servidor de Administração.

Para iniciar, interromper ou reiniciar um aplicativo:

1. Execute o utilitário de diagnóstico remoto e conecte-o ao dispositivo necessário, como descrito em "Conexão do utilitário de diagnóstico remoto com dispositivo cliente".
2. Selecione o aplicativo necessário na árvore de objetos do dispositivo.
3. Selecione uma ação na parte esquerda da janela do utilitário de diagnóstico remoto:
   - **Interromper o aplicativo**
   - **Reiniciar aplicativo**
   - **Iniciar o aplicativo**

Dependendo da ação que você selecionou, o aplicativo está iniciado, parado ou reiniciado.

Dispositivos de proteção UEFI

Um *dispositivo de proteção UEFI* é um dispositivo com uma solução ou aplicativo da Kaspersky para UEFI integrado no nível da BIOS. A proteção integrada assegura a segurança do dispositivo do momento do início do sistema, enquanto a proteção nos dispositivos sem software integrado somente começa a funcionar após o início do aplicativo de segurança. O Kaspersky Security Center suporta o gerenciamento destes dispositivos.

Para modificar as configurações de conexão de dispositivos de proteção UEFI:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, selecione **Configurações de conexão do servidor** → **Portas adicionais**.
4. Na seção **Portas adicionais**, modifique as configurações relevantes:
   - **Abrir porta para os dispositivos de proteção UEFI e dispositivos KasperskyOS**

     Os dispositivos de proteção UEFI poderão ser conectados ao Servidor de Administração.

   - **Porta para os dispositivos de proteção UEFI e dispositivos KasperskyOS**

     Você pode alterar o número da porta se a opção **Abrir porta para os dispositivos de proteção UEFI e dispositivos KasperskyOS** estiver ativada. O número da porta padrão é 13294.
5. Clique em **OK**.

Configurações de um dispositivo gerenciado

Para exibir as configurações de um dispositivo gerenciado:

1. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.
2. No espaço de trabalho da pasta, selecione um dispositivo.
3. No menu de contexto do dispositivo, selecione **Propriedades**.

A janela Propriedades do dispositivo selecionado abre com a seção **Geral** selecionada.

Geral

A seção **Geral** exibe as informações gerais sobre o dispositivo cliente. As informações são fornecidas com base nos dados recebidos durante a última sincronização do dispositivo cliente com o Servidor de Administração:

- **Nome**

  Neste campo, você poderá visualizar e modificar o nome de um dispositivo cliente no grupo de administração.

- **Descrição**

  Nesse campo, você poderá inserir uma descrição adicional de um dispositivo cliente.

- **Domínio do Windows**

  O domínio do Windows ou o grupo de trabalho, que contém o dispositivo.

- **Nome do NetBIOS**

  Nome de rede Windows do dispositivo cliente.

- **Nome DNS**

  Nome do domínio DNS do dispositivo cliente.

- **Endereço IP**

  Endereço IP do dispositivo.

- **Grupo**

  Grupo de administração que inclui o dispositivo cliente.

- **Última atualização**

  Data em que os bancos de dados de antivírus ou os aplicativos foram atualizados pela última vez no dispositivo.

- **Última visualização**

  Data e hora de quando o dispositivo esteve por último visível na rede.

- **Conectado ao Servidor de Administração**

  Data e hora da última vez que o Agente de Rede instalado no dispositivo cliente foi conectado ao Servidor de Administração.

- **Não desconectar do Servidor de Administração**

  Caso a opção seja ativada, será mantida uma conectividade contínua entre o dispositivo gerenciado e o Servidor de Administração. Convém usar a opção caso os servidores push, que fornecem a conectividade, não estejam sendo usados.

  Caso essa opção esteja desativada e os servidores push não estejam sendo utilizados, o dispositivo gerenciado somente se conectará ao Servidor de Administração para sincronizar dados ou transmitir informações.

  O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

  A opção é desativada por padrão em dispositivos gerenciados. A opção é ativada por padrão no dispositivo onde o Servidor de Administração está instalado e permanece ativada mesmo se você tentar desativá-la.

Proteção

A seção **Proteção** fornece informações sobre o status atual da proteção antivírus no dispositivo cliente:

- **Status do dispositivo**

  Status do dispositivo cliente atribuído com base nos critérios definidos pelo administrador para o status de proteção antivírus no dispositivo e na atividade do dispositivo na rede.

- **Todos os problemas**

  Esta tabela contém uma lista completa de problemas detectados pelos aplicativos gerenciados instalados no dispositivo cliente. Cada problema é acompanhado por um status, que o aplicativo sugere que você atribua ao dispositivo para esse problema.

- **Proteção em tempo real**

  Esse campo exibe o status atual da proteção em tempo real do dispositivo cliente.

  Quando o status é alterado no dispositivo, o novo status é exibido na janela de propriedades do dispositivo só depois que o dispositivo cliente é sincronizado com o Servidor de Administração.

- **Última verificação sob demanda**

  Data e hora em que a verificação de malwares foi executada por último no dispositivo cliente.

- **Número total de ameaças detectadas**

  Número total de ameaças detectadas no dispositivo cliente desde a instalação do aplicativo de segurança (primeira verificação) ou desde a última redefinição do contador de ameaças.

- **Ameaças ativas**

  Número de arquivos não processados no dispositivo cliente.

  Este campo ignora o número de arquivos não processados nos dispositivos móveis.

- **Status de criptografia do disco**

  O status atual da criptografia do arquivo nas unidades locais do dispositivo. Para obter uma descrição dos status, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

Aplicativos

A seção **Aplicativos** lista todos os aplicativos da Kaspersky instalados no dispositivo cliente: Essa seção contém o botão Iniciar () e o botão Interromper (), que permitem iniciar e interromper o aplicativo da Kaspersky selecionado (excluindo o Agente de Rede). Estes botões estarão ativados se a porta 15000 UDP estiver disponível no dispositivo gerenciado para recepção de notificações push do Servidor de Administração. Caso o dispositivo gerenciado não esteja disponível para notificações push, mas o modo estiver configurado para manter uma conexão contínua com o Servidor de Administração (com a opção **Não desconectar do Servidor de Administração** na seção **Geral** ativada), os botões iniciar e interromper ainda estarão disponíveis. Além disso, a seção **Aplicativos** contém os seguintes botões:

- **Eventos**

  Clique no botão para visualizar uma lista de eventos que ocorreram nos dispositivos cliente quando o aplicativo foi executado e para visualizar os resultados da tarefa para este aplicativo.

- **Estatísticas**

  Clique neste botão para visualizar as informações estatísticas atuais sobre o aplicativo.

- **Propriedades**

  Clique no botão para receber informações sobre o aplicativo e para configurar o aplicativo.

Tarefas

Na guia **Tarefas**, é possível gerenciar as tarefas do dispositivo cliente: visualizar a lista de tarefas existentes, criar novas, remover, iniciar e interromper tarefas, modificar as suas configurações e visualizar os resultados da execução. A lista de tarefas é fornecida com base nos dados recebidos durante a última sessão de sincronização do cliente com o Servidor de Administração. O Servidor de Administração solicita os detalhes do status de tarefa do dispositivo cliente.

Os botões iniciar (), interromper () e remover (unloc_red_cross_delete) estarão ativados se a porta 15000 UDP estiver disponível no dispositivo gerenciado para receber notificações push do Servidor de Administração. Caso o dispositivo gerenciado não esteja disponível para notificações push, mas o modo estiver configurado para manter uma conexão contínua com o Servidor de Administração (com a opção **Não desconectar do Servidor de Administração** na seção **Geral** ativada), os botões iniciar, interromper e remover ainda estarão disponíveis.

Caso a conexão não seja estabelecida, o status não será exibido e os botões ficarão desabilitados.

Eventos

A guia **Eventos** exibe os eventos registrados no Servidor de Administração para o dispositivo cliente selecionado.

Tags

Na guia **Tags**, é possível gerenciar a lista de palavras-chave que são usadas para localizar os dispositivos cliente: visualizar a lista de tags existentes, atribuir tags a partir da lista, configurar regras de identificação automática, adicionar novas tags, renomear as antigas e excluir tags.

Informação do sistema

A seção **Informações gerais do sistema** fornece informações sobre o aplicativo instalado em um dispositivo cliente.

Registro de aplicativos

Na seção **Registro de aplicativos**, é possível exibir o registro de aplicativos instalados no dispositivo cliente e suas atualizações, assim como configurar a exibição do registro de aplicativos.

Informações sobre os aplicativos instalados são fornecidas se o Agente de Rede instalado no dispositivo cliente enviar as informações necessárias ao Servidor de Administração. Você pode configurar o envio de informações para o Servidor de Administração na janela Propriedades do Agente de Rede ou sua política, na seção **Repositórios**.

- Exibir somente aplicativos de segurança incompatíveis

  Se esta opção estiver ativada, a lista de aplicativos contém apenas os aplicativos de segurança incompatíveis com aplicativos da Kaspersky.

  Por padrão, esta opção está desativada.

- Mostrar atualizações

  Caso essa opção esteja ativada, a lista de aplicativos contém não só os aplicativos, mas também os pacotes de atualização instalados para eles.

  Para exibir a lista de atualizações, são necessários 100 KB de tráfego. Caso a lista seja fechada e reaberta, será necessário gastar 100 KB de tráfego novamente.

  Por padrão, esta opção está desativada.

- Exportar para arquivo

  Clique neste botão para exportar a lista de aplicativos instalados no dispositivo para um arquivo CSV ou um arquivo TXT.

- Histórico

  Clique neste botão para exibir os eventos relativos à instalação de aplicativos no dispositivo. As informações que se seguem são exibidas:

  - Data e hora em que o aplicativo foi instalado no dispositivo
  - Nome do aplicativo
  - Versão do aplicativo

- Propriedades

  Clique neste botão para exibir as propriedades do aplicativo selecionado na lista de aplicativos instalados no dispositivo. As informações que se seguem são exibidas:

  - Nome do aplicativo
  - Versão do aplicativo
  - Fornecedor do aplicativo

Arquivos executáveis

A seção **Arquivos executáveis** exibe os arquivos executáveis encontrados no dispositivo cliente.

Registro de hardware

Na seção **Registro de hardware**, você poderá visualizar as informações sobre o hardware instalado no dispositivo cliente. Você pode ver essas informações para dispositivos Windows e Linux.

Verifique e confirme se o utilitário lshw está instalado nos dispositivos Linux a partir dos quais deseja buscar detalhes de hardware. Os detalhes de hardware obtidos de máquinas virtuais podem estar incompletos, dependendo do hipervisor usado.

Se o Agente de Rede estiver instalado em um dispositivo com Windows, ele enviará ao Servidor de Administração as seguintes informações sobre o hardware:

- RAM
- Dispositivos de armazenamento em massa
- Placa-mãe
- CPU

- Adaptadores de rede
- Monitores
- Adaptador de vídeo
- Placa de som

Se o Agente de Rede estiver instalado em um dispositivo com Linux ou macOS, ele enviará ao Servidor de Administração as seguintes informações sobre o hardware, caso o sistema operacional as forneça:

- Volume total de RAM
- Volume total de dispositivos de armazenamento em massa
- Placa-mãe
- CPU
- Adaptadores de rede

Sessões

A seção **Sessões** é exibida somente para os dispositivos Windows e contém as informações sobre o proprietário do dispositivo cliente, assim como as contas de usuários que trabalharam no dispositivo cliente selecionado.

As informações sobre usuários de domínio são geradas com base nos dados do Active Directory. Os detalhes de usuários locais são fornecidos pelo Windows Security Account Manager instalado no dispositivo cliente.

- **Proprietário do dispositivo**

  O campo **Proprietário do dispositivo** exibe o nome do usuário que pode ser contatado pelo administrador quando a necessidade surgir para executar determinadas operações no dispositivo cliente.

  Use os botões **Atribuir** e **Propriedades** para selecionar o proprietário do dispositivo e para exibir as informações sobre o usuário que foi indicado como o proprietário do dispositivo.

  Use o botão com a cruz vermelha para excluir o proprietário atual do dispositivo.

A lista exibe as contas dos usuários que trabalham no dispositivo cliente.

- **Nome**

  Nome do dispositivo na rede Windows.

- **Nome do participante**

  Nome (domínio ou local) do usuário que efetuou o login no sistema naquele dispositivo.

- **Conta**

  Conta do usuário que acessou esse dispositivo.

- **E-mail**

  Endereço de e-mail do usuário.

- **Telefone**

  Número de telefone do usuário.

Incidentes

Na guia **Incidentes**, é possível visualizar, editar e criar incidentes para o dispositivo cliente. Os incidentes podem ser criados automaticamente, através de aplicativos da Kaspersky gerenciados instalados no dispositivo cliente, ou manualmente pelo administrador. Por exemplo, se alguns usuários moverem regularmente malware de suas unidades removíveis para os dispositivos, o administrador poderá criar um incidente. O administrador pode fornecer no texto do incidente uma breve descrição do caso e as ações recomendadas (como ações disciplinares a serem tomadas contra um usuário) e pode adicionar um link para o usuário ou os usuários.

Um incidente no qual todas as ações necessárias tenham sido tomadas é chamado de *processado*. A presença de incidentes não processados pode ser escolhida como a condição para uma alteração do status do dispositivo para *Crítico* ou *Advertência*.

Essa seção contém uma lista de incidentes que foram criados para o de dispositivo. Os incidentes são classificados por nível de gravidade e tipo. O tipo de um incidente é definido pelo aplicativo da Kaspersky que cria o incidente. Você pode destacar incidentes processados na lista selecionando a caixa de seleção na coluna **Processado**.

Vulnerabilidades de software

A seção **Vulnerabilidades de software** fornece informações sobre as vulnerabilidades de aplicativos de terceiros instalados nos dispositivos cliente. Você pode usar o campo de pesquisa acima da lista para procurar as vulnerabilidades por nome.

- **Exportar para arquivo**

  Clique no botão **Exportar para arquivo** para salvar a lista de vulnerabilidades em um arquivo. Por padrão, o aplicativo exporta a lista de vulnerabilidades para um arquivo CSV.

- **Exibir somente vulnerabilidades que podem ser corrigidas**

  Se esta opção estiver ativada, a seção exibe vulnerabilidades que podem ser corrigidas usando um patch.

  Se essa opção estiver desativada, a seção exibe ambas as vulnerabilidades que podem ser corrigidas usando um patch, bem como as vulnerabilidades para as quais não foi lançado nenhum patch.

  Por padrão, esta opção está ativada.

- **Propriedades**

  Selecione uma vulnerabilidade de software na lista e clique no ícone **Propriedades** para exibir as propriedades da vulnerabilidade de software selecionada em uma janela separada. Na janela, você pode fazer o seguinte:

  - Ignore a vulnerabilidade de software neste dispositivo gerenciado (no Console de Administração ou no Kaspersky Security Center Web Console).
  - Consulte a lista de correções recomendadas para a vulnerabilidade.
  - Especifique manualmente as atualizações de software para corrigir a vulnerabilidade (no Console de Administração ou no Kaspersky Security Center Web Console).
  - Exibir as instâncias de vulnerabilidade.
  - Consulte a lista de tarefas existentes para corrigir a vulnerabilidade e crie novas tarefas para corrigir a vulnerabilidade.

Atualizações disponíveis

Esta seção exibe uma lista de atualizações de software encontradas neste dispositivo, mas ainda não instaladas. As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

- **Exibir atualizações instaladas**

  Se esta opção estiver ativada, a lista exibe as atualizações que não foram instaladas e aquelas que estão instaladas no dispositivo cliente.

  Por padrão, esta opção está desativada.

Políticas ativas

Esta seção exibe uma lista de políticas de aplicativos Kaspersky atualmente atribuídas a este dispositivo.

- Exportar para arquivo

  Você pode clicar no botão **Exportar para arquivo** para salvar a lista de perfis de políticas ativas em um arquivo. Por padrão, o aplicativo exporta a lista de políticas para um arquivo CSV.

Active policy profiles

- Perfis de política ativos

  A lista lhe permite visualizar as informações sobre os perfis de política existentes que estão ativas nos dispositivos cliente. Você pode usar a barra de pesquisa acima da lista para localizar os perfis de política ativos na lista ao inserir um nome de política ou um nome de perfil da política.

- Exportar para arquivo

  Você pode clicar no botão **Exportar para arquivo** para salvar a lista de perfis de política ativos em um arquivo. Por padrão, o aplicativo exporta a lista de perfis de política para um arquivo CSV.

Pontos de distribuição

Esta seção fornece uma lista de pontos de distribuição com os quais o dispositivo interage.

- Exportar para arquivo

  Clique no botão **Exportar para arquivo** para salvar a um arquivo de uma lista de pontos de distribuição com os quais o dispositivo interage. Por padrão, o aplicativo exporta a lista de dispositivos para um arquivo CSV.

- Propriedades

  Clique no botão **Propriedades** para exibir e configurar o ponto de distribuição com o qual o dispositivo interage.

Configurações da política gerais

Geral

Na seção **Geral**, você pode modificar o status da política e especificar a herança das configurações da política:

- No bloco **Status da política**, você poderá selecionar um dos modos de política:
  - **Política ativa**

    Se esta opção estiver selecionada, a política é habilitada.

    Por padrão, esta opção está selecionada.

  - **Política de ausência**

    Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

  - **Política inativa**

    Se esta opção estiver selecionada, a política é habilitada, mas continua armazenada na pasta **Políticas**. Se necessário, a política pode ser habilitada.

- No grupo de configurações **Herança de configurações**, você pode configurar a herança de política:
  - **Herdar configurações da política principal**

    Se esta opção estiver ativada, os valores das configurações de política são herdados da política de grupo de nível superior e, portanto são bloqueados.

    Por padrão, esta opção está ativada.

  - **Forçar herança de configurações nas políticas secundárias**

    Se esta opção estiver ativada, após a aplicação das alterações da política, as seguintes ações serão realizadas:

    - Os valores das configurações da política serão propagados às políticas de subgrupos de administração, ou seja, às políticas secundárias.
    - No bloco **Herança de configurações** da seção **Geral** na janela Propriedades de cada política secundária, a opção **Herdar configurações da política principal** será automaticamente ativada.

    Se a opção estiver ativada, as configurações das políticas secundárias são bloqueadas.

    Por padrão, esta opção está desativada.

Configuração de eventos

A seção **Configuração de eventos**, permite configurar o registro e a notificação de eventos. Os eventos são distribuídos por nível de importância nas seguintes guias:

- **Crítico**

  A guia **Crítico** não é exibida nas propriedades da política do Agente de Rede.

- **Falha funcional**
- **Advertência**
- **Informações**

Na cada guia, a lista de eventos exibe os tipos de eventos e o prazo de armazenamento de eventos padrão no Servidor de Administração (em dias). Clicar no botão **Propriedades** permite especificar as configurações do log de eventos e as notificações sobre eventos selecionados na lista. Por padrão, as configurações de notificação comuns especificadas para todo o Servidor de Administração são usadas para todos os tipos de evento. Contudo, você pode alterar configurações específicas dos tipos de evento necessários.

Por exemplo, na guia **Advertência**, é possível configurar o tipo de evento **Ocorreu um incidente**. Os eventos podem acontecer, por exemplo, quando o espaço livre em disco de um ponto de distribuição for inferior a 2 GB (pelo menos 4 GB são necessários para instalar aplicativos e baixar atualizações remotamente). Para configurar o evento **Ocorreu um incidente**, selecione-o e clique no botão **Propriedades**. Depois disso, será necessário especificar onde armazenar os eventos ocorridos e como notificá-los.

Caso o agente de rede tenha detectado um incidente, é possível gerenciá-lo usando as configurações de um dispositivo gerenciado.

Para selecionar múltiplos tipos de evento, use as teclas **Shift** ou **Ctrl**; para selecionar todos os tipos, use o botão **Selecionar tudo**.

Configurações de política do Agente de Rede

Para configurar uma política do Agente de Rede:

1. Na árvore do console, selecione a pasta **Políticas**.
2. No espaço de trabalho da pasta, selecione a política de Agente de rede.
3. No menu de contexto da política, selecione **Propriedades**.

A janela de propriedades da política do Agente de Rede se abre.

> Veja a tabela de comparação detalhando como as configurações abaixo se aplicam a depender do tipo de sistema operacional usado.

Geral

Na seção **Geral**, você pode modificar o status da política e especificar a herança das configurações da política:

- No bloco **Status da política**, você poderá selecionar um dos modos de política:
  - **Política ativa**

    Se esta opção estiver selecionada, a política é habilitada.

    Por padrão, esta opção está selecionada.

  - **Política de ausência**

    Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

  - **Política inativa**

    Se esta opção estiver selecionada, a política é habilitada, mas continua armazenada na pasta **Políticas**. Se necessário, a política pode ser habilitada.

- No grupo de configurações **Herança de configurações**, você pode configurar a herança de política:
  - **Herdar configurações da política principal**

    Se esta opção estiver ativada, os valores das configurações de política são herdados da política de grupo de nível superior e, portanto são bloqueados.

    Por padrão, esta opção está ativada.

  - **Forçar herança de configurações nas políticas secundárias**

    Se esta opção estiver ativada, após a aplicação das alterações da política, as seguintes ações serão realizadas:

    - Os valores das configurações da política serão propagados às políticas de subgrupos de administração, ou seja, às políticas secundárias.
    - No bloco **Herança de configurações** da seção **Geral** na janela Propriedades de cada política secundária, a opção **Herdar configurações da política principal** será automaticamente ativada.

    Se a opção estiver ativada, as configurações das políticas secundárias são bloqueadas.

    Por padrão, esta opção está desativada.

Configuração de eventos

A seção **Configuração de eventos**, permite configurar o registro e a notificação de eventos. Os eventos são distribuídos por nível de importância nas seguintes guias:

- **Crítico**

  A guia **Crítico** não é exibida nas propriedades da política do Agente de Rede.

- **Falha funcional**
- **Advertência**
- **Informações**

Na cada guia, a lista de eventos exibe os tipos de eventos e o prazo de armazenamento de eventos padrão no Servidor de Administração (em dias). Clicar no botão **Propriedades** permite especificar as configurações do log de eventos e as notificações sobre eventos selecionados na lista. Por padrão, as configurações de notificação comuns especificadas para todo o Servidor de Administração são usadas para todos os tipos de evento. Contudo, você pode alterar configurações específicas dos tipos de evento necessários.

Por exemplo, na guia **Advertência**, é possível configurar o tipo de evento **Ocorreu um incidente**. Os eventos podem acontecer, por exemplo, quando o espaço livre em disco de um ponto de distribuição for inferior a 2 GB (pelo menos 4 GB são necessários para instalar aplicativos e baixar atualizações remotamente). Para configurar o evento **Ocorreu um incidente**, selecione-o e clique no botão **Propriedades**. Depois disso, será necessário especificar onde armazenar os eventos ocorridos e como notificá-los.

Caso o agente de rede tenha detectado um incidente, é possível gerenciá-lo usando as configurações de um dispositivo gerenciado.

Para selecionar múltiplos tipos de evento, use as teclas **Shift** ou **Ctrl**; para selecionar todos os tipos, use o botão **Selecionar tudo**.

Configurações

Na seção **Configurações**, você pode configurar a política do Agente de Rede:

- **Distribuir os arquivos somente através dos pontos de distribuição**

  Se essa opção for ativada, os Agentes de Rede em dispositivos gerenciados recuperam atualizações apenas de pontos de distribuição.

  Se esta opção estiver desativada, os Agentes de Rede em dispositivos gerenciados recuperam atualizações de pontos de distribuição ou do Servidor de Administração.

  > Observe que os aplicativos de segurança em dispositivos gerenciados recuperam atualizações da fonte definida na tarefa de atualização para cada aplicativo de segurança. Se você ativar a opção **Distribuir os arquivos somente através dos pontos de distribuição**, certifique-se de que o Kaspersky Security Center está definido como uma fonte de atualização nas tarefas de atualização.

  Por padrão, esta opção está desativada.

- **Tamanho máximo da fila de eventos, em MB**

  Neste campo, você pode especificar o espaço máximo na unidade que uma fila de eventos pode ocupar.

  O valor predefinido é 2 megabytes (MB).

- **O aplicativo tem permissão para recuperar os dados estendidos da política no dispositivo**

  O Agente de Rede instalado em um dispositivo gerenciado transfere informações sobre a política do aplicativo de segurança aplicada ao aplicativo de segurança (por exemplo, Kaspersky Endpoint Security for Windows). Você pode visualizar as informações transferidas na interface do aplicativo de segurança.

  O Agente de Rede transfere as seguintes informações:

  - Hora da entrega da política para o dispositivo gerenciado.
  - Nome da política ativa no momento da entrega da política ao dispositivo gerenciado.
  - Nome da política de ausência temporária no momento da entrega da política ao dispositivo gerenciado (indisponível para o Agente de Rede para Linux).
  - Nome e caminho completo para o grupo de administração que continha o dispositivo gerenciado no momento da entrega da política para o dispositivo gerenciado.
  - Lista de perfis de política ativos com seus nomes e prioridades no momento da entrega da política ao dispositivo gerenciado.

  Você pode usar as informações para garantir que a política correta seja aplicada ao dispositivo e para fins de solução de problemas. Por padrão, esta opção está desativada.

- Proteger serviço do Agente de Rede contra remoção ou interrupção não autorizada e impedir alterações nas configurações

  Quando esta opção estiver ativado, após o Agente de Rede ter sido instalado em um dispositivo gerenciado, o componente não poderá ser removido ou reconfigurado sem os privilégios necessários. O serviço Agente de Rede não pode ser interrompido. Essa opção não tem efeito nos controladores de domínio.

  Ative esta opção para proteger o Agente de Rede em estações de trabalho operadas com direitos de administrador local.

  Por padrão, esta opção está desativada.

- Usar senha de desinstalação

  Caso esta opção esteja marcada, ao clicar no botão **Modificar**, será possível especificar a senha para o utilitário klmover e desinstalar remotamente o Agente de Rede.

  Por padrão, esta opção está desativada.

Repositórios

Na seção **Repositórios**, é possível selecionar os tipos de objetos cujos detalhes serão enviados do Agente de Rede para o Servidor de Administração:

- Detalhes das atualizações do Windows Update

  Se esta opção estiver marcada, as informações sobre as atualizações do Microsoft Windows Update que devem ser instaladas nos dispositivos clientes serão enviadas ao Servidor de Administração.

  Algumas vezes, mesmo se a opção estiver desativada, as atualizações são exibidas nas propriedades do dispositivo na seção **Atualizações disponíveis**. Pode acontecer se, por exemplo, os dispositivos da organização tiveram vulnerabilidades que poderiam ser corrigidas por estas atualizações.

  Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

  As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

- Detalhes das vulnerabilidades de software e das atualizações correspondentes

  Se essa opção estiver ativada, as informações sobre vulnerabilidades no software de terceiros (incluindo software da Microsoft), detectadas em dispositivos gerenciados e sobre atualizações de software para corrigir vulnerabilidades de terceiros (não incluindo o software da Microsoft) são enviadas ao Servidor de Administração.

  Selecionando esta opção (**Detalhes das vulnerabilidades de software e das atualizações correspondentes)** aumenta a carga da rede, a carga do disco do Servidor de Administração e o consumo de recurso pelo Agente de Rede.

  Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

  Para gerenciar atualizações de software da Microsoft, use a opção **Detalhes das atualizações do Windows Update**.

- **Detalhes do registro de hardware**

  O Agente de Rede instalado em um dispositivo envia informações sobre o hardware do dispositivo para o Servidor de Administração. Você pode exibir os detalhes do hardware nas propriedades do dispositivo.

  Verifique e confirme se o utilitário lshw está instalado nos dispositivos Linux a partir dos quais deseja buscar detalhes de hardware. Os detalhes de hardware obtidos de máquinas virtuais podem estar incompletos, dependendo do hipervisor usado.

- **Detalhes dos aplicativos instalados**

  Se esta opção estiver ativada, as informações sobre os aplicativos instalados nos dispositivos clientes serão enviadas ao Servidor de Administração.

  Por padrão, esta opção está ativada.

- **Incluir informações sobre patches**

  As informações sobre os patches para os aplicativos instalados nos dispositivos cliente são enviadas ao Servidor de Administração. A ativação desta opção pode aumentar a carga no Servidor de Administração e DBMS, assim como causar volume aumentado do banco de dados.

  Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

Se a modificação de algumas configurações nesta seção estiver bloqueada pela política do Agente de Rede, você não pode modificá-las.

Atualizações e vulnerabilidades de software

Na seção **Atualizações e vulnerabilidades de software**, é possível configurar a pesquisa e a distribuição de atualizações do Windows, assim como ativar a verificação de arquivos executáveis quanto a vulnerabilidades:

- **Usar Servidor de Administração como servidor WSUS**

  Se esta opção estiver ativada, as atualizações do Windows não serão baixadas no Servidor de Administração. O Servidor de Administração fornece atualizações baixadas para os serviços Windows Update em dispositivos cliente no modo centralizado através de Agentes de Rede.

  Se esta opção estiver ativada, o Servidor de Administração não é usado para baixar as atualizações do Windows. Neste caso, os dispositivos cliente recebem por si só as atualizações do Windows.

  Por padrão, esta opção está desativada.

- Em **Permitir aos usuários gerenciar a instalação de atualizações do Windows Update**, você pode limitar as atualizações do Windows que os usuários podem instalar em seus dispositivos manualmente usando o Windows Update.

  Em dispositivos que executam o Windows 10, se o Windows Update já tiver encontrado atualizações para o dispositivo, a nova opção selecionada em **Permitir aos usuários gerenciar a instalação de atualizações do Windows Update** será aplicada apenas depois que as atualizações encontradas forem instaladas.

  Selecione um item na lista suspensa:

  - **Permitir que os usuários instalem todas as atualizações do Windows Update**

    Os usuários podem instalar todas as atualizações do Microsoft Windows Update que são aplicáveis aos seus dispositivos.

    Selecione esta opção se você não quiser interferir na instalação das atualizações.

    Quando o usuário instala atualizações do Microsoft Windows Update manualmente, as atualizações podem ser baixadas de servidores da Microsoft e não do Servidor de Administração. Isso é possível se o Servidor de Administração ainda não tiver baixado as atualizações. Baixar atualizações dos servidores da Microsoft resulta em tráfego extra.

  - **Permitir que os usuários instalem apenas atualizações do Windows Update aprovadas**

    Os usuários podem instalar todas as atualizações do Microsoft Windows Update que são aplicáveis aos seus dispositivos e que você aprovou.

    Por exemplo, pode ser necessário verificar primeiro a instalação das atualizações em um ambiente de teste, assegurar-se de que elas não interferem na operação dos dispositivos e, só então, permitir a instalação dessas atualizações aprovadas nos dispositivos cliente.

    Quando o usuário instala atualizações do Microsoft Windows Update manualmente, as atualizações podem ser baixadas de servidores da Microsoft e não do Servidor de Administração. Isso é possível se o Servidor de Administração ainda não tiver baixado as atualizações. Baixar atualizações dos servidores da Microsoft resulta em tráfego extra.

- Não permitir que os usuários instalem atualizações do Windows Update

  Os usuários não podem instalar atualizações do Microsoft Windows Update em seus dispositivos manualmente. Todas das atualizações aplicáveis são instaladas conforme configuradas por você.

  Selecione esta opção se você deseja gerenciar a instalação das atualizações centralmente.

  Por exemplo, pode ser necessário otimizar o agendamento da atualização para que a rede não fique sobrecarregada. Você pode agendar atualizações fora do horário para que não interfiram na produtividade dos usuários.

- No grupo de configurações **Modo de pesquisa do Windows Update**, você pode selecionar um modo de pesquisa de atualizações:

  - Ativo

    Se essa opção estiver selecionada, o Servidor de Administração com suporte do Agente de Rede inicia uma solicitação ao Windows Update Agent no dispositivo cliente por uma fonte de atualização: Servidores do Windows Update ou WSUS. A seguir, o Agente de Rede passa as informações recebidas do Windows Update Agent para o Servidor de Administração.

    A opção entra em vigor somente se **Conectar com o servidor de atualizações para atualizar dados** A opção da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* está selecionada.

    Por padrão, esta opção está selecionada.

  - Passivo

    Se você selecionar esta opção, o Agente de Rede passa informações ao Servidor de Administração periodicamente sobre atualizações obtidas na última sincronização do Windows Update Agent com a fonte de atualização. Se não for efetuada uma sincronização do Windows Update Agent com uma fonte de atualização, as informações sobre as atualizações no Servidor de Administração se tornam desatualizadas.

    Selecione esta opção se desejar obter atualizações do cache de memória da fonte de atualização.

  - Desativado

    Se esta opção for selecionada, o Servidor de Administração não solicita qualquer informação sobre atualizações.

    Selecione esta opção se, por exemplo, quiser testar as atualizações no seu dispositivo local primeiro.

- Verificar a vulnerabilidade dos arquivos executáveis ao executá-los

  Se essa caixa de seleção estiver selecionada, as vulnerabilidades serão verificadas quando os arquivos executáveis forem executados.

  Por padrão, esta opção está ativada.

Gerenciamento de reinício

Na seção **Gerenciamento de reinício**, é possível especificar a ação a ser executada se o sistema operacional de um dispositivo gerenciado precisar ser reiniciado para uso correto, instalação ou desinstalação de um aplicativo:

- **Não reiniciar o sistema operacional**

  O sistema operacional não será reiniciado.

- **Reiniciar o sistema operacional automaticamente se necessário**

  Se necessário, o sistema operacional é reiniciado automaticamente.

- **Perguntar ao usuário o que fazer**

  O aplicativo solicita ao usuário que permita o reinício do sistema operacional.

  Por padrão, esta opção está selecionada.

  - **Repetir o aviso a cada (min.)**

    Se esta opção estiver ativada, o aplicativo solicita ao usuário que permita o reinício do sistema operacional com a frequência especificada no campo ao lado da caixa de seleção. Por padrão, a frequência da solicitação é de 5 minutos.

    Se esta opção estiver ativada, o aplicativo não solicita ao usuário permissão para o reinício repetidamente.

    Por padrão, esta opção está ativada.

  - **Forçar reinício após (min.)**

    Se esta opção estiver ativada, após solicitar ao usuário, o aplicativo força o reinício do sistema operacional após a expiração do intervalo especificado no campo ao lado da caixa de seleção.

    Se esta opção estiver ativada, o aplicativo não força o reinício.

    Por padrão, esta opção está ativada.

  - **Tempo de espera antes do fechamento forçado de aplicativos nas sessões bloqueadas (min)**

    Os aplicativos são fechados no modo forçado quando o dispositivo for bloqueado (automaticamente, após um intervalo especificado de inatividade ou manualmente).

    Se esta opção estiver ativada, os aplicativos serão forçados a fechar no dispositivo bloqueado após a expiração do intervalo de tempo especificado no campo de entrada.

    Se essa opção estiver ativada, os aplicativos não serão fechados no dispositivo bloqueado.

    Por padrão, esta opção está desativada.

Compartilhamento da Área de Trabalho do Windows

Na seção **Windows Desktop Sharing**, será possível ativar e configurar a auditoria das ações do administrador executadas em um dispositivo remoto quando o acesso à área de trabalho for compartilhado:

- **Ativar auditoria**

  Se a opção estiver marcada, a auditoria das ações do administrador no dispositivo remoto será ativada. Os registros de ações do administrador no dispositivo remoto são registrados:

  - No log de eventos no dispositivo remoto
  - Em um arquivo com a extensão syslog localizado na pasta de instalação do Agente de Rede no dispositivo remoto
  - No banco de dados de eventos do Kaspersky Security Center

  A auditoria das ações do administrador está disponível quando as seguintes condições são observadas:

  - A licença de Gerenciamento de patches e vulnerabilidades está em uso
  - O administrador tem o direito de iniciar o acesso compartilhado à área de trabalho do dispositivo remoto

  Se esta opção estiver desmarcada, a auditoria das ações do administrador no dispositivo remoto será desativada.

  Por padrão, esta opção está desativada.

- **Máscaras de arquivos para monitorar quando lidos**

  A lista contém máscaras de arquivos. Quando a auditoria é ativada, o aplicativo monitora a leitura do administrador de arquivos que correspondem às máscaras e salva informações sobre os arquivos lidos. A lista está disponível se a caixa de seleção **Ativar auditoria** for marcada. Você pode editar máscaras de arquivos e adicionar novas máscaras à lista. Cada nova máscara de arquivo deve ser especificada na lista em uma nova linha.

  Por padrão, são especificadas as seguintes máscaras de arquivos: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Máscaras de arquivos para monitorar quando modificados**

  A lista contém máscaras de arquivos no dispositivo remoto. Quando a auditoria é ativada, o aplicativo monitora alterações efetuadas pelo administrador em arquivos que correspondem a máscaras e salva informações sobre essas modificações. A lista está disponível se a caixa de seleção **Ativar auditoria** for marcada. Você pode editar máscaras de arquivos e adicionar novas máscaras à lista. Cada nova máscara de arquivo deve ser especificada na lista em uma nova linha.

  Por padrão, são especificadas as seguintes máscaras de arquivos: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Gerenciar patches e atualizações

Na seção **Gerenciar patches e atualizações**, você poderá configurar o download e a distribuição das atualizações, assim como a instalação dos patches nos dispositivos gerenciados:

- **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**

  Se esta opção estiver ativada, os patches da Kaspersky com o status de aprovação *Indefinido* são automaticamente instaladas nos dispositivos gerenciados imediatamente após terem sido baixadas dos servidores de atualização.

  Se esta opção estiver desativada, as correções da Kaspersky que foram baixadas e identificadas com o status *Indefinido* somente serão instaladas após você alterar o status para *Aprovado*.

  Por padrão, esta opção está ativada.

- **Fazer antecipadamente o download das atualizações e dos bancos de dados de antivírus via Servidor de Administração (recomendado)**

  Se esta opção está ativada, o modelo offline do download da atualização é usado. Quando o Servidor de Administração recebe atualizações, ele notifica o Agente de Rede (nos dispositivos em que ele esteja instalado) sobre as atualizações que serão necessárias para os aplicativos gerenciados. Quando o Agentes de Rede recebe informações sobre essas atualizações, ele baixa dos arquivos relevantes do Servidor de Administração com antecedência. Na primeira conexão com o Agente de Rede, o Servidor de Administração inicia um download de atualizações. Após o Agente de Rede ter baixado todas as atualizações em um dispositivo cliente, as atualizações se tornam disponíveis para os aplicativos naquele dispositivo.

  Quando um aplicativo gerenciado em um dispositivo cliente tentar acessar o Agente de Rede quanto a atualizações, o Agente de Rede verifica se ele tem todas as atualizações necessárias. Se as atualizações forem recebidas do Servidor de Administração até 25 horas antes de terem sido solicitadas pelo aplicativo gerenciado, o Agente de Rede não se conectará ao Servidor de Administração, mas fornecerá ao aplicativo gerenciado as atualizações do cache local. A conexão com o Servidor de Administração pode não ser estabelecida quando o Agente de Rede fornecer atualizações aos aplicativos em dispositivos cliente, mas a conexão não é necessária para a atualização.

  Se esta opção está desativada, o modelo offline do download da atualização é usado. As atualizações são distribuídas de acordo com o agendamento da tarefa de download da atualização.

  Por padrão, esta opção está ativada.

Conectividade

A seção **Conectividade** inclui três subseções aninhadas:

- **Rede**
- **Perfis de conexão** (apenas para Windows e macOS)
- **Agendador de conexão**

Na subseção **Rede**, você pode configurar a conexão ao Servidor de Administração, ativar o uso de uma porta UDP e especificar o seu número. As seguintes opções estão disponíveis:

- No grupo de configurações **Conexão ao Servidor de Administração**, você poderá configurar a conexão ao Servidor de Administração e especificar o intervalo de tempo para a sincronização entre os dispositivos cliente e o Servidor de Administração:

  - Compactar o tráfego de rede

    Se esta opção estiver ativada, a velocidade de transferência de dados pelo Agente de Rede é aumentada através da redução da quantidade de informação a ser transferida e consequente carga inferior sobre o Servidor de Administração.

    A carga na CPU do computador cliente pode aumentar.

    Por padrão, esta caixa de seleção é marcada.

  - Abrir portas do Agente de Rede no Firewall do Microsoft Windows

    Se esta opção estiver ativada, as portas, necessárias para o funcionamento do Agente de Rede, serão adicionadas à lista de exclusões do Firewall do Microsoft Windows.

    Por padrão, esta opção está ativada.

  - Usar SSL

    Se esta opção estiver ativada, a conexão com o Servidor de Administração é estabelecida através de uma porta segura via SSL.

    Por padrão, esta opção está ativada.

  - Use o gateway de conexão no ponto de distribuição (se disponível) sob as configurações de conexão padrão

    Se esta opção estiver marcada, o gateway de conexão no ponto de distribuição é usado sob as configurações especificadas nas propriedades do grupo de administração.

    Por padrão, esta opção está ativada.

- Usar porta UDP

  Caso deseje que o Agente de Rede seja conectado com o Servidor de Administração por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de **Porta UDP**. Por padrão, esta opção está ativada. A porta UDP padrão para estabelecer conexão com o Servidor de Administração é 15000.

- **Número da porta UDP**

  Neste campo, é possível inserir o número da porta UDP. O número da porta padrão é 15000.

  É usado o sistema decimal para registros.

  Se um dispositivo cliente estiver executando o Windows XP Service Pack 2, o firewall integrado bloqueará a porta UDP 15000. Essa porta deve ser aberta manualmente.

- **Use o ponto de distribuição para forçar a conexão ao Servidor de Administração**

  Selecione esta opção se você selecionou a opção **Usar este ponto de distribuição como um servidor push** na janela de configurações do ponto de distribuição. Do contrário, o ponto de distribuição não atuará como um servidor push.

Na subseção **Perfis de conexão**, você pode especificar as configurações da localização da rede, configurar perfis de conexão par o Servidor de Administração e ativar o modo ausente quando o Servidor de Administração não estiver disponível.

- **Configurações do local de rede**

  As configurações da localização da rede definem as características da rede à qual o dispositivo cliente está conectado e especifica as regras para o Agente de Rede alternando de um perfil de conexão do Servidor de Administração a outro quando aquelas características da rede forem alteradas.

- **Perfis de conexão do Servidor de Administração**

  Nesta seção, é possível visualizar e adicionar perfis para a conexão do Agente de Rede com o Servidor de Administração. Nesta seção, você também pode criar regras para alternar o Agente de Rede para diferentes Servidores de Administração quando os seguintes eventos ocorrem:

  - Quando o dispositivo cliente se conectar a outra rede local
  - Quando um dispositivo perde a conexão com a rede local da organização
  - Quando o endereço do gateway de conexão for alterado ou o endereço do servidor DNS for modificado

  Os perfis de conexão têm suporte somente para dispositivos que executam Windows e macOS.

- **Ativar modo ausente quando o Servidor de Administração não estiver disponível**

  Se esta opção estiver marcada, no caso da conexão com este perfil, os aplicativos instalados no dispositivo cliente irão usar as políticas de ausência de escritório, assim como as políticas de ausência de escritório. Se a política de ausência não estiver definida para o aplicativo, a política ativa será usada.

  Se esta opção estiver desativada, os aplicativos usarão as políticas ativas.

  Por padrão, esta opção está desativada.

Na subseção **Agendador de conexão**, você pode especificar os intervalos de tempo durante os quais o Agente de Rede envia dados para o Servidor de Administração:

- Conectar quando necessário

  Se esta opção estiver selecionada, a conexão é estabelecida quando o Agente de Rede tem de enviar dados para o Servidor de Administração.

  Por padrão, esta opção está selecionada.

- Conectar-se nos intervalos de tempo especificados

  Se esta opção estiver selecionada, o Agente de Rede se conecta ao Servidor de Administração numa hora específica. Você pode adicionar vários períodos de tempo de conexão.

Pontos de distribuição

A seção **Pontos de distribuição** inclui quatro subsecções aninhadas:

- **Sondagem da rede**
- **Configurações de conexão com a Internet**
- **Proxy da KSN**
- **Atualizações**

Na seção **Sondagem da rede**, você pode configurar a sondagem automática da rede. Você pode ativar três tipos de sondagem, ou seja, sondagem de rede, de intervalo de IP e do Active Directory:

- **Ativar sondagem da rede**

  Se a esta opção estiver ativada, o Servidor de Administração automaticamente efetua a sondagem da rede de acordo com o agendamento configurado ao clicar nos links **Definir agendamento da sondagem rápida** e **Definir agendamento da sondagem completa**.

  Caso essa opção esteja desativada, o Servidor de Administração sonda a rede com o intervalo especificado no campo **Frequência de sondagens da rede (min.)**.

  O intervalo de descoberta de dispositivos para versões do Agente de Rede anteriores a 10.2 pode ser configurado nos campos **Frequência de sondagens de domínios Windows (min.)** (para a sondagem rápida de rede do Windows) e **Frequência de sondagens da rede (min.)** (para a sondagem completa de rede do Windows).

  Por padrão, esta opção está desativada.

- **Ativar a sondagem de intervalos IP**

  Caso a opção esteja ativada, o ponto de distribuição automaticamente realiza a sondagem dos intervalos de IP de acordo com o agendamento configurado ao clicar no link **Definir agendamento da sondagem**.

  Se essa opção estiver desmarcada, o ponto de distribuição não faz a sondagem dos intervalos de IP.

  A frequência de sondagem de conjuntos de IPs para versões do Agente de Rede anteriores a 10.2 pode ser configurada no campo **Intervalo de sondagem (min.)**. O campo está disponível se a opção estiver ativada.

  Por padrão, esta opção está desativada.

- **Usar sondagem Zeroconf (em plataformas Linux apenas. Intervalos IP especificados manualmente serão ignorados)**

  Se esta opção for ativada, o ponto de distribuição sondará automaticamente a rede com dispositivos IPv6 usando a rede zero configuração (também referida como *Zeroconf*). Nesse caso, a sondagem de intervalo de IP ativada é ignorada, porque o ponto de distribuição sonda toda a rede.

  Para começar a usar o Zeroconf, as seguintes condições devem ser atendidas:

  - O ponto de distribuição deve executar Linux.
  - Você deve instalar o utilitário avahi-browse no ponto de distribuição.

  Se essa opção estiver desativada, o ponto de distribuição não faz a sondagem com dispositivos IPv6y.

  Por padrão, esta opção está desativada.

- **Ativar sondagem do Active Directory**

  Se a opção estiver habilitada, o ponto de distribuição sondará automaticamente o Active Directory de acordo com o agendamento que você configurou clicando no link **Definir agendamento da sondagem**.

  Se esta opção estiver desativada, o Servidor de Administração não faz a sondagem do Active Directory.

  A frequência de sondagem do Active Directory para versões do Agente de Rede anteriores a 10.2 pode ser configurada no campo **Intervalo de sondagem (min.)**. O campo está disponível caso a opção esteja ativada.

  Por padrão, esta opção está desativada.

Caso seus pontos de distribuição usem o servidor proxy para se conectar à internet, na subseção **Configurações de conexão com a internet**, você poderá especificar as seguintes configurações:

- Usar o servidor proxy

  Se esta caixa de seleção estiver selecionada, você pode configurar nos campos de entrada a conexão ao servidor proxy.

  Por padrão, esta caixa de seleção está desmarcada.

- Endereço do servidor proxy

  Endereço do servidor proxy.

- Número da porta

  O número da porta que é usada para conexão.

- Ignorar servidor proxy para endereços locais

  Se esta opção estiver ativada, nenhum servidor proxy será usado para se conectar aos dispositivos na rede local.

  Por padrão, esta opção está desativada.

- Autenticação do servidor proxy

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

  Por padrão, esta caixa de seleção está desmarcada.

- Nome do usuário

  Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida.

- Senha

  Senha da conta sob a qual a tarefa será executada.

Na seção **Proxy da KSN**, você pode configurar o aplicativo para usar o ponto de distribuição para encaminhar solicitações à KSN a partir dos dispositivos gerenciados:

- **Ativar Proxy da KSN no lado do ponto de distribuição**

  O serviço Proxy da KSN é executado no dispositivo que é usado como um ponto de distribuição. Use este recurso para redistribuir e otimizar o tráfego na rede.

  O ponto de distribuição envia as estatísticas da KSN, que são listadas na Declaração da Kaspersky Security Network, à Kaspersky. Por padrão, a Declaração da KSN está localizada em %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Por padrão, esta opção está desativada. A ativação desta opção somente terá efeito se as opções **Usar Servidor de Administração como um servidor proxy** e **Concordo em usar a Kaspersky Security Network** estiverem ativadas na janela de propriedades do Servidor de Administração.

  É possível atribuir um nó de um cluster ativo-passivo a um ponto de distribuição e habilitar o servidor proxy da KSN nesse nó.

- **Encaminhar solicitações da KSN para o Servidor de Administração**

  O ponto de distribuição encaminha solicitações do KSN dos dispositivos gerenciados para o Servidor de Administração.

  Por padrão, esta opção está ativada.

- **Acessar a KSN Cloud/KSN Privada diretamente pela internet**

  O ponto de distribuição encaminha solicitações à KSN dos dispositivos gerenciados para a KSN Cloud ou KSN Privada. As solicitações KSN geradas no próprio ponto de distribuição também são enviadas diretamente à KSN Cloud ou à KSN Privada.

  Os pontos de distribuição com o Agente de Rede versão 11 (ou anterior) instalado não podem acessar diretamente a KSN Privada. Se você deseja reconfigurar os pontos de distribuição para enviar solicitações à KSN à KSN Privada, ative a opção **Encaminhar solicitações da KSN para o Servidor de Administração** para cada ponto de distribuição.

  Os pontos de distribuição com o Agente de Rede versão 12 (ou posterior) instalado podem acessar diretamente a KSN Privada.

- **Porta TCP**

  O número da porta TCP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. O número da porta padrão é 13111.

- **Usar porta UDP**

  Caso deseje que o Agente de Rede seja conectado com o Servidor de Administração por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de **Porta UDP**. Por padrão, esta opção está ativada. A porta UDP padrão para estabelecer conexão com o Servidor de Administração é 15000.

Na subseção **Atualizações**, você pode especificar se o Agente de Rede deve baixar arquivos diff ativando ou desativando a opção **Baixar arquivos diff**. (Essa opção vem ativada por padrão.)

Histórico de revisões

Na guia **Histórico de revisões**, você poderá ver o histórico de revisões da política do Agente de Rede. Você pode comparar revisões, exibir revisões e realizar operações avançadas, como salvar revisões em um arquivo, reverter uma revisão, e adicionar e editar descrições da revisão.

Como gerenciar contas de usuário

Essa seção fornece informações sobre contas de usuário e funções suportadas pelo aplicativo. Essa seção contém instruções sobre como criar contas e funções para usuários do Kaspersky Security Center.

O Kaspersky Security Center lhe permite gerenciar contas de usuário e grupos de contas. O aplicativo é compatível com três tipos de contas:

- Contas dos funcionários da organização. O Servidor de Administração obtém dados das contas desses usuários de domínio ao fazer a sondagem da rede da organização.
- Contas de usuários locais. Contas locais em dispositivos gerenciados, bem como as contas locais no dispositivo no qual o Servidor de Administração está instalado.
- Contas de usuários internos do Kaspersky Security Center. É possível criar contas de usuários internos. As contas serão utilizadas apenas no Kaspersky Security Center.

Trabalhando com contas de usuário

O Kaspersky Security Center lhe permite gerenciar contas de usuário e grupos de contas. O aplicativo é compatível com dois tipos de contas:

- Contas dos funcionários da organização. O Servidor de Administração obtém dados das contas desses usuários ao amostrar a rede da organização.
- Contas de usuários internos. Estas contas são aplicadas quando os Servidores de Administração virtuais são usados. As contas de usuários internos são criadas e usadas somente dentro do Kaspersky Security Center.

É possível visualizar a lista de contas de usuário de uma das seguintes formas:

- Na árvore do console, vá para **Avançado** → **Contas de usuário**.
- Na árvore do console, vá para guia **Dispositivos gerenciados** → **Dispositivos** → link <nome do dispositivo> → seção **Sessões**.

  A seção **Sessões** exibe contas de usuários com sessões ativas em dispositivos que executam Windows.

A lista de contas de usuário será exibida corretamente se os seguintes requisitos forem atendidos:

- Use o Agente de Rede da mesma versão ou uma posterior à do Servidor de Administração.
- A sondagem do Active Directory está ativada para exibir as contas dos usuários do domínio.
- Em dispositivos gerenciados que executam o Windows, o serviço **Server (LanmanServer)** está em execução.

Você pode realizar as seguintes ações em contas do usuário e grupos de contas:

- Configure os direitos de acesso dos usuários aos recursos do aplicativo usando funções.
- Envie mensagens aos usuários usando e-mail e SMS.
- Visualizar a lista de dispositivos móveis do usuário.
- Emitir e instalar certificados nos dispositivos móveis do usuário.
- Visualizar a lista de certificados emitidos para o usuário.
- Desativar a verificação em duas etapas para uma conta de usuário.

Adicionar uma conta de usuário interno

Para adicionar uma nova conta de usuário interno ao Kaspersky Security Center:

1. Na árvore do console, abra a pasta **Contas de usuário**.

   A pasta **Contas de usuário** é uma subpasta da pasta **Avançado** por padrão.

2. No espaço de trabalho, clique no botão **Adicionar um usuário**.

3. Na janela **Novo usuário** que se abre, especifique as configurações da conta do novo usuário:

- Um nome de usuário ()

  > Tenha cuidado digitar o nome do usuário. Você não conseguirá modificá-lo após salvar as alterações.

- **Descrição**
- **Nome completo**
- **E-mail principal**
- **Telefone principal**
- **Senha** para a conexão do usuário ao Kaspersky Security Center

  A senha deve estar em conformidade com as seguintes regras:

  - A senha deve ter de 8 a 16 caracteres.
  - A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
    - Letras maiúsculas (A-Z)
    - Letras minúsculas (a-z)
    - Números (0-9)
    - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - A senha não deve conter nenhum espaço em branco, caracteres Unicode ou a combinação dos caracteres "." e "@", quando "." estiver colocado antes de "@".

  Para ver a senha inserida, mantenha pressionado o botão **Exibir**.

  > O número de tentativas de entrada da senha é limitado. Por padrão, o número máximo de tentativas permitidas de entrada da senha é de 10. Você pode modificar o número permitido de tentativas de inserção de senha, como descrito em "Alterar o número permitido de tentativas de entrada de senha".

  > Se o usuário inserir uma senha inválida no número especificado de vezes, a conta do usuário é bloqueada por um hora. Na lista de contas de usuário, o ícone de usuário () de uma conta bloqueada fica esmaecido (indisponível). Você pode desbloquear a conta do usuário somente ao alterar a senha.

- Se necessário, marque a caixa de seleção **Desativar conta** para proibir o usuário de conectar-se ao aplicativo. Você pode desativar uma conta, por exemplo, se desejar criá-la antes, mas ativá-la depois.
- Marque a caixa de seleção **Solicitar a senha quando as configurações de conta forem modificadas** se desejar ativar uma opção adicional para proteger uma conta de usuário de modificações não autorizadas. Se esta opção for ativada, a modificação das configurações da conta do usuário requer a autorização do usuário com direito a Modificar ACLs do objeto **da área funcional Recursos gerais: Permissões do usuário**.

4. Clique em **OK**.

A conta de usuário recém-criada é exibida no espaço de trabalho da pasta **Contas de usuário**.

Editar uma conta de usuário interno

Para editar uma nova conta de usuário interno ao Kaspersky Security Center:

1. Na árvore do console, abra a pasta **Contas de usuário**.

   Por padrão, a pasta **Contas de usuário** é uma subpasta da pasta **Avançado**.

2. No espaço de trabalho, clique duas vezes na conta de usuário interno que você deseja editar.

3. Na janela **Propriedades: <nome de usuário>** que se abre, altere as configurações da conta de usuário:

- **Descrição**
- **Nome completo**
- **E-mail principal**
- **Telefone principal**
- **Senha** para a conexão do usuário ao Kaspersky Security Center

  A senha deve estar em conformidade com as seguintes regras:

  - A senha deve ter de 8 a 16 caracteres.
  - A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
    - Letras maiúsculas (A-Z)
    - Letras minúsculas (a-z)
    - Números (0-9)
    - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - A senha não deve conter nenhum espaço em branco, caracteres Unicode ou a combinação dos caracteres "." e "@", quando "." estiver colocado antes de "@".

  Para ver a senha inserida, mantenha pressionado o botão **Exibir**.

  > O número de tentativas de entrada da senha é limitado. Por padrão, o número máximo de tentativas permitidas de entrada da senha é de 10. Você pode modificar o número permitido de tentativas de inserção de senha, como descrito em "Alterar o número permitido de tentativas de entrada de senha".

  > Se o usuário inserir uma senha inválida no número especificado de vezes, a conta do usuário é bloqueada por um hora. Na lista de contas de usuário, o ícone de usuário () de uma conta bloqueada fica esmaecido (indisponível). Você pode desbloquear a conta do usuário somente ao alterar a senha.

- Se necessário, marque a caixa de seleção **Desativar conta** para proibir o usuário de conectar-se ao aplicativo. Você pode desativar uma conta, por exemplo, depois que um funcionário sai da empresa.
- Selecione a opção **Solicitar a senha quando as configurações de conta forem modificadas** se você deseja ativar uma opção adicional para proteger uma conta de usuário de modificações não autorizadas. Se esta opção for ativada, a modificação das configurações da conta do usuário requer a autorização do usuário com direito a Modificar ACLs do objeto **da área funcional Recursos gerais: Permissões do usuário**.

4. Clique em **OK**.

Como resultado, a conta de usuário editada é exibida no espaço de trabalho da pasta **Contas de usuário**.

Alterar o número permitido de tentativas de entrada de senha

O usuário do Kaspersky Security Center pode inserir uma senha inválida um número limitado de vezes. Depois que o limite é atingido, a conta de usuário é bloqueada por uma hora.

Por padrão, o número máximo permitido de tentativas de entrada da senha é 10. Você pode alterar o número permitido de tentativas de entrada de senha, como descrito nesta seção.

Para alterar o número permitido de tentativas de entrada de senha:

1. Abra o registro do sistema do dispositivo cliente no qual o Servidor de Administração está instalado (por exemplo, usando o comando regedit no menu **Iniciar** → **Executar**).
2. Vá ao seguinte chave:
   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF
3. Crie o valor SrvSplPpcLogonAttempts, caso não esteja presente. O tipo de valor é DWORD.

   Por padrão, depois que o Kaspersky Security Center é instalado, esse valor não é criado.
4. Especifique o número necessário de tentativas no valor SrvSplPpcLogonAttempts.
5. Clique em **OK** para salvar as alterações.
6. Reinicie o serviço do Servidor de Administração.

O número máximo de tentativas permitidas de entrada da senha é alterado.

Configurar a verificação do nome de um usuário interno quanto a singularidade

Você pode configurar a verificação do nome de um usuário interno do Kaspersky Security Center quanto a exclusividade quando este nome for adicionado ao aplicativo. Para verificar o nome de um usuário interno quanto a exclusividade, somente pode ser executado em um Servidor de Administração virtual ou no Servidor de Administração principal, para o qual a contado usuário deve ser criada, em todos os Servidores de Administração virtuais e no Servidor de Administração principal. Por padrão, o nome de um usuário interno é verificado quanto à exclusividade em todos os Servidores de Administração virtuais e no Servidor de Administração principal.

Para ativar a verificação do nome de um usuário interno quanto à exclusividade em um Servidor de Administração virtual ou no Servidor de Administração principal:

1. Abra o registro do sistema do dispositivo cliente no qual o Servidor de Administração está instalado (por exemplo, usando o comando regedit no menu **Iniciar** → **Executar**).
2. Vá ao seguinte hive:
   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Para a chave LP_InterUserUniqVsScope (DWORD), defina o valor 00000001.

   O valor padrão especificado para esta chave é 0.
4. Reinicie o serviço do Servidor de Administração.

O nome somente será verificado quanto à exclusividade no Servidor de Administração virtual no qual o usuário interno foi criado, ou no Servidor de Administração principal se o usuário interno foi criado no Servidor de Administração principal.

Para ativar a verificação do nome de um usuário interno em todos os Servidores de Administração virtuais e no Servidor de Administração principal:

1. Abra o registro do sistema do dispositivo cliente no qual o Servidor de Administração está instalado (por exemplo, usando o comando regedit no menu **Iniciar** → **Executar**).
2. Vá ao seguinte hive:
   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
3. Para a chave LP_InterUserUniqVsScope (DWORD), defina o valor 00000000.

   O valor padrão especificado para esta chave é 0.
4. Reinicie o serviço do Servidor de Administração.

A verificação quanto à exclusividade do nome será executada em todos os Servidores de Administração virtuais e no Servidor de Administração principal.

Adicionar um grupo de segurança

Você pode adicionar grupos de segurança (grupos de usuários), executar a configuração flexível do acesso para grupos e grupos de segurança aos diversos recursos do aplicativo. Os grupos de segurança podem ter nomes atribuídos que correspondem a suas finalidades respectivas. Por exemplo, o nome pode corresponder a onde os usuários estão localizados no escritório ou ao nome da unidade organizacional da empresa a qual os usuários pertencem.

Um usuário pode pertencer a diversos grupos de segurança. Uma conta de usuário gerenciada por um Servidor de Administração virtual somente pode pertencer aos grupos de segurança deste servidor virtual e ter direitos de acesso somente neste servidor virtual.

Para adicionar um grupo de segurança:

1. Na árvore do console, selecione a pasta **Contas de usuário**.

   Por padrão, a pasta **Contas de usuário** é uma subpasta da pasta **Avançado**.

2. Clique no botão **Adicionar grupo de segurança**.

   A janela **Adicionar grupo de segurança** se abre.

3. Na janela **Adicionar grupo de segurança**, na seção **Geral**, especifique o nome do grupo.

   O nome do grupo não pode conter mais de 255 caracteres e conter determinados símbolos especiais, tais como *, <, >, ?, \, :, |. O nome do grupo precisa ser exclusivo.

   É possível inserir a descrição do grupo no campo de entrada **Descrição**. Preencher o campo **Descrição** é opcional.

4. Clique em **OK**.

O grupo de segurança que você adicionou aparece na pasta **Contas de usuário** na árvore do console. Você pode adicionar usuários ao grupo recentemente criado.

Adicionando um usuário a um grupo

Para adicionar um usuário em um grupo:

1. Na árvore do console, selecione a pasta **Contas de usuário**.

   A pasta **Contas de usuário** é uma subpasta da pasta **Avançado** por padrão.

2. Na lista de contas de usuário e grupos, selecione o grupo no qual você deseja adicionar o usuário.

3. Na janela de propriedades do grupo, selecione a seção **Grupo de usuários** e clique no botão **Adicionar**.

   Uma janela com uma lista de usuários é aberta.

4. Na lista, selecione um usuário que você deseja incluir no grupo.

5. Clique em **OK**.

O usuário é adicionado ao grupo e exibido na lista de usuários do grupo.

Configurar direitos de acesso aos recursos do aplicativo. Controle de acesso baseado em função

O Kaspersky Security Center fornece meios de acesso baseado em função para os recursos do Kaspersky Security Center e aplicativos gerenciados da Kaspersky.

Você pode configurar os direitos de acesso aos recursos do aplicativo para usuários do Kaspersky Security Center de uma das seguintes maneiras:

- Configurando os direitos para cada usuário ou grupo de usuários individualmente.
- Criando funções de usuário padrão com um conjunto predefinido de direitos e atribuindo tais funções aos usuários dependendo do escopo de obrigações deles.

Função de usuário (também conhecida como função) é um conjunto predefinido de direitos de acesso aos recursos do Kaspersky Security Center ou aplicativos gerenciados da Kaspersky. Uma função pode ser atribuída a um usuário ou a um grupo de usuários.

A aplicação de funções de usuário tem como objetivo simplificar e reduzir os procedimentos de rotina de configuração de direitos de acesso dos usuários aos recursos do aplicativo. Os direitos de acesso com em uma função são configurados de acordo com as tarefas "padrão" e o escopo de deveres do usuário.

As funções de usuários podem ter nomes que correspondem a suas finalidades respetivas. Você pode criar um número ilimitado de funções no aplicativo.

É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado ou criar novas funções e configurar os direitos necessários por conta própria.

Direitos de acesso ao Servidor de Administração e seus objetos

Os grupos **KLAdmins** e **KLOperators** são criados automaticamente durante a instalação do Kaspersky Security Center. Para estes grupos são concedidos os direitos de se conectar-se ao Servidor de Administração e processar os objetos do Servidor de Administração.

Dependendo de qual tipo de conta for usado para a instalação do Kaspersky Security Center, os grupos **KLAdmins** e **KLOperators** são criados como segue:

- Se o aplicativo for instalado com uma conta de usuário incluída em um domínio, os grupos são criados no Servidor de Administração e no domínio que inclui o Servidor de Administração.
- Se o aplicativo for instalado sob uma conta de sistema, os grupos são criados somente em um Servidor de Administração.

Você pode visualizar os grupos **KLAdmins** e **KLOperators** e modificar os privilégios de acesso dos usuários que pertençam aos grupos **KLAdmins** e **KLOperators**, usando as ferramentas administrativas padrão do sistema operacional.

Ao grupo **KLAdmins** são concedidos todos os direitos de acesso e ao grupo **KLOperators** são concedidos somente os direitos de Leitura e Execução. Os direitos concedidos ao grupo **KLAdmins** são bloqueados.

Os usuários que pertençam ao grupo **KLAdmins** são chamados de *Administradores do Kaspersky Security Center*, os usuários do grupo **KLOperators** são chamados de *Operadores do Kaspersky Security Center*.

Além dos usuários incluídos no grupo **KLAdmins**, os direitos de administrador do Kaspersky Security Center são fornecidos aos administradores locais de dispositivos nos quais o Servidor de Administração é instalado.

Você pode excluir administradores locais da lista de usuários que possuam direitos de administrador do Kaspersky Security Center.

Todas as operações iniciadas pelos administradores do Kaspersky Security Center serão realizadas usando os direitos da conta do Servidor de Administração.

Um grupo individual **KLAdmins** pode ser criado para cada Servidor de Administração na rede; o grupo terá os direitos de acesso necessários somente para esse Servidor de Administração.

Se os dispositivos pertencentes ao mesmo domínio forem incluídos nos grupos de administração de diferentes Servidores de Administração, o administrador do domínio é o administrador do Kaspersky Security Center para todos os grupos. O grupo **KLAdmins** é o mesmo para esses grupos de administração; é criado durante a instalação do primeiro Servidor de Administração. Todas as operações iniciadas pelo administrador do Kaspersky Security Center são realizadas usando os direitos de conta do Servidor de Administração para o qual estas operações foram iniciadas.

Após a instalação do aplicativo, um administrador do Kaspersky Security Center pode fazer o seguinte:

- Modificar os direitos concedidos aos grupos **KLOperators**.
- Conceder direitos de acesso à funcionalidade do Kaspersky Security Center a outros grupos de segurança e a usuários individuais registrados na estação de trabalho do administrador.
- Atribuir direitos de acesso do usuário em cada grupo de administração.

O administrador do Kaspersky Security Center pode atribuir direitos de acesso a cada grupo de administração ou a outros objetos do Servidor de Administração na seção **Segurança**, na janela de propriedades do objeto selecionado.

Você pode acompanhar a atividade do usuário usando os registros de eventos na operação do Servidor de Administração. Os registros de evento são exibidos no nó do **Servidor de Administração** na guia **Eventos**. Esses eventos possuem o nível de importância **Eventos de informações** e os tipos de evento começam com "**Auditoria**".

Direitos de acesso aos recursos do aplicativo

A tabela abaixo mostra os recursos do Kaspersky Security Center com os direitos de acesso para gerenciar as tarefas, relatórios e configurações associadas, bem como executar as ações do usuário associadas.

Para executar as ações do usuário listadas na tabela, o usuário deve ter o direito especificado ao lado da ação.

Os direitos de **Ler**, **Gravar** e **Executar** são aplicáveis a qualquer tarefa, relatório ou configuração. Além desses direitos, o usuário precisa ter o direito de **Executar as operações nas seleções de dispositivos** para gerenciar tarefas, relatórios ou configurações nas seleções de dispositivos.

> Todas as tarefas, relatórios, configurações e pacotes de instalação que não constam na tabela pertencem à área funcional **Funcionalidades gerais: Funcionalidade básica**.

Direitos de acesso aos recursos do aplicativo

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: Gerenciamento de grupos de administração	**Gravar**	• Adicionar o dispositivo a um grupo de administração: **Gravar** • Excluir o dispositivo de um grupo de administração: **Gravar** • Adicionar um grupo de administração a outro grupo de administração: **Gravar** • Excluir um grupo de administração de outro grupo de administração: **Gravar**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: Acessar objetos independentemente de suas ACLs	**Ler**	Obter acesso de Ler a todos os objetos: **Ler**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: Funcionalidade básica	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Regras de movimentação de dispositivos (criar, modificar ou excluir) para o servidor virtual: **Gravar**, **Executar as operações nas seleções de dispositivos** • Obter um certificado personalizado para o Protocolo móvel (LWNGT): **Ler** • Configurar o certificado personalizado para o Protocolo móvel (LWNGT): **Gravar** • Obter a lista de redes definidas pela NLA: **Ler** • Adicionar, modificar ou excluir a lista de redes definidas por NLA: **Gravar** • Exibir a Lista de controle de acesso dos grupos: **Ler** • Visualizar o Log de eventos da Kaspersky: **Ler** • Visualizar a chave de recuperação para restaurar o acesso a um disco rígido criptografado pelo BitLocker: **Executar**	• "Baixar atualizações no repositório do Servidor de Administração" • "Entregar relatórios" • "Distribuir pacote de instalação" • "Instalar aplicativos nos Servidores de Administração secundários remotamente"	• "Relatório do status de proteção" • "Relatório de ameaças" • "Relatório de dispositivos mais infectados" • "Relatório de status dos bancos de dados antivírus" • "Relatório de erros" • "Relatório de ataques de rede" • "Relatório resumido de aplicativos de proteção do sistema de e-mail instalados" • "Relatório resumido de aplicativos de defesa de perímetro instalados" • "Relatório resumido dos tipos de aplicativos instalados" • "Relatório de usuários de dispositivos infectados" • "Relatório de incidentes" • "Relatório de eventos" • "Relatório de atividade dos pontos de distribuição" • "Relatório de Servidores de Administração secundários" • "Relatório de eventos de Controle de Dispositivos" • "Relatório de vulnerabilidades" • "Relatório de aplicativos proibidos" • "Relatório de Controle da Web" • "Relatório de status da criptografia de dispositivos gerenciados"	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
				• "Relatório de status da criptografia de dispositivos de armazenamento em massa" • "Relatório de erros de criptografia de arquivos" • "Relatório de bloqueio de acesso a dispositivos criptografados" • "Relatório de direitos de acesso a dispositivos criptografados" • "Relatório de permissões do usuário em vigor" • "Relatório de direitos"	
Funcionalidades gerais: Objetos excluídos	• **Ler** • **Gravar**	• Visualizar objetos excluídos na Lixeira: **Ler** • Excluir objetos da Lixeira: **Gravar**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: Processamento de eventos	• **Excluir eventos** • **Editar as configurações de notificação de eventos** • **Editar as configurações de log de eventos** • **Gravar**	• Alterar as configurações de registro de eventos: **Editar as configurações de log de eventos** • Alterar configurações de notificação de eventos: **Editar as configurações de notificação de eventos** • Excluir eventos: **Excluir eventos**	Nenhum	Nenhum	Configurações: • Configurações de ataque de vírus: número de detecções de vírus necessárias para criar um evento de ataque de vírus • Configurações de ataque de vírus: período de tempo para avaliação das detecções de vírus • O número máximo de eventos armazenados no banco de dados • Período de tempo para armazenar eventos dos dispositivos excluídos

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: Operações no Servidor de administração	• **Ler** • **Gravar** • **Executar** • **Modificar os objetos ACLs** • **Executar as operações nas seleções de dispositivos**	• Especificar as portas do Servidor de Administração para a conexão do Agente de Rede: **Gravar** • Especificar as portas do Proxy de ativação iniciado no Servidor de Administração: **Gravar** • Especificar as portas do Proxy de ativação para dispositivos móveis iniciadas no Servidor de Administração: **Gravar** • Especificar as portas do Servidor Web para distribuição de pacotes independentes: **Gravar** • Especificar as portas do Servidor Web para distribuição de perfis MDM: **Gravar** • Especificar as portas SSL do Servidor de Administração para a conexão pelo Kaspersky Security Center Web Console: **Gravar** • Especificar as portas do Servidor de Administração para a conexão móvel: **Gravar** • Especificar o número máximo de eventos armazenados no banco de dados do Servidor de Administração: **Gravar** • Especificar o número máximo de eventos que podem ser enviados pelo Servidor de Administração: **Gravar** • Especificar o período de tempo durante o qual os eventos podem ser enviados pelo Servidor de Administração: **Gravar**	• "Backup de dados do Servidor de Administração" • "Manutenção do banco de dados"	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: Implementação do software da Kaspersky	• **Gerenciar patches da Kaspersky** • **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	Aprovar ou rejeitar a instalação do patch: **Gerenciar patches da Kaspersky**	Nenhum	• "Relatório de uso da chave de licença pelo Servidor de Administração virtual" • "Relatório de versões de software da Kaspersky" • "Relatório de aplicativos incompatíveis" • "Relatório de versões das atualizações dos módulos de software da Kaspersky" • "Relatório de implementação da proteção"	Pacote de instalação: "Kaspersky"
Funcionalidades gerais: Gerenciamento de chaves de licença	• **Exportar arquivo de chave** • **Gravar**	• Exportar arquivo de chave: **Exportar arquivo de chave** • Modificar as configurações da chave de licença do Servidor de Administração: **Gravar**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: Gerenciamento de relatórios forçado	• **Ler** • **Gravar**	• Criar relatórios independentemente das suas ACLs: **Gravar** • Executar relatórios independentemente de suas ACLs: **Ler**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: Hierarquia de Servidores de Administração	**Configurar a hierarquia de Servidores de Administração**	Registrar, atualizar ou excluir Servidores de Administração secundários: **Configurar a hierarquia de Servidores de Administração**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: Permissões do usuário	**Modificar os objetos ACLs**	• Alterar as Propriedades de segurança de qualquer objeto: **Modificar os objetos ACLs** • Gerenciar funções de usuário: **Modificar os objetos ACLs** • Gerenciar usuários internos: **Modificar os objetos ACLs** • Gerenciar grupos de segurança: **Modificar os objetos ACLs** • Gerenciar aliases: **Modificar os objetos ACLs**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: Servidores de Administração virtuais	• **Gerenciar Servidores de Administração virtuais** • **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Obter a lista de Servidores de Administração virtuais: **Ler** • Obter informações sobre o Servidor de Administração virtual: **Ler** • Criar, atualizar ou excluir um Servidor de Administração virtual: **Gerenciar Servidores de Administração virtuais** • Mover um Servidor de Administração virtual para outro grupo: **Gerenciar Servidores de Administração virtuais** • Definir permissões do Servidor de Administração virtual: **Gerenciar Servidores de Administração virtuais**	Nenhum	"Relatório de resultados da instalação de atualizações de software de terceiros"	Nenhum
Funcionalidades gerais: Gerenciamento de chaves de criptografia	• **Ler** • **Gravar**	• Exporte as chaves de criptografia: **Ler** • Importar as chaves de criptografia: **Gravar**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Gerenciamento de Dispositivos Móveis: Geral	• **Conectar novos dispositivos** • **Enviar somente comandos de informações para dispositivos móveis** • **Enviar comandos para dispositivos móveis** • **Gerenciar certificados** • **Ler** • **Gravar**	• Obter os dados de restauração do Serviço de gerenciamento de chaves: **Ler** • Excluir os certificados de usuário: **Gerenciar certificados** • Obter a parte pública do certificado do usuário: **Ler** • Verificar se a Infraestrutura de chave pública está ativada: **Ler** • Verificar a conta da Infraestrutura de chave pública: **Ler** • Obter modelos de Infraestrutura de chave pública: **Ler** • Obter modelos de Infraestrutura de chave pública por meio do certificado de Uso de chave estendido: **Ler** • Verificar se o certificado da Infraestrutura de chave pública foi revogado: **Ler** • Atualizar as configurações de emissão de certificado do usuário: **Gerenciar certificados** • Obter as configurações de emissão de certificado do usuário: **Ler** • Obter pacotes pelo nome e versão do aplicativo: **Ler** • Definir ou cancelar o certificado do usuário: **Gerenciar certificados** • Renovar o certificado do usuário: **Gerenciar certificados** • Definir etiqueta de certificado do usuário: **Gerenciar certificados** • Executar a geração do pacote de instalação do MDM; cancelar a geração do pacote de instalação do MDM: **Conectar novos dispositivos**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Gerenciamento do sistema: Conectividade	• **Iniciar sessões RDP** • **Conexão para sessões RDP existentes** • **Iniciar túnel** • **Salvar os arquivos dos dispositivos na estação de trabalho do administrador** • **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Criar sessão de compartilhamento da área de trabalho: **Iniciar sessões RDP** • Criar sessão RDP: **Conexão para sessões RDP existentes** • Criar túnel: **Iniciar túnel** • Salvar a lista de conteúdo da rede: **Salvar os arquivos dos dispositivos na estação de trabalho do administrador**	Nenhum	"Relatório de usuários dos dispositivos"	Nenhum
Gerenciamento do sistema: Inventário de hardware	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Obter ou exportar objeto de inventário de hardware: **Ler** • Adicionar, definir ou excluir objeto de inventário de hardware: **Gravar**	Nenhum	• "Relatório do registro de hardware" • "Relatório de alterações de configuração" • "Relatório de hardware"	Nenhum
Gerenciamento do sistema: Controle de Acesso de Rede	• **Ler** • **Gravar**	• Visualizar configurações da CISCO: **Ler** • Alterar configurações da CISCO: **Gravar**	Nenhum	Nenhum	Nenhum
Gerenciamento do sistema: Implementação do sistema operacional	• **Implementar servidores PXE** • **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Implementar servidores PXE: **Implementar servidores PXE** • Visualizar uma lista de servidores PXE: **Ler** • Iniciar ou interromper o processo de instalação em clientes PXE: **Executar** • Gerenciar drivers para WinPE e imagens de sistema operacional: **Gravar**	"Criar pacote de instalação mediante imagem do SO do dispositivo de referência"	Nenhum	Pacote de instalação: "Imagem do SO"

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Gerenciamento do sistema: Gerenciamento de Patches e Vulnerabilidades	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Visualizar propriedades de patches de terceiros: **Ler** • Alterar propriedades de patches de terceiros: **Gravar**	• "Executar a sincronização com o Windows Update" • "Instalar atualizações do Windows Update" • "Corrigir vulnerabilidades" • "Instalar as atualizações necessárias e corrigir vulnerabilidades"	"Relatório de atualizações de software"	Nenhum
Gerenciamento do sistema: Instalação remota	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Visualizar as propriedades do pacote de instalação de terceiros com base no Gerenciamento de vulnerabilidades e patches: **Ler** • Alterar as propriedades do pacote de instalação de terceiros com base no Gerenciamento de vulnerabilidades e patches: **Gravar**	Nenhum	Nenhum	Pacotes de instalação: • "Aplicativo personalizado" • "Pacote VAPM"
Gerenciamento do sistema: Inventário de software	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	Nenhum	Nenhum	• "Relatório de aplicativos instalados" • "Relatório do histórico de registro de aplicativos" • "Relatório de status dos grupos de aplicativos licenciados" • "Relatório de chaves de licença de software de terceiros"	Nenhum

Funções de usuário predefinidas

As funções de usuário atribuídas aos usuários do Kaspersky Security Center fornecem conjuntos de direitos de acesso aos recursos do aplicativo.

Os usuários criados em um servidor virtual não podem receber uma função no Servidor de Administração.

É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado ou criar novas funções. Ao criar uma nova função, defina o escopo da função e atribua os direitos de acessibilidade aos recursos do Kaspersky Security Center manualmente. Algumas das funções de usuário predefinidas disponíveis no Kaspersky Security Center podem ser associadas a cargos específicos, por exemplo, **Auditor**, **Diretor de segurança**, **Supervisor** (essas funções estão presentes no Kaspersky Security Center a partir da versão 11). Os direitos de acesso dessas funções são pré-configurados de acordo com as tarefas padrão e o escopo das obrigações dos cargos associados. A tabela abaixo mostra como as funções podem ser associadas a cargos específicos.

Exemplos de funções para cargos específicos

Função	Comentário
Auditor	Permite realizar todas as operações de visualização e execução de qualquer tarefa em seleções de dispositivos conectados ao Servidor de Administração via Agente de Rede, com privilégios de administrador local (root no Linux). Recomendamos designar essa função com cautela, restrita a um grupo limitado de usuários que realmente necessitam dela para cumprir suas funções oficiais.
Supervisor	Permite a visualização de todas as operações; não permite outras operações. Você pode atribuir esta função a um diretor de segurança e a outros gerentes responsáveis pela segurança de TI em sua organização.
Diretor de segurança	Permite todas as operações de visualização, permite o gerenciamento de relatórios; concede permissões limitadas na área **Gerenciamento do sistema**: **Conectividade**. Você pode atribuir esta função a um diretor responsável pela segurança de TI em sua organização.

A tabela abaixo mostra os direitos de acesso atribuídos a cada função de usuário predefinida.

Direitos de acesso de funções de usuário predefinidas

Função	Descrição

Administrador do Servidor de Administração	Permite todas as operações nas seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Processamento de eventos**
	  • **Hierarquia de Servidores de Administração**
	  • **Servidores de Administração virtuais**
	• **Gerenciamento do sistema**:
	  • **Conectividade**
	  • **Inventário de hardware**
	  • **Inventário de software**
	
	Concede os direitos de **Leitura** e **Gravação** na área funcional **recursos gerais: gerenciamento de chaves de criptografia**.

Operador do Servidor de Administração	Concede os direitos de **Leitura** e **Execução** em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Servidores de Administração virtual**
	• **Gerenciamento do sistema**:
	  • **Conectividade**
	  • **Inventário de hardware**
	  • **Inventário de software**

Função	Descrição
Auditor	Permite todas as operações nas áreas funcionais, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Objetos excluídos** • **Gerenciamento de relatórios aplicado** Você pode atribuir esta função a uma pessoa que realiza a auditoria da sua organização.

Administrador de instalação	Permite todas as operações nas seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Implementação de software da Kaspersky**
	  • **Gerenciamento de chaves de licença**
	• **Gerenciamento do sistema**:
	  • **Implementação do sistema operacional**
	  • **Gerenciamento de patches e vulnerabilidades**
	  • **Instalação remota**
	  • **Inventário de software**
	Concede os direitos de **Leitura** e **Execução** na área funcional **Recursos gerais: Servidores de Administração virtuais**.

Operador de instalação	Concede os direitos de **Ler** e **Executar** em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Implementação de software Kaspersky** (também concede o direito de **Gerenciar patches da Kaspersky** nesta área)
	  • **Servidores de Administração virtual**
	• **Gerenciamento do sistema**:
	  • **Implementação do sistema operacional**
	  • **Gerenciamento de patches e vulnerabilidades**
	  • **Instalação remota**
	  • **Inventário de software**

Administrador do Kaspersky Endpoint Security	Permite todas as operações nas seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • Área do Kaspersky Endpoint Security, incluindo todos os recursos Concede os direitos de **Leitura** e **Gravação** na área funcional **recursos gerais: gerenciamento de chaves de criptografia**.
Operador do Kaspersky Endpoint Security	Concede os direitos de **Ler** e **Executar** em todas as seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • Área do Kaspersky Endpoint Security, incluindo todos os recursos
Administrador Principal	Permite todas as operações em áreas funcionais, *exceto* as seguintes áreas, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Gerenciamento de relatórios aplicado** Concede os direitos de **Leitura** e **Gravação** na área funcional **recursos gerais: gerenciamento de chaves de criptografia**.

Função	Descrição

Operador Principal	Concede os direitos de **Leitura** e **Execução** (quando aplicável) em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Objetos excluídos**
	  • **Operações no Servidor de Administração**
	  • **Implementação do software da Kaspersky**
	  • **Servidores de Administração virtual**
	• **Gerenciamento de Dispositivos Móveis: Geral**
	• **Gerenciamento do sistema**, incluindo todos os recursos
	• Área do Kaspersky Endpoint Security, incluindo todos os recursos

Administrador do Gerenciamento de Dispositivos Móveis	Permite todas as operações nas seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • **Gerenciamento de Dispositivos Móveis: Geral**
Operador do Gerenciamento de Dispositivos Móveis	Concede os direitos de **Leitura** e **Execução** na área funcional **Recursos gerais: Funcionalidade básica**. Concede os comandos **Leitura** e **Enviar somente informações para dispositivos móveis** na área funcional **Gerenciamento de dispositivos móveis**: **Geral**.
Diretor de segurança	Permite todas as operações nas seguintes áreas funcionais, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Gerenciamento de relatórios aplicado** Concede os direitos de **Leitura**, **Gravação**, **Execução** e **Salvamento dos arquivos dos dispositivos na estação de trabalho do administrador** e **executar operações nas seleções de dispositivos** na área funcional **gerenciamento do sistema: conectividade**. Você pode atribuir esta função a um diretor responsável pela segurança de TI em sua organização.
Usuário do Self Service Portal	Permite todas as operações na área funcional **Gerenciamento de Dispositivos Móveis: Self Service Portal**. Este recurso não é compatível com o Kaspersky Security Center 11 e versões posteriores.
Supervisor	Concede o direito de **Leitura** nas áreas funcionais **Recursos gerais**: **Acessar objetos independentemente de suas ACLs** e **Recursos gerais**: **Gerenciamento de relatórios aplicado**. Você pode atribuir esta função a um diretor de segurança e a outros gerentes responsáveis pela segurança de TI em sua organização.
Administrador de gerenciamento de patches e vulnerabilidades	Permite todas as operações nas áreas funcionais **Recursos gerais**: **Funcionalidade básica** e **Gerenciamento do sistema** (incluindo todos os recursos).
Operador de gerenciamento de patches e vulnerabilidades	Concede os direitos de **Leitura** e **Execução** (quando aplicável) nas áreas funcionais **Recursos gerais**: **Funcionalidade básica** e **Gerenciamento do sistema** (incluindo todos os recursos).
Web Console como administrador de serviço	Concede os direitos de **Leitura** e **Gravação** nos **Recursos gerais**:área funcional **Integração de aplicativos**.

Adicionar uma função de usuário

Para adicionar uma função de usuário:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.

3. Na janela de propriedades do Servidor de Administração, no painel **Seções** selecione **Funções do usuário** e clique no botão **Adicionar**.

   A seção **Funções do usuário** está disponível ser a opção **Exibir as seções das configurações de segurança** estiver ativada.

4. Na janela de propriedades **Nova função** configure a função:

   - Em **Seções**, selecione **Geral** e especifique o nome da função.

     O nome de uma função não pode incluir mais do que 100 caracteres.

   - Selecione a seção **Direitos**, e configure o conjunto de direitos ao selecionar as caixas de seleção **Permitir** e **Negar** junto aos recursos do aplicativo.

   Se estiver operando no Servidor de Administração principal, você pode ativar a opção **Retransmitir lista de funções para o Servidores de Administração secundário**.

5. Clique em **OK**.

A função foi adicionada.

As funções do usuário que foram criadas para o Servidor de Administração são exibidas na janela Propriedades do Servidor de Administração, na seção **Funções do usuário**. É possível modificar e excluir as funções do usuário, bem como atribuir funções a grupos de segurança ou usuários selecionados.

Atribuição de uma função a um usuário ou grupo de segurança

Para atribuir uma função a um usuário ou grupo de usuários:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, selecione a seção **Segurança**.

   A seção **Segurança** está disponível se a caixa de seleção **Exibir as seções das configurações de segurança** for selecionada na janela de configurações da interface.

4. No campo **Nomes de grupos ou usuários**, selecione um usuário ou grupo de usuários aos quais você deseja atribuir uma função.

   Se o usuário ou o grupo não estiver incluído no campo, você pode adicioná-lo clicando no botão **Adicionar**.

   Quando você adiciona um usuário clicando no botão **Adicionar**, você pode selecionar o tipo de autenticação do usuário (Microsoft Windows ou Kaspersky Security Center). A autenticação do Kaspersky Security Center é usada para selecionar as contas de usuários internos que são usadas para trabalhar com Servidores de Administração virtuais.

5. Selecione a guia **Funções** e clique no botão **Adicionar**.

   A janela **Funções do usuário** é exibida. Essa janela exibe funções do usuário que foram criadas.

6. Na janela **Funções do usuário**, selecione uma função para o grupo do usuário.

7. Clique em **OK**.

A função com um conjunto de direitos para trabalhar com o Servidor de Administração será atribuída ao usuário ou ao grupo de segurança. As funções que foram atribuídas são exibidas na guia **Funções** na seção **Segurança** da janela de propriedades do Servidor de Administração.

Atribuir permissões a usuários e grupos

Você pode conceder aos usuários e grupos permissões para usar recursos diferentes do Servidor de Administração e dos programas da Kaspersky para os quais você tem plugins de gerenciamento como, por exemplo, o Kaspersky Endpoint Security for Windows.

Para atribuir as permissões a um usuário ou grupo de usuários:

1. Na árvore do console, execute uma das seguintes ações:

   - Expanda o nó do **Servidor de Administração** e selecione a subpasta com o nome do Administração de Administração desejado.

   - Selecione o grupo de administração.

2. No menu de contexto do Servidor de Administração ou o grupo de administração, selecione **Propriedades**.

3. Na janela de propriedades do Servidor de Administração (ou na janela de propriedades do grupo de administração) que se abre, no painel esquerdo **Seções**, selecione **Segurança**.

   A seção **Segurança** está disponível se a caixa de seleção **Exibir as seções das configurações de segurança** for selecionada na janela de configurações da interface.

4. Na seção **Segurança**, na lista **Nomes de grupos ou usuários**, selecione um usuário ou um grupo.

5. Na lista de permissões na parte inferior do espaço de trabalho, na guia **Direitos**, configure o conjunto de direitos do usuário ou grupo:

   a. Clique nos sinais de mais (+) para expandir os nós na lista e obter acesso às permissões.

   b. Marque as caixas de seleção **Permitir** e **Negar**, ao lado das permissões que você deseja.

      Exemplo 1: expanda o nó **Acessar objetos independentemente de suas ACLs** ou o nó **Objetos excluídos** e selecione **Ler**.

      Exemplo 2: expanda o nó **Funcionalidade básica** e selecione **Gravar**.

6. Quando você tiver configurado o conjunto de direitos, clique em **Aplicar**.

O conjunto de direitos do usuário ou do grupo de usuários será configurado.

As permissões do Servidor de Administração (ou do grupo de administração) estão divididas nas seguintes áreas:

- Recursos gerais:
  - Gerenciamento de grupos de administração
  - Acessar objetos independentemente de suas ACLs
  - Funcionalidade básica
  - Objetos excluídos
  - Processamento de eventos
  - Operações no Servidor de administração (somente na janela de propriedades do Servidor de Administração)
  - Implementar aplicativos Kaspersky
  - Gerenciamento de chaves de licença
  - Gerenciamento de relatórios aplicado
  - Hierarquia dos Servidores
  - Direitos de usuário
  - Servidores de Administração virtual
- Gerenciamento de Dispositivos Móveis:
  - Geral
- Gerenciamento do sistema:
  - Conectividade
  - Inventário de hardware
  - Controle de Acesso de Rede
  - Implementação do sistema operacional
  - Gerenciar vulnerabilidades e patches
  - Instalação remota
  - Inventário de software

Se nem **Permitir** nem **Negar** estiverem selecionados para uma permissão, a permissão será considerada como *indefinida*: será negada até que seja explicitamente negada ou permitida pelo usuário.

Os direitos de um usuário são a soma:

- Dos direitos do próprio usuário
- Dos direitos de todas as funções atribuídas a esse usuário
- Dos direitos de todo o grupo de segurança ao qual o usuário pertence
- Dos direitos de todas as funções atribuídas aos grupos de segurança aos quais o usuário pertence

Se pelo menos um desses conjuntos de direitos tiver **Negar** em uma permissão, a permissão será negada ao usuário, mesmo se outros conjuntos permitirem-na ou deixarem-na indefinida.

Propagando funções de usuário aos Servidores de Administração secundários

Por padrão, as listas de funções de usuário dos Servidores de Administração principal e secundários são independentes. Você pode configurar o aplicativo para propagar automaticamente as funções de usuário criadas no Servidor de Administração principal a todos dos Servidores de Administração secundários. As funções de usuário também podem ser propagadas de um Servidor de Administração secundário para seus próprios Servidores de Administração secundários.

Para propagar funções de usuário do Servidor de Administração principal aos Servidores de Administração secundários:

1. Abra a janela principal do aplicativo.
2. Execute uma das seguintes ações:
   - Na árvore do console, clique com o botão direito no nome do Servidor de Administração e selecione **Propriedades** no menu de contexto.
   - Se você tem uma política de Servidor de Administração ativa, no espaço de trabalho da pasta **Políticas**, clique com o botão direito nessa política e selecione **Propriedades** no menu de contexto.
3. Na janela de propriedades do Servidor de Administração ou na janela de configurações da política, no painel **Seções**, selecione **Funções de usuário**.

   A seção **Funções do usuário** está disponível ser a opção **Exibir as seções das configurações de segurança** estiver ativada.

4. Ative a opção **Retransmitir lista de funções para Servidores de Administração secundários**.
5. Clique em **OK**.

   O aplicativo copia as funções de usuário do Servidor de Administração principal para os Servidores de Administração secundários.

Quando a opção **Retransmitir lista de funções para Servidores de Administração secundários** é ativada e as funções de usuário são propagadas, elas não podem ser editadas nem excluídas nos Servidores de Administração secundários. Ao criar uma nova função ou editar uma função existente no Servidor de Administração principal, as modificações são automaticamente copiadas para os Servidores de Administração secundários. Ao excluir uma função de usuário no Servidor de Administração principal, essa função permanece nos Servidores de Administração secundários posteriormente, mas pode ser editada, nem excluída.

As funções propagadas para o Servidor de Administração secundário a partir do Servidor principal são exibidas com o ícone de cadeado (🔒). Você não pode editar essas funções no Servidor de Administração secundário.

Se você criar uma função no Servidor de Administração principal e existir uma função com o mesmo nome no Servidor de Administração secundário, a nova função será copiada para o Servidor de Administração secundário com o índice adicionado ao nome, por exemplo, ~~1, ~~2 (o índice pode ser aleatório).

Se você desativar a opção **Retransmitir lista de funções para Servidores de Administração secundários**, todas as funções de usuário permanecerão nos Servidores de Administração secundários, mas serão independentes das que estão no Servidor de Administração principal. Após se tornarem independentes, as funções de usuário nos Servidores de Administração secundários podem ser editadas ou excluídas.

Atribuindo o usuário como proprietário de dispositivo

Você pode indicar o usuário como um proprietário de um dispositivo para alocar um dispositivo àquele usuário. Se você precisar executar algumas ações no dispositivo (por exemplo, um upgrade de hardware), o administrador poderá notificar o proprietário do dispositivo para autorizar estas ações.

Para atribuir um usuário como o proprietário de um de dispositivo:

1. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.
2. No espaço de trabalho da pasta, na guia **Dispositivos**, selecione o dispositivo para o qual você precisar atribuir um proprietário.
3. No menu de contexto do dispositivo, selecione **Propriedades**.
4. Na janela de propriedades do dispositivo, selecione **Informações do sistema** → **Sessões**.
5. Clique no botão **Atribuir** junto ao campo **Proprietário do dispositivo**.
6. Na janela **Seleção de usuários**, selecione o usuário o qual você deseja atribuir como o proprietário do dispositivo, e clique no botão **OK**.
7. Clique em **OK**.

O proprietário de dispositivo está atribuído. Por padrão, o campo **Proprietário do dispositivo** é preenchido com um valor do Active Directory e é atualizado durante cada sondagem do Active Directory. Você pode exibir a lista de proprietários de dispositivo na pasta **Relatório de proprietários de dispositivo**. Você pode criar um relatório usando o Assistente de novo modelo de relatório.

Enviar mensagens a utilizadores

Para enviar uma mensagem a um usuário por e-mail:

1. Na árvore do console, na pasta **Contas de usuário**, selecione um usuário.

   A pasta **Contas de usuário** é uma subpasta da pasta **Avançado** por padrão.
2. No menu de contexto do usuário, selecione **Notificar por e-mail**.
3. Preencha os campos relevantes na janela **Enviar mensagem ao usuário** e clique no botão **OK**.

A mensagem será enviada para o e-mail especificado nas propriedades do usuário.

Para enviar uma mensagem SMS a um usuário:

1. Na árvore do console, na pasta **Contas de usuário**, selecione um usuário.
2. No menu de contexto do usuário, selecione **Enviar um SMS**.
3. Preencha os campos relevantes na janela **Texto do SMS** e clique no botão **OK**.

A mensagem será enviada para o dispositivo móvel com o número especificado nas propriedades do usuário.

Visualizar a lista de dispositivos móveis de usuários

Para visualizar a lista de dispositivos móveis de um usuário:

1. Na árvore do console, na pasta **Contas de usuário**, selecione um usuário.

   A pasta **Contas de usuário** é uma subpasta da pasta **Avançado** por padrão.
2. No menu de contexto da conta do usuário, selecione **Propriedades**.
3. Na janela de propriedades da conta do usuário, selecione a seção **Dispositivos móveis**.

Na seção **Dispositivos móveis**, você pode visualizar a lista de dispositivos móveis do usuário e informações sobre cada um deles. Você pode clicar no botão **Exportar para arquivo** para salvar a lista de dispositivos móveis em um arquivo.

Instalar um certificado de um usuário

Você pode instalar três tipos de certificados para um usuário:

- Certificado compartilhado, o qual é necessário para identificar o dispositivo móvel do usuário.
- Certificado de correio, o qual é requerido para configurar o correio corporativo no dispositivo móvel do usuário.
- Certificado de VPN, o qual é requerido para configurar a rede privada virtual do dispositivo móvel do usuário.

Para emitir um certificado a um usuário e o instalar:

1. Na árvore do console, abra a pasta **Contas de usuário** e selecione uma conta de usuário.

   A pasta **Contas de usuário** é uma subpasta da pasta **Avançado** por padrão.
2. No menu de contexto da conta do usuário, selecione **Instalar certificado**.

O Assistente de Instalação de Certificado é iniciado. Siga as instruções do Assistente.

Após a conclusão do Assistente de Instalação de Certificado, o certificado será criado e instalado para o usuário. Você pode visualizar a lista de certificados de usuário instalados e exportá-la para um arquivo.

Visualizar a lista de certificados emitidos a um usuário

Para visualizar uma lista de todos os certificados emitidos a um usuário:

1. Na árvore do console, na pasta **Contas de usuário**, selecione um usuário.

   A pasta **Contas de usuário** é uma subpasta da pasta **Avançado** por padrão.

2. No menu de contexto da conta do usuário, selecione **Propriedades**.

3. Na janela de propriedades da conta do usuário, selecione a seção **Certificados**.

Na seção **Certificados**, você pode visualizar a lista de certificados do usuário e informações sobre cada um deles. Você pode clicar no botão **Exportar para arquivo** para salvar a lista de certificados em um arquivo.

Sobre o administrador de um Servidor de Administração virtual

Um administrador da rede corporativa gerenciada através de um Servidor de Administração virtual inicia o Kaspersky Security Center Web Console sob a conta de usuário especificada nesta janela para exibir os detalhes da proteção antivírus.

Se necessário, podem ser criadas várias contas de administrador num Servidor virtual.

Os usuários criados em um servidor virtual não podem receber uma função no Servidor de Administração.

O administrador de um Servidor de Administração virtual é um usuário interno do Kaspersky Security Center. Os dados sobre os usuários internos não são transferidos para o sistema operacional. O Kaspersky Security Center autentica os usuários internos.

Instalação remota de sistemas operacionais e aplicativos

O Kaspersky Security Center permite criar imagens de sistemas operacionais e implementá-los em dispositivos cliente na rede, assim como executar a instalação remota de aplicativos Kaspersky ou de outros fornecedores.

Para criar imagens de sistemas operacionais, instale as ferramentas de implementação do Windows ADK e o complemento do Windows PE para Windows ADK no Servidor de Administração. É possível criar uma imagem de qualquer versão do sistema operacional Windows que atenda aos requisitos do Kaspersky Security Center.

O Kaspersky Security Center não é compatível com as versões de 64 bits do Windows ADK e do Windows PE.

Capturar imagens de sistemas operacionais

O Kaspersky Security Center pode capturar imagens de sistemas operacionais de dispositivos e transferir essas imagens para o Servidor de Administração. Essas imagens de sistemas operacionais são armazenadas no Servidor de Administração em uma pasta dedicada. A imagem do sistema operacional de um dispositivo de referência é capturada e então criada através de uma tarefa de criação de pacote de instalação.

A funcionalidade da captura de imagens de sistemas operacionais tem os seguintes recursos:

- Uma imagem do sistema operacional não pode ser capturada em um dispositivo no qual o Servidor de Administração está instalado.
- Durante a captura de uma imagem do sistema operacional, um utilitário denominado sysprep.exe redefine as configurações do dispositivo de referência. Se for necessário restaurar as configurações do dispositivo de referência, marque a caixa de seleção **Criar uma cópia backup do estado do dispositivo** no Assistente de criação de tarefas de imagem de SO.
- O processo de captura da imagem fornece um reinício do dispositivo de referência.

Implementar imagens de sistemas operacionais em novos dispositivos

Você pode usar as imagens recebidas para implementar em novos dispositivos na rede nos quais ainda não foi instalado nenhuma sistema operacional. Nesse caso, é usada uma tecnologia denominada Preboot eXecution Environment (PXE). Você seleciona um dispositivo na rede que será usado como Servidor PXE. Este dispositivo deve atender os seguintes requisitos:

- O Agente de Rede deve ser instalado no dispositivo.
- Um servidor DHCP não pode estar ativo no dispositivo, já que um servidor PXE usa as mesmas portas que um servidor DHCP.
- O segmento da rede que inclui o dispositivo não deve conter nenhum Servidor PXE.

Para implementar um sistema operacional, as seguintes condições devem ser atendidas:

- Uma placa de rede deve estar instalada no dispositivo.
- O dispositivo deve estar conectado à rede.
- A opção inicialização de rede deve ser selecionada no BIOS ao inicializar o dispositivo.

A implementação de um sistema operacional é efetuada do seguinte modo:

1. O dispositivo cliente estabelece uma conexão com o servidor PXE durante o processo de inicialização.
2. O dispositivo cliente inicia no Windows Preinstallation Environment (WinPE).

   Adicionar o dispositivo ao WinPE pode requerer a configuração do conjunto de drivers para WinPE.

3. O dispositivo cliente é registrado no Servidor de Administração.

4. O administrador atribui ao dispositivo cliente um pacote de instalação com uma imagem do sistema operacional.

   O administrador pode adicionar os drivers necessários para o pacote de instalação com a imagem de sistema operacional. O administrador também pode especificar um arquivo de configuração com as configurações do sistema operacional (arquivo de resposta) que deve ser aplicado durante a instalação.

5. O sistema operacional é implementado no dispositivo cliente.

O administrador pode especificar manualmente os endereços MAC dos dispositivos cliente que ainda não foram conectados e atribuir aos mesmos o pacote de instalação com a imagem do sistema operacional. Quando os dispositivos cliente selecionados estiverem conectados ao Servidor PXE, o sistema operacional é instalado automaticamente nesses dispositivos.

Implementar imagens de sistemas operacionais em dispositivos onde outro sistema operacional já foi instalado

A implementação de imagens de sistemas operacionais em dispositivos cliente onde outro sistema operacional já foi instalado é executada através da tarefa de instalação remota para dispositivos específicos.

Observe que é realizada uma instalação limpa do sistema operacional. Todos os dados serão excluídos.

Instalar aplicativos Kaspersky e de outros fornecedores

O administrador pode criar pacotes de instalação de quaisquer aplicativos, incluindo os aplicativos especificados pelo usuário e instalar os aplicativos nos dispositivos cliente através da tarefa de instalação remota.

Criação de imagens de sistemas operacionais

As imagens de sistemas operacionais são criadas usando a tarefa de remover a imagem de sistema operacional do dispositivo de referência.

Para criar uma tarefa de criação de imagens do sistema operacional:

1. Na pasta **Instalação remota** na árvore do console, selecione a subpasta **Pacotes de instalação**.
2. Clique no botão **Criar pacote de instalação** para executar o Assistente de novo pacote.
3. Na janela **Selecione o tipo de pacote de instalação** do assistente, clique no botão **Criar um pacote de instalação com a imagem do sistema operacional**.
4. Siga as instruções do Assistente.

   Quando o assistente for concluído, uma tarefa do Servidor de Administração é criada denominada **Criar pacote de instalação conforme a imagem do SO do dispositivo de referência**. Você pode visualizar a tarefa na pasta **Tarefas**.

Quando a tarefa **Criar pacote de instalação conforme a imagem do SO do dispositivo de referência** estiver concluída, é criado um pacote de instalação que você pode usar para implementar o sistema operacional em dispositivos cliente através de um Servidor PXE ou da tarefa de instalação remota. Você pode visualizar o pacote de instalação na pasta **Pacotes de instalação**.

Imagens de instalação de sistemas operacionais

O Kaspersky Security Center permite implementar imagens WIM de sistemas operacionais Windows® desktop com base em servidor em dispositivos dentro de uma rede da organização.

Os seguintes métodos podem ser usados para recuperar uma imagem do sistema operacional que seria implementável usando as ferramentas do Kaspersky Security Center:

- Importar de um arquivo install.wim incluído no pacote de distribuição do Windows
- Capturar uma imagem de um dispositivo de referência

Dois cenários são suportados para a implementação de imagens do sistema operacional:

- A implementação em um dispositivo "limpo", ou seja, sem qualquer sistema operacional instalado
- A implementação em um dispositivo executando o Windows

Use o Windows Preinstallation Environment (Windows PE) para capturar e implementar imagens do sistema operacional. Todos os drivers necessários para o funcionamento apropriado de todos os dispositivos alvo devem ser adicionados ao WinPE. Geralmente, os drivers do adaptador de rede e do controlador de armazenamento devem ser adicionados.

Os seguintes requisitos devem ser atendidos para poder implementar cenários de implementação de imagem e captura:

- O kit de instalação automática do Windows (WAIK) versão 2.0 ou superior ou Windows ADK com o complemento do Windows PE para o Windows ADK deve ser instalado no Servidor de Administração. Se o cenário permitir a instalação ou a captura de imagens no Windows XP, o WAIK deve ser instalado.
- Um servidor DHCP deve estar disponível na rede onde o dispositivo-alvo estiver localizado.
- A pasta compartilhada do Servidor de Administração deve estar aberta para ler da rede onde o dispositivo alvo estiver localizado. Se a pasta compartilhada estiver localizada no Servidor de Administração, o acesso é necessário para a conta KlPxeUser (a contra é criada automaticamente ao executar o Instalador do Servidor de Administração). Se a pasta compartilhada estiver localizada fora do Servidor de Administração, o acesso deve ser concedido a todos.

Ao selecionar a imagem do sistema operacional a ser instalado, o administrador deve especificar explicitamente a arquitetura da CPU do dispositivo alvo: x86 ou x86-64.

Configurar endereço de servidor proxy da KSN

Por padrão, o nome da conexão ou endereço IP do Servidor de Administração coincide com os endereços de servidor proxy da KSN. Caso você altere o nome da conexão ou o endereço IP do Servidor de Administração, será necessário especificar o endereço correto do servidor proxy KSN para evitar a perda de conexão entre os dispositivos host e a KSN.

Para configurar endereço de servidor proxy da KSN:

1. Na árvore do console, vá para **Avançado** → **Instalação remota** → **Pacotes de instalação**.
2. No menu contextual **Pacotes de instalação**, selecione **Propriedades**.
3. Na janela exibida, especifique o endereço do novo servidor proxy da KSN na guia **Geral**.
4. Clique no botão **Aplicar**.

A partir de agora, o endereço especificado será usado como endereço de servidor proxy da KSN. Recomendamos ativar a opção **Usar proxy da KSN** para otimizar o tráfego na rede.

Adição de drivers ao Windows Preinstallation Environment (WinPE)

Para adicionar drivers ao Windows Preinstallation Environment (WinPE):

1. Na pasta **Instalação remota** da árvore do console, selecione a subpasta **Implementar imagens de dispositivos**.
2. No espaço de trabalho da pasta **Implementar imagens de dispositivos**, clique no botão **Ações adicionais** e selecione **Configurar conjunto de drivers para Windows Preinstallation Environment (WinPE)** na lista suspensa.

   A janela **Drivers do ambiente de pré-instalação do Windows** se abre.
3. Na janela **Drivers do ambiente de pré-instalação do Windows** clique no botão **Adicionar**.

   A janela **Selecionar driver** se abre.
4. Na janela **Selecionar driver**, selecione um driver na lista.

   Se o driver necessário estiver ausente da lista, clique no botão **Adicionar** e especifique o nome do driver e a pasta do pacote de distribuição do driver na janela **Adicionar driver** que será aberta.

   Você pode selecionar uma pasta ao clicar no botão **Procurar**.

   Na janela **Adicionar driver** clique em **OK**.
5. Na janela **Selecionar driver** clique em **OK**.

   O driver será adicionado ao repositório do Servidor de Administração. Quando o driver é adicionado ao repositório, ele é exibido na janela **Selecionar driver**.
6. Na janela **Drivers do ambiente de pré-instalação do Windows** clique em **OK**.

O driver será adicionado ao Windows Preinstallation Environment (WinPE).

Adição de drivers a um pacote de instalação com uma imagem de sistema operacional

Para adicionar drivers a um pacote de instalação com uma imagem de sistema operacional:

1. Na pasta **Instalação remota** na árvore do console, selecione a subpasta **Pacotes de instalação**.
2. No menu de contexto de um pacote de instalação com uma imagem do sistema operacional, selecione **Propriedades**.

   A janela de propriedades do pacote de instalação abre.
3. Na janela Propriedades do pacote de instalação, selecione a seção **Drivers adicionais**.
4. Clique no botão **Adicionar** na seção **Drivers adicionais**.

   A janela **Selecionar driver** se abre.
5. Na janela **Selecionar driver**, selecione os drivers que você deseja adicionar ao pacote de instalação com a imagem do sistema operacional.

   Você pode adicionar novos drivers ao repositório do Servidor de Administração, clicando no botão **Adicionar** na janela **Selecionar driver**.
6. Clique em **OK**.

Os drivers adicionados são exibidos na seção **Drivers adicionais** da janela Propriedades do pacote de instalação com a imagem do sistema operacional.

Configuração do utilitário sysprep.exe

O utilitário sysrep.exe destina-se a preparar o dispositivo para a criação de uma imagem do sistema operacional.

Para configurar o utilitário sysprep.exe:

1. Na pasta **Instalação remota** na árvore do console, selecione a subpasta **Pacotes de instalação**.
2. No menu de contexto de um pacote de instalação com uma imagem do sistema operacional, selecione **Propriedades**.

   A janela de propriedades do pacote de instalação abre.
3. Na janela Propriedades do pacote de instalação, selecione a seção **Configurações de sysprep.exe**.

4. Na seção **Configurações de sysprep.exe**, especifique um arquivo de configuração que será usado durante a implementação do sistema operacional no dispositivo cliente:

   - **Utilizar arquivo de configuração padrão**. Selecione esta opção para usar o arquivo de resposta gerado por padrão durante a captura da imagem do sistema operacional.
   - **Especificar valores personalizados das configurações principais**. Selecione esta opção para especificar valores de configurações através da interface do usuário.
   - **Especificar arquivo de configuração**. Selecione esta opção para usar um arquivo de resposta padrão.

5. Para aplicar as alterações feitas, clique no botão **Aplicar**.

Implementação de sistemas operacionais em novos dispositivos na rede

Para implementar um sistema operacional em novos dispositivos que ainda não tiveram um sistema operacional instalado:

1. Na pasta **Instalação remota** da árvore do console, selecione a subpasta **Implementar imagens de dispositivos**.

   Verifique e confirme se a opção **Exibir o Gerenciamento de Patches e Vulnerabilidades** está ativada na janela **Configurar a interface**. Caso contrário, a pasta de **Instalação remota** não será exibida.

2. Clique no botão **Ações adicionais** e selecione **Gerenciar a lista de servidores PXE na rede** na lista suspensa.

   A janela **Propriedades: Implementar imagens do dispositivo** será aberta na seção **Servidores PXE**.

3. Na seção **Servidores PXE**, clique no botão **Adicionar** e na janela **Servidores PXE** que se abre, selecione o dispositivo que será usados com o servidor PXE.

   O dispositivo que você adicionou é exibido na seção Servidores PXE. Os arquivos WinPE criados são transferidos para o dispositivo a partir do Servidor de Administração. O processo de transferência de arquivos geralmente leva 10 minutos. Após a conclusão da transferência, o valor **Status** exibido muda de **Iniciar** para **Pronto**.

4. Na seção **Servidores PXE**, selecione um servidor PXE e clique no botão **Propriedades**.

5. Na janela de propriedades do servidor PXE selecionado, na guia **Configurações da conexão com o servidor PXE**, configure a conexão entre o Servidor de Administração e o servidor PXE.

6. Inicialize o dispositivo cliente no qual você quer implementar o sistema operacional.

7. Na BIOS do dispositivo cliente, selecione a opção Instalação de inicialização da rede.

   O dispositivo cliente se conecta ao servidor PXE e é então exibido no espaço de trabalho da pasta **Implementar imagens de dispositivos**.

8. Na seção **Ações**, clique no link **Atribuir pacote de instalação** para selecionar um pacote de instalação que será usado para instalar o sistema operacional no dispositivo selecionado.

   Use a ferramenta DiskPart no dispositivo selecionado para verificar os discos disponíveis. No prompt de comando do Windows PE, digite `diskpart` para abrir a ferramenta DiskPart. Digite `list disk` para listar os discos.

   Após você ter adicionado o dispositivo e atribuído o pacote de instalação ao mesmo, a implementação do sistema operacional é iniciada automaticamente nesse dispositivo.

9. Para cancelar a implementação de um sistema operacional no dispositivo cliente, clique no link **Cancelar a instalação da imagem do SO** na seção **Ações**.

Para adicionar dispositivos por endereço MAC:

- Na pasta **Implementar imagens de dispositivos**, clique em **Adicionar endereços MAC do dispositivo** para abrir a janela **Novo dispositivo**, e especifique o endereço MAC do dispositivo que você quer adicionar.

- Na pasta **Implementar imagens de dispositivos**, clique em **Importar endereços MAC de dispositivos a partir do arquivo** para selecionar o arquivo que contém uma lista de endereços MAC de todos os dispositivos nos quais você quer implementar um sistema operacional.

Implementação de sistemas operacionais em dispositivos cliente

Para implementar um sistema operacional em dispositivos clientes com outro sistema operacional já instalado:

1. Na árvore do console, abra a pasta **Instalação remota** e clique no link **Implementar o pacote de instalação nos dispositivos gerenciados (estações de trabalho)** para executar o Assistente de implementação da proteção.

2. Na janela **Selecionar o pacote de instalação** do assistente, especifique um pacote de instalação com uma imagem do sistema operacional.

3. Siga as instruções do Assistente.

Quando o assistente concluir sua operação, uma tarefa de instalação remota será criada para a instalação do sistema operacional em dispositivos cliente. Você pode iniciar ou parar a tarefa na pasta **Tarefas**.

Criação de pacotes de instalação de aplicativos

Para criar um pacote de instalação do aplicativo:

1. Na pasta **Instalação remota** na árvore do console, selecione a subpasta **Pacotes de instalação**.

2. Clique no botão **Criar pacote de instalação** para executar o Assistente de novo pacote.

3. Na janela **Selecione o tipo de pacote de instalação** do assistente, clique em um dos seguintes botões:

- **Criar um pacote de instalação para um aplicativo da Kaspersky**. Selecione esta opção se você quiser criar um pacote de instalação para um aplicativo da Kaspersky.

- **Criar um pacote de instalação para o arquivo executável especificado**. Selecione esta opção se você quiser criar um pacote de instalação para um aplicativo de terceiro ao usar um arquivo executável. Normalmente, o arquivo executável é um arquivo de instalação do aplicativo.

  - Copiar pastas inteira para o pacote de instalação

    Selecione esta opção se o arquivo executável está acompanhado por arquivos adicionais necessários para a instalação do aplicativo. Antes de você ativar esta opção, assegure-se de que todos os arquivos necessários estão armazenados na mesma pasta. Se esta opção estiver ativada, o aplicativo adiciona todo o conteúdo da pasta, incluindo o arquivo executável, no pacote de instalação.

  - Especificar os parâmetros de instalação

    Para a instalação remota com êxito, a maioria dos aplicativos requer que a instalação seja executada no modo silencioso. Se este for o caso, você precisa especificar o parâmetro para a instalação silenciosa.

    Defina as configurações de instalação:

    - **Linha de comando de arquivo executável**

      Se o aplicativo requer parâmetros adicionais para uma instalação silenciosa, especifique-os neste campo. Consulte a documentação do fornecedor para obter detalhes.

      Você também pode inserir outros parâmetros.

    - **Converter configurações nos valores recomendados para aplicativos reconhecidos pelo Kaspersky Security Center**

      O aplicativo será instalado com as configurações recomendadas, se as informações sobre o aplicativo especificado estiverem contidas no banco de dados da Kaspersky.

      Se você inseriu parâmetros no campo **Linha de comando de arquivo executável**, ela é reescrita com as configurações recomendadas.

      Por padrão, esta opção está ativada.

      O banco de dados da Kaspersky é criado e mantido pelos analistas da Kaspersky. Para cada aplicativo que for adicionado no banco de dados, os analistas da Kaspersky definem as configurações ótimas de instalação. As configurações são definidas para assegurar a instalação remota com êxito de um aplicativo em um dispositivo cliente. O banco de dados é atualizado no Servidor de Administração quando a tarefa Baixar as atualizações no repositório do Servidor de Administração for executada.

- **Selecione um aplicativo no banco de dados da Kaspersky para criar um pacote de instalação**. Selecione esta opção se você quiser selecionar o aplicativo de terceiro necessário no banco de dados da Kaspersky para criar um pacote de instalação. O banco de dados da Kaspersky é criado automaticamente quando a tarefa Baixar as atualizações no repositório do Servidor de Administração for executada; os aplicativos são exibidos na lista.

- **Crie um pacote de instalação com a imagem do sistema operacional**. Selecione esta opção se você desejar criar um pacote de instalação com uma imagem do sistema operacional de um dispositivo de referência.

Quando o assistente for concluído, uma tarefa do Servidor de Administração é criada denominada **Criar pacote de instalação quando da referência da imagem**. Quando a tarefa estiver concluída, é criado um pacote de instalação que você pode usar para implementar a imagem do sistema operacional através de um servidor PXE ou da tarefa de instalação remota.

4. Siga as instruções do Assistente.

Quando o assistente concluir sua operação, um pacote de instalação será criado que você poderá usar para instalar o aplicativo nos dispositivos cliente. Você pode visualizar o pacote de instalação ao selecionar **Pacotes de instalação** na árvore do console.

Emitindo um certificado para pacotes de instalação de aplicativos

Para emitir um certificado para o pacote de instalação de um aplicativo:

1. Na pasta **Instalação remota** na árvore do console, selecione a subpasta **Pacotes de instalação**.

   Por padrão, a pasta **Instalação remota** é uma subpasta da pasta **Avançado**.

2. No menu de contexto da pasta **Pacotes de instalação**, selecione **Avançado**.

   Isso abre a janela Propriedades da pasta **Pacotes de instalação**.

3. Na janela de propriedades da pasta **Pacotes de instalação**, selecione a seção **Assinar pacotes independentes**.

4. Na seção **Assinar pacotes independentes**, clique no botão **Especificar**.

   A janela **Certificado**.

5. No campo **Tipo de certificado**, especifique o tipo de certificado público ou privado:

   - Se o valor **Contêiner PKCS#12** for selecionado, especifique o arquivo de certificado e a senha.
   - Se o valor **Certificado X.509** estiver selecionado:

     a. Especifique um arquivo de chave privada (um com a extensão *.prk ou *.pem).

     b. Especifique a senha da chave privada.

     c. Especifique o arquivo de chave pública (com a extensão *.cer).

6. Clique em **OK**.

Um certificado para o pacote de instalação do aplicativo é emitido.

Instalar aplicativos em dispositivos cliente

Para instalar um aplicativo nos dispositivos cliente:

1. Na árvore do console, abra a pasta **Instalação remota** clique no link **Implementar o pacote de instalação nos dispositivos gerenciados (estações de trabalho)** para executar o Assistente de implementação da proteção.
2. Na janela **Selecionar o pacote de instalação** do assistente, especifique o pacote de instalação de um aplicativo que você deseja instalar.
3. Siga as instruções do Assistente.

Quando o assistente concluir sua operação, uma tarefa de instalação remota é criada para instalar o aplicativo em dispositivos de cliente. Você pode iniciar ou parar a tarefa na pasta **Tarefas**.

Usando o Assistente de implementação da proteção, você pode instalar o Agente de Rede nos dispositivos clientes que executam o Windows, Linux e macOS.

Para gerenciar aplicativos de segurança de 64 bits usando o Kaspersky Security Center nos dispositivos executando o sistema operacional Linux, você deve usar o Agente de Rede Linux de 64 bits. Você pode baixar a versão necessária do Agente de Rede do site de Suporte Técnico.

Antes da instalação remota do Agente de Rede em um dispositivo que executa o Linux, você deve preparar o dispositivo.

Gerenciar revisões de objeto

Esta seção contém informações sobre o gerenciamento de revisão de objeto. O Kaspersky Security Center lhe permite acompanhar a modificação de objeto. Cada vez quando você salva modificações feitas à um objeto, uma *revisão* é criada. Cada revisão tem um número.

Os objetos do aplicativo suportam o gerenciamento de revisão incluem:

- Propriedades do Servidor de Administração
- Políticas
- Tarefas
- Grupos de administração
- Contas de usuário
- Pacotes de instalação

Você pode executar as seguintes ações nas revisões do objeto:

- Comparar uma revisão selecionada à atual
- Compare selected revisions
- Comparar um objeto com uma revisão selecionada de outro objeto do mesmo tipo
- Exibir uma revisão selecionada
- Reverter as modificações feitas a um objeto para uma revisão selecionada
- Salve as revisões como um arquivo .txt

Na janela de propriedades de qualquer objeto que suporta o gerenciamento de revisão, a seção **Histórico de revisões** exibe uma lista de revisões de objeto com os seguintes detalhes:

- Número de revisão do objeto
- Data e hora em que o objeto foi modificado
- Nome do usuário que modificou o objeto
- A ação executada no objeto
- A descrição da revisão relativa à modificação feita nas configurações do objeto

Exibir a seção de Histórico de revisão

Você pode comparar revisões de um objeto à revisão atual, comparar revisões diferentes selecionadas na lista ou comparar uma revisão de um objeto a uma revisão de outro objeto do mesmo tipo.

*Para exibir a seção **Histórico de revisões** de um objeto:*

1. Na árvore do console, selecione um dos seguintes objetos:

   - Nó do **Servidor de Administração**
   - Pasta **Políticas**
   - Pasta **Tarefas**
   - Pasta de um grupo de administração
   - Pasta **Contas de usuário**
   - Pasta **Objetos excluídos**
   - Subpasta **Pacotes de instalação** aninhada na pasta **Instalação remota**

2. Dependendo da localização do objeto relevante, execute uma das seguintes ações:

   - Se o objeto estiver no nó do **Servidor de Administração** ou em um nó do grupo de administração, clique com o botão direito no nó e, no menu de contexto, selecione **Propriedades**.
   - Se o objeto estiver na pasta **Políticas**, **Tarefas**, **Contas de usuário**, **Objetos excluídos** ou **Pacotes de instalação**, selecione a pasta, e no espaço de trabalho correspondente selecione o objeto.

   A janela de propriedades do objeto é aberta.

3. No painel esquerdo **Seções**, selecione **Histórico de revisões**.

   O histórico de revisão é exibido no espaço de trabalho.

Comparar revisões de objeto

Você pode comparar revisões passadas de um objeto à revisão atual, comparar revisões diferentes selecionadas na lista ou comparar uma revisão de um objeto a uma revisão de outro objeto do mesmo tipo.

Para comparar revisões de um objeto:

1. Selecione um objeto e prossiga para a janela de propriedades do objeto.
2. Na janela de propriedades, siga para a seção **Histórico de revisões**.

3. No espaço de trabalho, na lista de revisões de objeto, selecione a revisão para comparação.

   Para selecionar mais de uma revisão de objeto, use as teclas **Shift** e **Ctrl**.

4. Execute uma das seguintes ações:

   - Clique no botão de divisão **Comparar** e selecione um dos valores na lista suspensa:

     - **Comparar com a revisão atual**

       Selecione esta opção para comparar a revisão selecionada à atual.

     - **Comparar as revisões selecionadas**

       Selecione esta opção de comparar duas revisões selecionadas.

     - **Comparar com outra tarefa**

       Se você trabalha com revisões de tarefa, selecione **Comparar com outra tarefa** para comparar a revisão selecionada com a revisão de outra tarefa.

       Se você trabalha com revisões de política, selecione **Comparar com outra política** para comparar a revisão selecionada com a revisão de outra política.

   - Clique duas vezes no nome de uma revisão e, na janela de propriedades de revisão que se abre, clique em um dos seguintes botões:

     - **Comparar com a atual**

       Clique neste botão para comparar a revisão selecionada à atual.

     - **Comparar com a anterior**

       Clique neste botão para comparar a revisão selecionada à anterior.

   Um relatório no formato de HTML sobre a comparação de revisões é exibido no suo navegador padrão.

   Neste relatório, você pode minimizar algumas seções que contêm configurações de revisão. Para minimizar uma seção com as configurações de revisão de objeto, clique no ícone (▲) ao lado do nome da seção.

As revisões do Servidor de Administração incluem todos os detalhes das modificações feitas, exceto as detalhes das áreas seguintes:

- Seção **Tráfego**
- Seção **Regras de aplicação de tags**
- Seção **Notificação**

- Seção **Pontos de distribuição**
- Seção **Surto de vírus**

  Nenhuma informação é registrada, na seção **Surto de vírus**, sobre a configuração da ativação da política que ocorre quando um evento de Ataque de vírus é acionado.

É possível comparar as revisões de um objeto excluído com a revisão de um objeto existente, mas não o contrário: não é possível comparar as revisões de um objeto existente com a revisão de um objeto excluído.

Configurar o prazo de armazenamento das revisões de objeto e das informações de objeto excluídas

O prazo de armazenamento das revisões de objeto e das informações sobre objetos excluídos é igual. O prazo de armazenamento padrão é de 90 dias. Esse tempo é suficiente para a auditoria regular do programa.

Somente os usuários com a permissão **Modificar** na área **Objetos excluídos** pode alterar o período de armazenamento.

Para alterar o período de armazenamento das revisões de objeto e das informações sobre objetos excluídos:

1. Na árvore do console, selecione o Servidor de Administração para o qual você deseja modificar o período de armazenamento.
2. Clique com o botão direito e, no menu de contexto, selecione **Propriedades**.
3. Na janela de propriedades Servidor de Administração que se abre, na seção **Repositório de histórico de revisões**, insira o período de armazenamento desejado (o número de dias).
4. Clique em **OK**.

As revisões de objeto e as informações sobre objetos excluídos serão armazenadas pelo número de dias que você inseriu.

Exibir uma revisão de objeto

Se você precisar quais modificações foram feitas a um objeto ao longo de um determinado período de tempo, você pode exibir as revisões deste objeto.

Para exibir as revisões de um objeto:

1. Siga para a seção **Histórico de revisões** do objeto.
2. Na lista de revisões de objeto, selecione a revisão cujas configurações você deseja exibir.
3. Execute uma das seguintes ações:
   - Clique no botão **Exibir a revisão**.
   - Abra a janela Propriedades da revisão clicando duas vezes no nome da revisão e, a seguir, clique no botão **Exibir a revisão**.

Um relatório no formato de HTML com as configurações da revisão de objeto selecionada é exibido. Neste relatório, você pode minimizar algumas seções com as configurações de revisão de objeto. Para minimizar uma seção com as configurações de revisão de objeto, clique no ícone (▲) ao lado do nome da seção.

Salvar uma revisão do objeto em um arquivo

Você pode salvar uma revisão de objeto como um arquivo de texto, por exemplo, para enviá-lo por e-mail.

Para salvar uma revisão de objeto em um arquivo:

1. Siga para a seção **Histórico de revisões** do objeto.
2. Na lista de revisões de um objeto, selecione aquele cujas configurações você precisa salvar.
3. Clique no botão **Avançado** e selecione o valor **Salvar no arquivo** na lista suspensa.

A revisão é agora salva como um arquivo .txt.

Reverter modificações

Você poderá reverter as alterações feitas à um objeto, se necessário. Por exemplo, você poderá ter que reverter as configurações de uma política ao seu estado em uma data específica.

Para reverter as alterações feitas à um objeto:

1. Siga para a seção **Histórico de revisões** do objeto.
2. Na lista de revisões de objeto, selecione o número da revisão para a qual você precisa reverter as modificações.
3. Clique no botão **Avançado** e selecione o valor **Reverter** na lista suspensa.

O objeto é agora revertido à revisão selecionada. A lista de revisões de objeto exibe um registro da ação que foi executada. A descrição da revisão exibe as informações sobre o número da revisão à qual você reverteu o objeto.

Adicionar uma descrição da revisão

Você pode adicionar uma descrição da revisão para simplificar a procura por revisões na lista.

Para adicionar uma descrição para uma revisão:

1. Siga para a seção **Histórico de revisões** do objeto.
2. Na lista de revisões de objeto, selecione a revisão para a qual você precisa adicionar uma descrição.
3. Clique no botão **Descrição**.

4. Na janela **Descrição da revisão do objeto**, insira algum texto para a descrição da revisão.

   Por padrão, a descrição da revisão do objeto está em branco.

5. Clique em **OK**.

Exclusão de objetos

Esta seção fornece informações sobre como excluir objetos.

Você pode excluir objetos, como os seguintes:

- Políticas
- Tarefas
- Pacotes de instalação
- Servidores de Administração virtual
- Usuários
- Grupos de segurança
- Grupos de administração

Para excluir um objeto:

1. Abra a seção necessária do Kaspersky Security Center Web Console e selecione o objeto.
2. Na barra de ferramentas, clique no botão **Excluir**.
3. Na janela que se abre, clique em **OK** para confirmar a sua seleção.

O objeto selecionado será excluído.

Quando você exclui um objeto, as informações sobre ele permanecem no banco de dados. O período de armazenamento das informações sobre os objetos excluídos é igual ao período de armazenamento das revisões de objetos (o período recomendado é de 90 dias). Você pode alterar o prazo de armazenamento somente se tiver a permissão **Modificar** na área de direitos **Objetos excluídos**.

Sobre a exclusão de dispositivos clientes

Quando um dispositivo gerenciado é excluído de um grupo de administração, o aplicativo move o dispositivo para o grupo dispositivos não atribuídos. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados, o Agente de Rede e qualquer aplicativo de segurança, por exemplo, o Kaspersky Endpoint Security, permanecem no dispositivo.

O Kaspersky Security Center gerencia os dispositivos no grupo Dispositivos não atribuídos de acordo com as seguintes regras:

- Caso tenha configurado as regras de movimentação de dispositivo e um dispositivo atenda aos critérios de uma regra de movimentação, o dispositivo é automaticamente movido para um grupo de administração de acordo com a regra.

- O dispositivo é armazenado no grupo dispositivos não atribuídos e é automaticamente removido do grupo de acordo com as regras de retenção de dispositivos.

  As regras de retenção de dispositivo não afetam os dispositivos que têm uma ou mais unidades criptografadas com criptografia completa do disco. Esses dispositivos não são excluídos automaticamente. Somente é possível excluí-los manualmente. Caso necessite excluir um dispositivo com uma unidade criptografada, primeiro descriptografe a unidade e, em seguida, exclua o dispositivo.

  > Ao excluir um dispositivo com unidade criptografada, os dados necessários para descriptografar a unidade também são excluídos. Se você marcar a caixa de seleção **Eu entendo o risco e desejo excluir os dispositivos selecionados** na janela de confirmação que é aberta quando você exclui esses dispositivos (do grupo **Dispositivos não atribuídos** ou **Dispositivos gerenciados**), significa que você está ciente da exclusão de dados.

  Para descriptografar o dispositivo, as seguintes condições devem ser atendidas:

  - O dispositivo é reconectado ao Servidor de Administração para restaurar os dados necessários para descriptografar a unidade.

  - O usuário do dispositivo lembra a senha de descriptografia.

  - O aplicativo de segurança usado para criptografar o dispositivo, por exemplo, o Kaspersky Endpoint Security for Windows, ainda está instalado nele.

  Caso o dispositivo seja criptografado pela tecnologia Kaspersky Disk Encryption, também é possível tentar recuperar os dados usando o utilitário de restauração FDERT.

> Na VDI, se você tiver um equipamento com dispositivos criptografados, as informações no dispositivo criptografado serão excluídas após a exclusão do equipamento.

Quando um dispositivo é excluído manualmente do grupo dispositivos não atribuídos, o aplicativo remove o dispositivo da lista. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados (se houver) permanecem no dispositivo. Assim, caso o dispositivo ainda esteja visível para o Servidor de Administração e a sondagem de rede regular tenha sido configurada, o Kaspersky Security Center descobre o dispositivo durante a sondagem e o recoloca no grupo Dispositivos não atribuídos. Portanto, é razoável excluir um dispositivo manualmente somente se o dispositivo estiver invisível para o Servidor de Administração.

Excluir um objeto

É possível excluir objetos como políticas, tarefas, pacotes de instalação, usuários internos e grupos de segurança internos caso você tenha a permissão Modificar, que pertence à categoria de Funcionalidade básica de direitos (consulte o artigo Atribuir permissões a usuários e grupos para obter mais informações).

Não é possível excluir pacotes de instalação que são usados em tarefas de instalação remota. É necessário encerrar as tarefas correspondentes primeiro. Para obter mais informações sobre tarefas de instalação automática em um grupo de administração, consulte o artigo Instalação automática de aplicativos em dispositivos em um grupo de administração.

Para excluir um objeto:

1. Na árvore do console, no espaço de trabalho da pasta necessária, selecione um objeto.
2. Execute uma das seguintes ações:
   - Clique com o botão direito no objeto e selecione **Excluir**.
   - Pressione a tecla **DELETE**.

O objeto será excluído e as informações sobre ele serão armazenadas no banco de dados.

Exibir informações sobre objetos excluídos

As informações sobre objetos excluídos são armazenadas na pasta **Objetos excluídos** pelo mesmo período de tempo que as revisões dos objetos (o período recomendado é de 90 dias).

Apenas os usuários com a permissão **Ler** na área de direitos **Objetos excluídos** podem visualizar a lista de objetos excluídos (consulte Atribuir permissões a usuários e grupos para mais informações).

Para visualizar a lista de objetos excluídos,

Na árvore do console, selecione **Objetos excluídos** (por padrão, **Objetos excluídos** é uma subpasta da pasta **Avançado**).

Se você não tiver permissão Ler na área de direitos **Objetos excluídos**, uma lista vazia será exibida na pasta **Objetos excluídos**.

O espaço de trabalho da pasta **Objetos excluídos** contém as seguintes informações sobre objetos excluídos:

- **Nome**. O nome do objeto.
- **Tipo**. Tipo de objeto, como política, tarefa ou pacote de instalação.
- **Hora**. A hora em que o objeto foi excluído.
- **Usuário**. Nome da conta do usuário que excluiu o objeto.

Para visualizar mais informações sobre um objeto:

1. Na árvore do console, selecione **Objetos excluídos** (por padrão, **Objetos excluídos** é uma subpasta da pasta **Avançado**).
2. No espaço de trabalho **Objetos excluídos**, selecione o objeto desejado.

   A caixa para uso com o objeto selecionado é exibida no lado direito do espaço de trabalho.
3. Execute uma das seguintes ações:

   - Clique no link **Propriedades** na caixa.
   - Clique com o botão direito no objeto que você selecionou no espaço de trabalho e, no menu de contexto, selecione **Propriedades**.

   A janela de propriedades do objeto abre, exibindo as seguintes guias:

   - **Geral**
   - Histórico de revisões

Excluir objetos permanentemente da lista de objetos excluídos

Apenas os usuários com a permissão **Modificar** na área de direitos **Objetos excluídos** podem excluir objetos permanentemente da lista de objetos excluídos (consulte Atribuir permissões a usuários e grupos para mais informações).

Para excluir um objeto da lista de objetos excluídos:

1. Na árvore do console, selecione o nó do Servidor de Administração necessário e selecione a pasta **Objetos excluídos**.
2. No espaço de trabalho, selecione o(s) objeto(s) que você deseja excluir.
3. Execute uma das seguintes ações:

   - Pressione a tecla **DELETE**.
   - No menu de contexto do(s) objeto(s) que você selecionou, selecione **Excluir**.
4. Na caixa de diálogo de confirmação, clique em **Sim**.

   O objeto é excluído permanentemente da lista de objetos excluídos. Todas as informações sobre esse objeto (inclusive todas as suas revisões) são permanentemente removidas do banco de dados. Você não pode restaurar essas informações.

Gerenciamento de Dispositivos Móveis

O gerenciamento da proteção de dispositivos móveis através do Kaspersky Security Center é executado usando o recurso Gerenciamento de Dispositivos Móveis, o qual requer uma licença dedicada. Se você está pretendendo gerenciar dispositivos móveis de propriedade dos funcionários da sua organização, você deve ativar o Gerenciamento de Dispositivos Móveis.

Esta seção fornece instruções para ativar, configurar e desativar o Gerenciamento de Dispositivos Móveis. Esta seção também descreve como gerenciar dispositivos móveis conectados ao Servidor de Administração.

Para obter detalhes sobre o Kaspersky Security for Mobile, consulte a *Ajuda do Kaspersky Security for Mobile*.

Cenário: Implementação do Gerenciamento de Dispositivos Móveis

Esta seção fornece um cenário para configurar o recurso de Gerenciamento de dispositivos móveis no Kaspersky Security Center.

Pré-requisitos

Certifique-se de que você tenha uma licença que conceda acesso ao recurso Gerenciamento de Dispositivos Móveis.

Fases

A implementação do recurso de Gerenciamento de dispositivos móveis procede em estágios:

1. **Preparar as portas**

   Assegure-se de que a porta 13292 esteja disponível no Servidor de Administração. Essa porta é necessária para conexão aos dispositivos móveis. Também, você pode desejar tornar a porta 17100 disponível. Essa porta somente é necessária para o servidor proxy de ativação para dispositivos móveis gerenciados, e se eles têm acesso à Internet, você não precisa tornar esta porta disponível.

2. **Ativar o Gerenciamento de Dispositivos Móveis**

   Você poderá ativar o Gerenciamento de dispositivos móveis quando estiver executando o Assistente de início rápido do Servidor de Administração ou posterior.

3. **Especificar o endereço externo do Servidor de Administração**

   Você pode especificar o endereço externo quando executar o Assistente de início rápido do Servidor de Administração ou posterior. Se você não tiver selecionado o Gerenciamento de Dispositivos Móveis para instalação e não tiver especificado o endereço no Assistente de instalação, especifique o endereço externo nas propriedades do pacote de instalação.

4. **Adição de dispositivos móveis ao grupo Dispositivos gerenciados**

   Adicione os dispositivos móveis ao grupo Dispositivos gerenciados para que seja possível gerenciar esses dispositivos por meio de políticas. Você pode criar uma regra de migração em uma das etapas do Assistente de início rápido do Servidor de Administração. Você também pode criar a regra de movimentação depois. Se não criar tal regra, você poderá adicionar dispositivos móveis ao grupo Dispositivos gerenciados manualmente.

   Você pode adicionar dispositivos móveis ao grupo Dispositivos gerenciados diretamente ou criar um subgrupo (ou vários subgrupos) para eles.

   A qualquer momento posteriormente, você pode conectar qualquer novo dispositivo móvel ao Servidor de Administração usando o Assistente de conexão de novos dispositivos móveis.

5. **Criar uma política para dispositivos móveis**

   Para gerenciar dispositivos móveis, crie uma política (ou várias) para eles nos grupos aos quais os dispositivos pertencem. Você pode alterar as configurações dessa política a qualquer momento posteriormente.

Resultados

Após concluir este cenário, você poderá gerenciar dispositivos Android e iOS usando o Kaspersky Security Center. Você pode trabalhar com certificados de dispositivos móveis e enviar comandos para dispositivos móveis.

Sobre a política de grupo para gerenciar dispositivos EAS e MDM do iOS

Para gerenciar dispositivos MDM do iOS e EAS, você pode usar o plugin de gerenciamento do Kaspersky Device Management for iOS, que está incluído no kit de distribuição do Kaspersky Security Center. O Kaspersky Device Management for iOS permite que você crie políticas de grupo para especificar as definições de configuração de dispositivos MDM do iOS e EAS sem usar o iPhone® Configuration Utility e o perfil de gerenciamento do Exchange ActiveSync.

Uma política de grupo para gerenciamento de dispositivos MSM do MDM do iOS fornece ao administrador as seguintes opções:

- Para gerenciar dispositivos EAS:
  - Configurar a senha de desbloqueio do dispositivo.
  - Configurar o armazenamento de dados no dispositivo em formato criptografado.
  - Configurar a sincronização do correio corporativo.
  - Configurar as funções de hardware de dispositivos móveis, como o uso de multimídia removível, câmera ou Bluetooth.
  - Configurar restrições sobre o uso de aplicativos móveis no dispositivo.
- Para gerenciar dispositivos MDM do iOS:
  - Especificar as configurações de segurança da senha do dispositivo.
  - Configurar as restrições sobre o uso de recursos de hardware do dispositivo e restrições na instalação e remoção de aplicativos móveis.
  - Configurar restrições sobre o uso de aplicativos móveis pré-instalados, como o YouTube™, iTunes® Store ou Safari.
  - Configurar as restrições sobre conteúdo de mídia visualizado (como filmes e programas de TV) pela região onde o dispositivo está localizado.
  - Definir as configurações da conexão do dispositivo à Internet através do servidor proxy (proxy HTTP Global).
  - Configurar a conta com a qual o usuário pode acessar os aplicativos e serviços corporativos (tecnologia de autenticação única [SSO]).
  - Monitoramento do uso da Internet (visitas a sites) em dispositivos móveis.
  - Configurar as redes sem fios (Wi-Fi), os pontos de acesso (APN) e as redes privadas virtuais (VPN) que usam diferentes mecanismos de autenticação e protocolos de rede.
  - Especificar as configurações da conexão com dispositivos AirPlay® para transmissão de fotos, música e vídeos.
  - Especificar as configurações da conexão com impressoras AirPrint™ para impressão de documentos sem fios a partir do dispositivo.
  - Configurar a sincronização com o servidor Microsoft Exchange e contas do usuário para usar e-mails corporativos em dispositivos.
  - Configurar as credenciais do usuário para a sincronização com o serviço de diretório LDAP.
  - Configurar as credenciais do usuário para conexão com serviços CalDAV e CardDAV que fornecem aos usuários o acesso aos calendários e listas de contatos corporativos.
  - Definir as configurações da interface iOS, tal como fontes ou ícones de sites favoritos no dispositivo do usuário.

- Adicionar novos certificados de segurança em dispositivos.
- Configurar o servidor SCEP (Simple Certificate Enrollment Protocol) para recuperação automática de certificados por dispositivo a partir da Autoridade de Certificação.
- Adicionar configurações personalizadas para operação de aplicativos móveis.

Uma política para gerenciar dispositivos EAS e MDM do iOS é especial, na medida em que é atribuída a um grupo de administração que inclui o Servidor de MDM do iOS e o Servidor de dispositivos móveis Exchange ActiveSync (doravante referidos coletivamente como "Servidores de dispositivos móveis"). Todas as configurações especificadas nesta política são primeiramente aplicadas a Servidores de dispositivos móveis e, em seguida, a dispositivos móveis gerenciados por esses servidores. No caso de uma estrutura hierárquica de grupos de administração, os Servidores de dispositivos móveis secundários recebem as configurações de política dos Servidores de dispositivos móveis principal e as distribuem para dispositivos móveis.

Para mais detalhes sobre como usar a política de grupo para gerenciar dispositivos EAS e MDM do iOS no Console de Administração do Kaspersky Security Center, consulte a documentação do *Kaspersky Security for Mobile*.

Ativar o Gerenciamento de Dispositivos Móveis

Para gerenciar dispositivos móveis, você deve ativar o Gerenciamento de Dispositivos Móveis. Se você não ativou esse recurso no Assistente de início rápido, você pode ativá-lo mais tarde. O Gerenciamento de Dispositivos Móveis requer uma licença.

Ativar o Gerenciamento de Dispositivos Móveis somente está disponível no Servidor de Administração principal.

Para exibir o Gerenciamento de Dispositivos Móveis:

1. Na árvore do console, selecione a pasta **Gerenciamento de Dispositivos Móveis**.
2. No espaço de trabalho da pasta, clique no botão **Ativar o Gerenciamento de Dispositivos Móveis**. Este botão somente estará disponível se você não tiver ativado o **Gerenciamento de Dispositivos Móveis** antes.

   A página **Componentes adicionais** do Assistente de início rápido do Servidor de Administração é exibida.
3. Selecione **Ativar o Gerenciamento de Dispositivos Móveis** para poder gerenciar dispositivos móveis.
4. Na página **Selecione o método de ativação do aplicativo**, ative o aplicativo usando um arquivo de chave ou um código de ativação.

   O gerenciamento de dispositivos móveis estará impossível a menos que você ative o recurso de Gerenciamento de Dispositivos Móveis.
5. Na página **Configurações do servidor proxy para acessar a Internet**, selecione a caixa de seleção **Usar o servidor proxy** se você quiser usar um servidor proxy ao se conectar à Internet. Quando essa caixa de seleção estiver marcada, os campos se tornam disponíveis para inserir configurações. Especifique as configurações para a conexão ao servidor proxy.

6. Na página **Verificar se há atualizações para plug-ins e pacotes de instalação**, selecione uma das seguintes opções:

   - **Verificar se os plug-ins e os pacotes de instalação estão atualizados**

     Iniciar a verificação do status atualizado. Se a verificação detectar versões desatualizadas de alguns plugins ou pacotes de instalação, o assistente solicita-o a baixar versões atualizadas para substituir as desatualizadas.

   - **Ignorar a verificação**

     Continue a trabalhar sem verificar se os plugins e os pacotes de instalação estão atualizados. Você pode selecionar esta opção se, por exemplo, não tiver acesso à Internet ou se quiser prosseguir com a versão desatualizada do aplicativo por algum motivo.

     Ignorar a verificação de atualizações para plugins pode resultar no funcionamento impróprio do aplicativo.

7. Na página **Versões mais recentes do plug-in disponíveis**, baixe e instale as versões mais recentes dos plugins no idioma que a versão de seu aplicativo requer. A atualização dos plugins não requer uma licença.

   Após você ter instalado os plugins e os pacotes, o aplicativo verifica se todos os plugins necessários para o funcionamento apropriado dos dispositivos móveis foram instalados. Se forem detectadas versões desatualizadas de alguns plugins, o assistente solicita que você baixe versões atualizadas para substituir as desatualizadas.

8. Na página **Configurações de conexão do dispositivo móvel**, configure as portas do Servidor de Administração.

Quando o assistente for concluído, as seguintes alterações serão feitas:

- A política do Kaspersky Endpoint Security for Android será criada.
- A política do Kaspersky Device Management for iOS será criada.
- As portas estarão abertas no Servidor de Administração para os dispositivos móveis.

Modificar as configurações de Gerenciamento de Dispositivos Móveis

Para ativar o suporte de dispositivos móveis:

1. Na árvore do console, selecione a pasta **Gerenciamento de Dispositivos Móveis**.
2. No espaço de trabalho da pasta, clique no link **Portas para a conexão de dispositivos móveis**.

   A seção **Portas adicionais** da janela Propriedades do Servidor de Administração é exibida.

3. Na seção **Portas adicionais**, modifique as configurações relevantes:

   - **Porta SSL para servidor proxy de ativação**
   - **Open port for mobile devices**

     Uma porta é aberta para os dispositivos móveis conectarem-se ao Servidor de Licenciamento. Você pode definir o número da porta e outras configurações nos campos abaixo.

     Por padrão, esta opção está ativada.

   - **Port for mobile device synchronization**

     O número da porta através da qual os dispositivos móveis conectam-se ao Servidor de Administração e trocam dados com o mesmo. O número da porta padrão é 13292.

     Você pode atribuir uma porta diferente se a porta 13292 estiver sendo usada para outros propósitos.

   - **Porta para ativação de dispositivos móveis**

     A porta para conexão do Kaspersky Endpoint Security for Android para os servidores de ativação da Kaspersky.

     O número da porta padrão é 17100.

4. Clique em **OK**.

Desativar o Gerenciamento de Dispositivos Móveis

Desativar o Gerenciamento de Dispositivos Móveis somente está disponível no Servidor de Administração principal.

Para desativar o Gerenciamento de Dispositivos Móveis:

1. Na árvore do console, selecione a pasta **Gerenciamento de Dispositivos Móveis**.
2. No espaço de trabalho da pasta, clique no link **Configurar componentes adicionais**.

   A página **Componentes adicionais** do Assistente de início rápido do Servidor de Administração é exibida.
3. Selecione **Não ativar Gerenciamento de Dispositivos Móveis** se você não quiser mais gerenciar dispositivos móveis.
4. Clique em **OK**.

Os dispositivos móveis anteriormente conectados não serão capazes de conectar-se ao Servidor de Administração. A porta para a conexão de dispositivo móvel e a porta para a ativação de dispositivo móvel serão fechadas automaticamente.

A políticas que foram criada para o Kaspersky Endpoint Security for Android e para o Kaspersky Device Management for iOS não serão excluídas. As regras de emissão de certificado não serão modificadas. Os plugins que foram instalados não serão removidos. A regra para migrar dispositivos móveis não será excluída.

Após você tiver reativado o Gerenciamento de Dispositivos Móveis nos dispositivos móveis gerenciados, talvez terá que reinstalar os aplicativos móveis que são necessários para o gerenciamento de dispositivos móveis.

Trabalhar com comandos para dispositivos móveis

Esta seção contém informações sobre os comandos para o gerenciamento de dispositivos móveis compatíveis com o Kaspersky Security Center. A seção fornece instruções sobre como enviar comandos para dispositivos móveis, assim como visualizar o status de execução de comandos no log de comandos.

Comandos para gerenciamento de dispositivos móveis

O Kaspersky Security Center é compatível com comandos para o gerenciamento de dispositivos móveis.

Tais comandos são usados para o gerenciamento remoto do dispositivo móvel. Por exemplo, se dispositivo móvel seja perdido, você pode excluir todos os dados corporativos do dispositivo usando um comando.

Você pode usar comandos para os seguintes tipos de dispositivos móveis gerenciados:

- Dispositivos MDM do iOS
- Dispositivos Kaspersky Endpoint Security (KES)
- Dispositivos EAS

Cada tipo de dispositivo é compatível com um conjunto dedicado de comandos.

Considerações especiais para determinados comandos

- Para todos os tipos de dispositivos, se o comando **Redefinir as configurações padrão** for executado com êxito, todos os dados serão excluídos do dispositivo e as configurações do dispositivo serão revertidas para seus valores de fábrica.
- Após a execução bem sucedida do comando **Limpar os dados corporativos** em um dispositivo MDM do iOS, todos os perfis de configuração instalados, perfis de provisionamento, o perfil de MDM do iOS e os aplicativos para os quais a caixa de seleção **Remover junto com o perfil de MDM do iOS** estiver selecionada, serão removidos do dispositivo.

- Se o comando **Limpar os dados corporativos** for executado com êxito em um dispositivo KES, todos os dados corporativos, entradas nos Contatos, o histórico de SMS, o registro de chamadas, o calendário, as configurações de conexão com a Internet e as contas do usuário, exceto a conta Google™, serão excluídos do dispositivo. Para um dispositivo KES, todos os dados do cartão de memória também serão excluídos.

- Antes de enviar o comando **Localizar** para um dispositivo KES, você terá de confirmar que está usando este comando para uma procura autorizada de um dispositivo perdido que pertence à sua organização ou a um dos seus funcionários. Um dispositivo móvel que recebe o comando **Localizar** não está bloqueado.

Lista de comandos para dispositivos móveis

A tabela a seguir exibe conjuntos de comandos para cada dispositivo MDM do iOS.

Comandos compatíveis para gerenciamento de dispositivos móveis: dispositivos MDM do iOS

Comandos	Resultado da execução de comandos
Bloquear	O dispositivo móvel é bloqueado.
Desbloquear	O bloqueio de dispositivo móvel com um PIN está desativado. O PIN especificado anteriormente foi redefinido.
Redefinir as configurações padrão	Todos os dados são excluídos do dispositivo móvel e as configurações são revertidas aos seus valores padrão.
Limpar os dados corporativos	Todos os perfis de configuração instalados, perfis de provisionamento, o perfil de MDM do iOS e os aplicativos para os quais a caixa de seleção **Remover junto com o perfil de MDM do iOS** estiver selecionada, serão removidos do dispositivo.
Sincronizar o dispositivo	Os dados dos dispositivo móvel são sincronizados com o Servidor de Administração.
Instalar o perfil	O perfil de configuração é instalado no dispositivo móvel.
Remover o perfil	O perfil de configuração é excluído do dispositivo móvel.
Instalar o perfil de provisionamento	O perfil de provisionamento é instalado no dispositivo móvel.
Remover o perfil de provisionamento	O perfil de provisionamento é excluído do dispositivo móvel.
Instalar o aplicativo	O aplicativo é instalado no dispositivo móvel.
Remover o aplicativo	O aplicativo é removido do dispositivo móvel.
Insira o código de resgate	Código de resgate inserido para um aplicativo pago.
Configurar o roaming	Roaming de dados e voz ativado ou desativado.

A tabela a seguir exibe conjuntos de comandos para dispositivos KES.

Comandos compatíveis com o gerenciamento de dispositivos móveis: dispositivos KES

Comando	Resultado da execução de comandos
Bloquear	O dispositivo móvel é bloqueado.
Desbloquear	O bloqueio de dispositivo móvel com um PIN está desativado. O PIN especificado anteriormente foi redefinido.
Redefinir as configurações padrão	Todos os dados são excluídos do dispositivo móvel e as configurações são revertidas aos seus valores padrão.
Limpar os dados corporativos	Dados corporativos, entradas em Contatos, o histórico de SMS, o registro de chamadas, o calendário, as configurações de conexão com a Internet, as contas do usuário (exceto a conta Google) foram excluídos. Os dados do cartão de memória foram limpos.
Sincronizar o dispositivo	Os dados dos dispositivo móvel são sincronizados com o Servidor de Administração.
Localizar dispositivo	O dispositivo é localizado e exibido no Google Maps™. A operadora móvel cobra uma taxa para enviar a mensagem SMS e para fornecer a conexão à Internet.

Retrato	O dispositivo móvel é bloqueado. A foto foi tirada pela câmara frontal do dispositivo e salva no Servidor de Administração. As fotos podem ser visualizadas no registro de comandos. A operadora móvel cobra uma taxa para enviar a mensagem SMS e para fornecer a conexão à Internet.
Alarme	O dispositivo móvel soa um alarme.

A tabela a seguir exibe os comandos para dispositivos EAS.

Comandos compatíveis com o gerenciamento de dispositivos móveis: dispositivos EAS

Comandos	Resultado da execução de comandos
Redefinir as configurações padrão	Todos os dados são excluídos do dispositivo móvel e as configurações são revertidas aos seus valores padrão.

Usar o Firebase Cloud Messaging

Para assegurar a entrega em tempo dos comandos para dispositivos KES gerenciados pela sistema operacional Android, o Kaspersky Security Center usa o mecanismo de notificações push. As notificações push são trocadas entre os dispositivos KES e o Servidor de Administração por meio do Firebase Cloud Messaging (aqui referido como FCM). No Console de Administração do Kaspersky Security Center, é possível especificar as configurações do Firebase Cloud Messaging para conectar dispositivos KES ao serviço.

Para recuperar as configurações do Firebase Cloud Messaging, é necessário ter uma conta do Google.

Para ativar o uso do FCM:

1. No console de administração, selecione o nó **Gerenciamento de Dispositivos Móveis** e a pasta **Dispositivos móveis**.
2. No menu de contexto da pasta **Dispositivos móveis**, selecione **Propriedades**.
3. Nas propriedades da pasta, selecione a seção **Configurações do Google Firebase Cloud Messaging**.
4. No campo **ID do Remetente**, especifique o ID do remetente do FCM.
5. No campo **Arquivo de chave privada (em formato JSON)**, selecione o arquivo de chave privada.

   Na próxima sincronização com o Servidor de Administração, os dispositivos KES gerenciados por sistemas operacionais Android serão conectados ao Firebase Cloud Messaging.

É possível editar as configurações do Firebase Cloud Messaging clicando no botão **Redefinir as configurações**.

Enviar comandos

Para enviar um comando para o dispositivo móvel do usuário:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.
2. Selecione o dispositivo móvel do usuário para o qual você deseja enviar um comando.
3. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

4. Na janela **Comandos de gerenciamento de dispositivos móveis**, siga para a seção com o nome do comando que você precisar enviar para o dispositivo móvel e, a seguir, clique no botão **Enviar comando**.

   Dependendo do comando que você selecionou, clicar no botão **Enviar comando** poderá abrir a janela de configurações avançadas do aplicativo. Por exemplo, quando você enviar o comando para excluir um perfil de provisionamento de um dispositivo, o aplicativo solicita-lhe que selecione o perfil de provisionamento que deve ser excluído do dispositivo móvel. Especifique as configurações avançadas do comando nessa janela e confirme sua seleção. Posteriormente, o comando será enviado para o dispositivo móvel.

   Você pode clicar no botão **Reenviar** para enviar novamente o comando para o dispositivo móvel do usuário.

   Você pode clicar no botão **Remover da fila** para cancelar a execução de um comando que foi enviado, se o comando ainda não tenha sido executado.

   A seção **Log de comandos** exibe comandos que foram enviados para o dispositivo móvel, com os respetivos status de execução. Clique em **Atualizar** para atualizar a lista de comandos.

5. Clique em **OK** para fechar a janela **Comandos de gerenciamento de dispositivos móveis**.

Visualização do status de comandos no registro de comandos

O aplicativo salva no registro de comandos as informações sobre todos os comandos que foram enviados para dispositivos móveis. O registro de comandos contém informações sobre a hora e data em que cada comando foi enviado para o dispositivo móvel, seu status e descrições detalhadas dos resultados da execução do comando. Por exemplo, caso um comando não seja executado com êxito, o registro exibe a causa do erro. Os registros são armazenados no registro de comandos durante, no máximo, 30 dias.

Os comandos enviados para dispositivos móveis podem ter os seguintes status:

- *Em execução* – O comando foi enviado para o dispositivo móvel.
- *Concluído* – A execução do comando foi concluída com êxito.
- *Concluído com erro* – A execução do comando falhou.
- *Excluindo* – O comando está sendo removido da fila de comandos enviados para o dispositivo móvel.
- *Excluído* – O comando foi removido com êxito da fila de comandos enviados para o dispositivo móvel.
- *Erro ao excluir* – O comando não pôde ser removido da fila de comandos enviados para o dispositivo móvel.

O aplicativo mantém um registro de comandos para cada dispositivo móvel.

Para visualizar o registro de comandos enviados para um dispositivo móvel:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. Na lista de dispositivos móveis, selecione o dispositivo para o qual você deseja visualizar o registro de comandos.

3. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

   A janela **Comandos de gerenciamento de dispositivos móveis** será aberta. As seções da janela **Comandos de gerenciamento de dispositivos móveis** corresponde aos comandos que podem ser enviados para o dispositivo móvel.

4. Selecione as seções que contêm os comandos necessários e visualize as informações sobre como os comandos são enviados e executados na seção **Log de comandos**.

Na seção **Log de comandos**, você pode visualizar a lista de comandos que foram enviados para o dispositivo móvel e detalhes sobre esses comandos. O filtro **Mostrar comandos** permite que você exiba na lista somente os comandos com o status selecionado.

Trabalhar com certificados de dispositivos móveis

Essa seção contém informações sobre como trabalhar com certificados de dispositivos móveis.

O certificado raiz para dispositivos móveis tem um prazo de expiração fixo de 700 dias após sua geração. O certificado de reserva é gerado 60 dias antes da data de expiração. É possível modificar o período de geração de um certificado de reserva com o seguinte comando:

`klscflag.exe -fset -pv klserver -n KLSRV_AKLWNGT_MDM_CERT_CHANGE_TIMEOUT -t d -v <tempo limite em segundos>`

O período de geração de um certificado de reserva deve ser longo o suficiente para que todos os dispositivos móveis gerenciados sincronizem com o Servidor de Administração e recuperem o certificado.

O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Não há suporte para a renovação manual do certificado raiz para dispositivos móveis.

Iniciar o Assistente de instalação de certificados

Você pode instalar os seguintes tipos de certificados no dispositivo móvel de um usuário:

- Certificados compartilhados para identificar o dispositivo móvel
- Certificados de correio para configurar o correio corporativo no dispositivo móvel
- Certificado da VPN para configurar o acesso a uma rede privada virtual no dispositivo móvel

Para instalar um certificado no dispositivo móvel de um usuário:

1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis** e selecione a subpasta **Certificados**.

2. No espaço de trabalho da pasta **Certificados**, clique no link **Adicionar certificado** para executar o Assistente de instalação de certificados.

Siga as instruções do Assistente.

Após o assistente concluir suas atividades, um certificado será criado e adicionado à lista de certificados do usuário; além disso, uma notificação será enviada ao usuário, fornecendo-lhe um link para baixar e instalar o certificado no dispositivo móvel. Você pode exibir a lista de todos os certificados e exportá-la para um arquivo. Você pode excluir e reemitir certificados, assim como visualizar suas propriedades.

Etapa 1. Selecionando o tipo de certificado

Especifique o tipo do certificado que deve ser instalado no dispositivo móvel do usuário:

- **Certificado de dispositivos móveis** – para identificar o dispositivo móvel
- **Certificado de e-mail** – para configurar o correio corporativo no dispositivo móvel
- **Certificado VPN** – para configurar o acesso a uma rede privada virtual no dispositivo móvel

Etapa 2. Selecionando o tipo de dispositivo

Esta janela somente será exibida se você selecionou **Certificado de e-mail** ou **Certificado VPN** como o tipo de certificado.

Especifique o tipo do sistema operacional no dispositivo:

- **Dispositivo MDM do iOS**. Selecione esta opção se você tiver que instalar um certificado em um dispositivo móvel que está conectado ao servidor MDM do iOS usando o protocolo MDM do iOS.
- **Dispositivo KES gerenciado pelo Kaspersky Security for Mobile**. Selecione esta opção se você tiver que instalar um certificado em um dispositivo KES. Neste caso, o certificado será usado para a identificação de usuário em cada conexão ao Servidor de Administração.
- **Dispositivo KES conectado ao Servidor de Administração sem a autenticação do certificado do usuário**. Selecione esta opção se você tiver que instalar um certificado em um dispositivo KES usando nenhuma autenticação de certificado. Neste caso, na etapa final do assistente, na janela **Método de notificação ao usuário** o administrador deve selecionar o tipo de autenticação do usuário usado em cada conexão ao Servidor de Administração.

Etapa 3. Seleção de um usuário

Na lista, selecione usuários, grupos de segurança ou grupos de segurança do Active Directory para os quais é necessário instalar o certificado.

Na janela **Seleção de usuários**, você pode pesquisar por usuários internos do Kaspersky Security Center. Você pode clicar em **Adicionar** para adicionar um usuário interno.

Etapa 4. Selecionando a origem do certificado

Nesta janela, você poderá selecionar a fonte do certificado que o Servidor de Administração usará para identificar o dispositivo móvel. Você poderá especificar um certificado usando um dos seguintes métodos:

- Crie um certificado automaticamente, por meio das ferramentas do Servidor de Administração, e então entregue o certificado ao dispositivo.
- Especifique um arquivo de certificado que foi criado antes. Este método não está disponível se múltiplos usuários foram selecionados na etapa anterior.

Selecione a caixa de seleção **Publicar certificado** se você tiver de enviar a um usuário uma notificação sobre a criação de um certificado para o dispositivo móvel dele.

Se o dispositivo móvel do usuário já tiver sido anteriormente autenticado usando um certificado, então não há necessidade de especificar um nome da conta e senha para receber um novo certificado, desmarque a caixa de seleção **Publicar certificado**. Neste caso, a janela **Método de notificação ao usuário** não será exibida.

Etapa 5. Atribuindo uma tag ao certificado

A janela **Tag do certificado** é exibida se **Dispositivo MDM do iOS** foi selecionado na **Tipo de dispositivo**.

Na lista suspensa, você pode atribuir uma tag ao certificado do dispositivo MDM do iOS do usuário. O certificado com a tag atribuída pode ter parâmetros específicos definidos para esta tag nas propriedades da política do Kaspersky Device Management for iOS.

A lista suspensa solicita selecionar a tag *Modelo 1 de certificado*, *Modelo 2 de certificado* ou *Modelo 3 de certificado*. Você pode configurar as tags nas seguintes seções:

- Se **Certificado de e-mail** foi selecionado na janela **Tipo de certificado**, os tags para o mesmo podem ser configurados na conta do Exchange ActiveSync para dispositivos móveis (**Dispositivos gerenciados** → **Políticas** → Propriedades política do Kaspersky Device Management for iOS > **Exchange ActiveSync** seção → **Adicionar** → **Avançado**).
- Se **Certificado VPN** foi selecionado na janela **Tipo de certificado**, os tags para o mesmo podem ser configurados nas propriedades da VPN para dispositivos móveis (**Dispositivos gerenciados** → **Políticas** → Propriedades da política do Kaspersky Device Management for iOS > Exchange ActiveSync **VPN** seção → **Adicionar** → **Avançado**). Você não pode configurar as tags usadas para certificados VPN se o tipo de conexão L2TP, PPTP ou IPSec (Cisco™) estiver selecionado para sua VPN.

Etapa 6. Especificando as configurações de publicação de certificado

Nesta janela, você pode alterar as seguintes configurações de publicação de certificado:

- **Não notificar o usuário sobre um novo certificado**

  Ative esta opção se você não quiser enviar uma notificação sobre a criação de um certificado para o dispositivo móvel do usuário. Neste caso, a janela **Método de notificação ao usuário** não será exibida.

  Esta opção é aplicável somente aos dispositivos com o Kaspersky Endpoint Security for Android instalado.

  Você pode ativar esta opção, por exemplo, se o dispositivo móvel do usuário já tiver sido autenticado anteriormente por meio de um certificado; portanto, não há necessidade de especificar um nome de conta e senha para receber um novo certificado.

- **Permitir que o dispositivo tenha vários recibos de um único certificado (somente para dispositivos com Kaspersky Endpoint Security for Android instalado)**

  Ative esta opção se você quiser que o Kaspersky Security Center reenvie automaticamente o certificado sempre que ele estiver prestes a expirar ou quando não for encontrado no dispositivo de destino.

  O certificado é reenviado automaticamente vários dias antes da data de expiração. Você pode definir o número de dias na janela Regras de emissão do certificado.

  Em alguns casos, o certificado não é encontrado no dispositivo. Por exemplo, isso pode acontecer quando o usuário reinstala o aplicativo de segurança da Kaspersky no dispositivo ou redefine as configurações e os dados de dispositivo aos padrões de fábrica. Nessa caso, o Kaspersky Security Center verifica o ID do dispositivo na próxima tentativa de conexão do dispositivo ao Servidor de Administração. Se o dispositivo tiver o mesmo ID criado no momento em que o certificado foi emitido, o aplicativo reenviará o certificado ao dispositivo.

Etapa 7. Selecionando um método de notificação ao usuário

Esta janela não será exibida se você selecionou **Dispositivo MDM do iOS** como o tipo de dispositivo ou se você selecionou a opção **Não notificar o usuário sobre um novo certificado**.

Na janela **Método de notificação ao usuário**, você pode especificar a notificação ao usuário sobre a instalação do certificado no dispositivo móvel.

No campo **Método de autenticação**, especifique o tipo de autenticação do usuário:

- **Credenciais (domínio ou codinome)**

  Neste caso, o usuário emprega a senha do domínio ou a senha de um usuário interno do Kaspersky Security Center para receber um novo certificado.

- **Senha de uso único**

  Neste caso, o usuário recebe uma senha para uma só utilização que será enviada por e-mail ou SMS. Esta senha deve ser inserida para receber um novo certificado.

  Esta opção é alterada para **Senha** se você ativou (selecionou) a opção **Permitir ao dispositivo múltiplos recibos de um único certificado (somente para dispositivos com aplicativos de segurança da Kaspersky para dispositivos móveis instalados)**, na janela **Configurações de publicação de certificado**.

- **Senha**

  Neste caso, a senha é usada sempre que o certificado é enviado ao usuário.

  Esta opção é alterada para **Senha de uso único** se você desativou (desmarcou) a opção **Permitir ao dispositivo múltiplos recibos de um único certificado (somente para dispositivos com aplicativos de segurança da Kaspersky para dispositivos móveis instalados)**, na janela **Configurações de publicação de certificado**.

Este campo é exibido se você selecionou **Certificado de dispositivos móveis** na janela **Tipo de certificado** ou se selecionou **Dispositivo KES conectado ao Servidor de Administração sem a autenticação do certificado do usuário** como o tipo de dispositivo.

Selecione a opção de notificação ao usuário:

- **Mostrar a senha de autenticação após a conclusão do assistente**

  Se você selecionar esta opção, o nome do usuário, o nome do usuário no Security Account Manager (SAM), e a senha para recuperação do certificado de todos os usuários selecionados serão exibidos na etapa final do Assistente de instalação de certificados. A configuração da notificação ao usuário sobre um certificado instalado estará indisponível.

  Quando você adiciona certificados para múltiplos usuários, você pode salvar em um arquivo as credenciais fornecidas clicando no botão **Exportar**, na última etapa do Assistente de instalação de certificados.

  Esta opção está indisponível se você selecionou **Credenciais (domínio ou codinome)** na etapa **Método de notificação ao usuário** do Assistente de instalação de certificados.

- **Notificar usuário sobre novo certificado**

  Se você selecionar esta opção, poderá configurar a notificação ao usuário sobre um novo certificado.

  - **Por e-mail**

    Nesse grupo de configurações, você pode configurar a notificação ao usuário sobre a instalação de um novo certificado em seu dispositivo móvel usando mensagens de e-mail. Este método de notificação somente está disponível se o Servidor de SMTP estiver ativado.

    Clique no link **Editar mensagem** para exibir e editar a mensagem de notificação, se necessário.

  - **Por SMS**

    Neste grupo de configurações, você pode configurar a notificação ao usuário sobre como usar SMS para instalar um certificado em dispositivos móveis. Este método de notificação somente está disponível se notificação por SMS estiver ativada.

    Clique no link **Editar mensagem** para exibir e editar a mensagem de notificação, se necessário.

Etapa 8. Geração do certificado

Nesta etapa, o certificado é criado.

Você pode clicar em **Concluir** para sair do Assistente.

O certificado é gerado e exibido na lista de certificados no espaço de trabalho da pasta **Certificados**.

Configurar as regras de emissão do certificado

Os certificados são usados para autenticação do dispositivo no Servidor de Administração. Todos os dispositivos móveis gerenciados devem ter certificados. Você pode configurar a forma como os certificados são emitidos.

Para configurar as regras de emissão de certificado:

1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis** e selecione a subpasta **Certificados**.

2. No espaço de trabalho da pasta **Certificados**, clique no botão **Configurar as regras de emissão de certificados** para abrir a janela **Regras de emissão do certificado**.

3. Avance para a seção com o nome de um tipo de certificado:

   Emissão de certificados móveis – Para configurar a emissão de certificados para os dispositivos móveis.

   Emissão de certificados de correio – Para configurar a emissão de certificados de correio.

   Emissão de certificados VPN – Para configurar a emissão de certificados VPN.

4. Na seção **Configurações de emissão**, configure a emissão do certificado:

   - Especifique o termo de certificado em dias.

     Os certificados para dispositivos móveis são limitados pela data de expiração do certificado raiz. Caso o período do certificado seja mais longo do que a data de expiração do certificado raiz, o período do certificado será ajustado automaticamente na geração.

   - Selecione uma fonte de certificado (**Servidor de Administração** ou **Os certificados são especificados manualmente**).

     O Servidor de Administração é selecionado como a fonte padrão de certificados.

   - Especifique um modelo de certificado (**Modelo padrão**, **Outros modelos**).

     A configuração de modelos está disponível se a seção **Integração com PKI** tiver a integração com a infraestrutura de chaves públicas ativada.

5. Na seção **Configurações das Atualizações Automáticas**, configure as atualizações automáticas do certificado:

   - No campo **Renovar quando o certificado estiver prestes a expirar em (dias)**, especifique quantos dias antes da expiração o certificado deve ser renovado.

   - Para ativar atualizações automáticas de certificados, selecione a caixa de seleção **Reemitir o certificado automaticamente se possível**.

6. Na seção **Proteção por senha**, ative e configure o uso de uma senha ao descriptografar certificados.

   > A Proteção por senha está disponível somente para certificados de tipo móvel.

   a. Marque a caixa de seleção **Solicitar a senha durante a instalação do certificado**.

   b. Use o botão deslizante para definir o número máximo de símbolos na senha para criptografia.

7. Clique em **OK**.

Integração com a infraestrutura de chaves públicas

A integração do aplicativo com a infraestrutura de chaves públicas (PKI) é necessária para simplificar a emissão de certificados de domínio para os usuários. Após a integração, os certificados são emitidos automaticamente.

A versão mínima do servidor PKI suportada é o Windows Server 2008.

Você deve configurar a conta para integração com a PKI. A conta deve cumprir os seguintes requisitos:

- Ser um usuário de domínio e administrador em um dispositivo com o Servidor de Administração instalado.
- Ser concedido o privilégio SeServiceLogonRight no dispositivo com o Servidor de Administração instalado.

Para criar um perfil de usuário permanente, faça login pelo menos uma vez com a conta de usuário configurada no de dispositivo com o Servidor de Administração instalado. Nesse repositório de certificados do usuário no dispositivo do Servidor de Administração, instale o certificado do Agente de Inscrição fornecido por administradores de domínio.

Para configurar a integração com a infraestrutura de chaves públicas:

1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis** e selecione a subpasta **Certificados**.
2. No espaço de trabalho, clique no botão **Integrar com infraestrutura de chave pública** para abrir a seção **Integração com PKI** da janela **Regras de emissão do certificado**.

   A seção **Integração com PKI** da janela **Regras de emissão do certificado** é aberta.
3. Marque a caixa de seleção **Integrar a emissão certificados com PKI**.
4. No campo **Conta**, especifique o nome da conta de usuário a usar para integração com a infraestrutura de chaves públicas.
5. No campo **Senha**, insira a senha do domínio para a conta.
6. Na lista **Nome do modelo de certificado no sistema PKI**, selecione o modelo de certificado que será usado para a emissão de certificados para os usuários de domínio.

   Um serviço dedicado é executado no Kaspersky Security Center sob a conta especificada. Este serviço é responsável por emitir certificados de domínio de usuários. O serviço é executado quando a lista de modelos de certificado for carregada clicando no botão **Atualizar a lista** ou quando um certificado for gerado.
7. Clique em **OK** para salvar as configurações.

Após a integração, os certificados são emitidos automaticamente.

Ativar o suporte de Kerberos Constrained Delegation

O aplicativo suporta o uso de Kerberos Constrained Delegation.

Para ativar o suporte de Kerberos Constrained Delegation:

1. Na árvore do console, abra a pasta **Gerenciamento de Dispositivos Móveis**.
2. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Servidores de dispositivos móveis**.
3. No espaço de trabalho da pasta **Servidores de dispositivos móveis**, selecione um Servidor de MDM do iOS.
4. No menu de contexto do servidor MDM do iOS, selecione **Propriedades**.
5. Na janela de propriedades do Servidor de MDM do iOS, selecione a seção **Configurações**.
6. Na seção **Configurações**, selecione a caixa de seleção **Assegurar compatibilidade com a delegação restrita de Kerberos**.
7. Clique em **OK**.

Adicionando dispositivos móveis iOS na lista de dispositivos gerenciados

Para adicionar um dispositivo móvel iOS de um usuário na lista de dispositivos gerenciados, um certificado compartilhado deve ser entregue e instalado no dispositivo. Os certificados compartilhados são usados pelo Servidor de Administração para identificar os dispositivos móveis. Um certificado compartilhado para um dispositivo móvel iOS é fornecido em um perfil de MDM do iOS. Após um certificado compartilhado ter sido fornecido e instalado em um dispositivo móvel, o dispositivo é exibido na lista de dispositivos gerenciados.

A Kaspersky não dá mais suporte ao Kaspersky Safe Browser.

Você pode adicionar dispositivos móveis de usuários à lista de dispositivos gerenciados por meio do Assistente de conexão de novos dispositivos móveis.

Para conectar um dispositivo iOS ao Servidor de Administração usando um certificado compartilhado:

1. Inicie o Assistente de conexão de novos dispositivos móveis de uma das seguintes maneiras:

   - Use o menu contextual na pasta **Contas de usuário**:

     1. Na árvore do console, expanda a pasta **Avançado** e selecione a subpasta **Contas de usuário**.

     2. No espaço de trabalho da pasta **Contas de usuário**, selecione os usuários, grupos de segurança ou grupos de segurança do Active Directory para os quais deseja adicionar na lista de dispositivos gerenciados.

     3. Clique com o botão direito no menu contextual da conta do usuário, selecione **Adicionar dispositivo móvel**.

        O Assistente de conexão de novos dispositivos móveis é iniciado.

   - No espaço de trabalho da pasta **Dispositivos móveis**, clique no botão **Adicionar dispositivo móvel**:

     1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis** e selecione a subpasta **Dispositivos móveis**.

     2. No espaço de trabalho da subpasta **Dispositivos móveis**, clique no botão **Adicionar dispositivo móvel**.

        O Assistente de conexão de novos dispositivos móveis é iniciado.

2. Na página **Sistema operacional** do assistente, selecione **iOS** como o tipo de sistema operacional do dispositivo móvel.

3. Na página **Selecionando um Servidor de MDM do iOS**, selecione o servidor MDM do iOS.

4. Na página **Selecionar usuários cujos dispositivos móveis devem ser gerenciados**, selecione os usuários, grupos de segurança ou grupos de segurança do Active Directory para os quais deseja adicionar na lista de dispositivos gerenciados.

   Esta etapa será ignorada se você iniciar o assistente, selecionando **Adicionar dispositivo móvel** no menu de contexto da pasta **Contas de usuário**.

   Se deseja adicionar uma nova conta de usuário à lista, clique no botão **Adicionar** e insira as propriedades da conta na janela que é aberta. Se deseja modificar ou revisar as propriedades da conta do usuário, selecione a conta do usuário na lista e clique no botão **Propriedades**.

5. No assistente, na página **Origem do certificado**, especifique o método para a criação do certificado compartilhado que o Servidor de Administração usará para identificar o dispositivo móvel. Você poderá especificar um certificado compartilhado usando uma das seguintes formas:

   - **Emitir o certificado através das ferramentas do Servidor de Administração**

     Selecione esta opção para criar um novo certificado através das ferramentas do Servidor de Administração, se você não o criou anteriormente.

     Se essa opção for selecionada, o perfil de MDM do iOS será assinado com um certificado gerado automaticamente pelo Servidor de Administração.

     Esta opção está marcada por padrão.

   - **Especificar arquivo do certificado**

     Selecione esta opção para especificar um arquivo de certificado criado anteriormente.

     Este método não está disponível se múltiplos usuários foram selecionados na etapa anterior.

6. No assistente, na página **Método de notificação ao usuário**, defina as configurações para notificar o usuário do dispositivo móvel sobre a criação do certificado com uma mensagem SMS ou por e-mail:

   - **Mostrar link no assistente**

     Se você selecionar esta opção, um link ao pacote de instalação será mostrado na etapa final do Assistente de conexão de novos dispositivos móveis.

     Esta opção não está disponível se múltiplos usuários foram selecionados para a conexão do dispositivo.

   - **Enviar link para o usuário**

     A seleção desta opção permite configurar a notificação ao usuário sobre a conexão de um novo dispositivo móvel.

     Você pode selecionar o tipo de endereço de e-mail, especificar um endereço de e-mail adicional e editar o texto da mensagem. Você também pode selecionar o tipo de telefone do usuário para enviar uma mensagem de SMS, especificar um número de telefone adicional e editar o texto da mensagem de SMS.

     Se o Servidor de SMTP não tiver sido configurado, nenhuma mensagem de e-mail poderá ser enviada aos usuários. Se a notificação de SMS não tiver sido configurada, nenhuma mensagem de SMS pode ser enviada aos usuários.

7. Na página **Resultados**, clique no botão **Concluir** para fechar o assistente.

O perfil de MDM do iOS será automaticamente publicado no Servidor Web do Kaspersky Security Center. Os usuários de dispositivos móveis recebem uma notificação com um link para baixar o perfil de MDM do iOS a partir do Servidor da Web. O usuário clica no link. Após isso, o sistema operacional do dispositivo móvel solicita que o usuário a aceite a instalação do perfil de MDM do iOS. O usuário deve aceitar instalar o perfil MDM iOS antes que possa baixar o perfil MDM iOS no dispositivo móvel. Após o perfil de MDM do iOS ter sido baixado e o dispositivo móvel for sincronizado com o Servidor de Administração, o dispositivo será exibido na pasta **Dispositivos móveis** que é uma subpasta da pasta **Gerenciamento de Dispositivos Móveis** na árvore do console.

Para permitir ao usuário prosseguir para o Servidor Web do Kaspersky Security Center usando o link, a conexão com o Servidor de Administração através da porta 8061 deve estar disponível no dispositivo móvel.

Adicionando dispositivos móveis Android na lista de dispositivos gerenciados

Para adicionar um dispositivo móvel Android à lista de dispositivos gerenciados, o Kaspersky Endpoint Security for Android e um certificado compartilhado devem ser fornecidos e instalados no dispositivo móvel. Os certificados compartilhados são usados pelo Servidor de Administração para identificar os dispositivos móveis. Após um certificado compartilhado ter sido fornecido e instalado em um dispositivo móvel, o dispositivo é exibido na lista de dispositivos gerenciados.

Você pode adicionar dispositivos móveis de usuários à lista de dispositivos gerenciados por meio do Assistente de conexão de novos dispositivos móveis. O assistente fornece duas opções para fornecimento e instalação de um certificado compartilhado e o Kaspersky Endpoint Security for Android:

- Ao usar o link ao Google Play
- Ao usar um link do Servidor Web do Kaspersky Security Center

  O pacote de instalação do Kaspersky Endpoint Security for Android armazenado para distribuição no Servidor de Administração é usado para instalação

Iniciar o Assistente de conexão de novos dispositivos móveis

Para iniciar o Assistente de conexão de novos dispositivos móveis, siga um destes procedimentos:

- Use o menu contextual na pasta **Contas de usuário**:

  1. Na árvore do console, expanda a pasta **Avançado** e selecione a subpasta **Contas de usuário**.
  2. No espaço de trabalho da pasta **Contas de usuário**, selecione os usuários, grupos de segurança ou grupos de segurança do Active Directory para os quais deseja adicionar na lista de dispositivos gerenciados.
  3. Clique com o botão direito no menu contextual da conta do usuário, selecione **Adicionar dispositivo móvel**.

     O Assistente de conexão de novos dispositivos móveis é iniciado.

- No espaço de trabalho da pasta **Dispositivos móveis**, clique no botão **Adicionar dispositivo móvel**:

  1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis** e selecione a subpasta **Dispositivos móveis**.
  2. No espaço de trabalho da subpasta **Dispositivos móveis**, clique no botão **Adicionar dispositivo móvel**.

     O Assistente de conexão de novos dispositivos móveis é iniciado.

Adicionando um dispositivo móvel Android usando um link do Google Play

Para instalar o Kaspersky Endpoint Security for Android e um certificado compartilhado em um dispositivo móvel usando um link do Google Play:

1. Inicie o Assistente de conexão de novos dispositivos móveis.
2. Na página **Sistema operacional** do assistente, selecione **Android** como o tipo de sistema operacional do dispositivo móvel.
3. Na página **Método de instalação do Kaspersky Endpoint Security for Android** do assistente, selecione **Ao usar um link ao Google Play**.
4. Na página **Selecionar usuários cujos dispositivos móveis devem ser gerenciados** do assistente, selecione os usuários, grupos de segurança ou grupos de segurança do Active Directory cujos dispositivos móveis deseja adicionar na lista de dispositivos gerenciados.

   Esta etapa será ignorada se o assistente for iniciado, selecionando **Adicionar dispositivo móvel** no menu contextual da pasta **Contas de usuário**.

   Se deseja adicionar uma nova conta de usuário à lista, clique no botão **Adicionar** e insira as propriedades da conta na janela que é aberta. Se deseja modificar ou revisar as propriedades da conta do usuário, selecione a conta do usuário na lista e clique no botão **Propriedades**.
5. No assistente, na página **Origem do certificado**, especifique o método para a criação do certificado compartilhado que o Servidor de Administração usará para identificar o dispositivo móvel. Você poderá especificar um certificado compartilhado usando uma das seguintes formas:

   - **Emitir o certificado através das ferramentas do Servidor de Administração**

     Selecione esta opção para criar um novo certificado através das ferramentas do Servidor de Administração, se você não o criou anteriormente.

     Se essa opção for selecionada, o certificado é automaticamente emitido usando as ferramentas do Servidor de Administração.

     Esta opção está marcada por padrão.

   - **Especificar arquivo do certificado**

     Selecione esta opção para especificar um arquivo de certificado criado anteriormente.

     Este método não está disponível se múltiplos usuários foram selecionados na etapa anterior.

6. No assistente, na página **Método de notificação ao usuário**, defina as configurações para notificar o usuário do dispositivo móvel sobre a criação do certificado com uma mensagem SMS ou por e-mail:

   - **Mostrar link no assistente**

     Se você selecionar esta opção, um link ao pacote de instalação será mostrado na etapa final do Assistente de conexão de novos dispositivos móveis.

     Esta opção não está disponível se múltiplos usuários foram selecionados para a conexão do dispositivo.

   - **Enviar link para o usuário**

     A seleção desta opção permite configurar a notificação ao usuário sobre a conexão de um novo dispositivo móvel.

     Você pode selecionar o tipo de endereço de e-mail, especificar um endereço de e-mail adicional e editar o texto da mensagem. Você também pode selecionar o tipo de telefone do usuário para enviar uma mensagem de SMS, especificar um número de telefone adicional e editar o texto da mensagem de SMS.

     Se o Servidor de SMTP não tiver sido configurado, nenhuma mensagem de e-mail poderá ser enviada aos usuários. Se a notificação de SMS não tiver sido configurada, nenhuma mensagem de SMS pode ser enviada aos usuários.

7. Na página **Resultados**, clique no botão **Concluir** para fechar o assistente.

Após a conclusão do assistente, um link e um código QR serão enviados para o dispositivo móvel do usuário, permitindo-lhe baixar o Kaspersky Endpoint Security for Android. O usuário clica no link ou digitaliza o código QR. Após isso, o sistema operacional do dispositivo móvel solicita que o usuário aceite a instalação do Kaspersky Endpoint Security for Android. Depois que Kaspersky Endpoint Security para Android for baixado e instalado, o dispositivo móvel conecta-se ao Servidor de Administração e baixa um certificado compartilhado. Após o certificado ter sido instalado no dispositivo móvel, este é exibido na pasta **Dispositivos móveis**, que é uma subpasta da pasta **Gerenciamento de Dispositivos Móveis** na árvore do console.

Adicionando um dispositivo móvel Android usando um link do Servidor Web do Kaspersky Security Center

O pacote de instalação do Kaspersky Endpoint Security for Android publicado no Servidor de Administração é usado para a instalação.

Para instalar o Kaspersky Endpoint Security for Android e um certificado compartilhado em um dispositivo móvel usando um link do servidor da Web:

1. Inicie o Assistente de conexão de novos dispositivos móveis.

2. Na página **Sistema operacional** do assistente, selecione **Android** como o tipo de sistema operacional do dispositivo móvel.

3. Na página **Método de instalação do Kaspersky Endpoint Security for Android** do assistente, selecione **Ao usar um link do Servidor da Web**.

   No campo que aparece abaixo, selecione um pacote de instalação ou crie um novo um clicando em **Novo**.

4. Na página **Selecionar usuários cujos dispositivos móveis devem ser gerenciados** do assistente, selecione os usuários, grupos de segurança ou grupos de segurança do Active Directory cujos dispositivos móveis deseja adicionar na lista de dispositivos gerenciados.

   Esta etapa será ignorada se o assistente for iniciado, selecionando **Adicionar dispositivo móvel** no menu contextual da pasta **Contas de usuário**.

   Se deseja adicionar uma nova conta de usuário à lista, clique no botão **Adicionar** e insira as propriedades da conta na janela que é aberta. Se deseja modificar ou revisar as propriedades da conta do usuário, selecione a conta do usuário na lista e clique no botão **Propriedades**.

5. No assistente, na página **Origem do certificado**, especifique o método para a criação do certificado compartilhado que o Servidor de Administração usará para identificar o dispositivo móvel. Você poderá especificar um certificado compartilhado usando uma das seguintes formas:

   - **Emitir o certificado através das ferramentas do Servidor de Administração**

     Selecione esta opção para criar um novo certificado através das ferramentas do Servidor de Administração, se você não o criou anteriormente.

     Se essa opção for selecionada, o certificado é automaticamente emitido usando as ferramentas do Servidor de Administração.

     Esta opção está marcada por padrão.

   - **Especificar arquivo do certificado**

     Selecione esta opção para especificar um arquivo de certificado criado anteriormente.

     Este método não está disponível se múltiplos usuários foram selecionados na etapa anterior.

6. No assistente, na página **Método de notificação ao usuário**, defina as configurações para notificar o usuário do dispositivo móvel sobre a criação do certificado com uma mensagem SMS ou por e-mail:

   - **Mostrar link no assistente**

     Se você selecionar esta opção, um link ao pacote de instalação será mostrado na etapa final do Assistente de conexão de novos dispositivos móveis.

     Esta opção não está disponível se múltiplos usuários foram selecionados para a conexão do dispositivo.

   - **Enviar link para o usuário**

     A seleção desta opção permite configurar a notificação ao usuário sobre a conexão de um novo dispositivo móvel.

     Você pode selecionar o tipo de endereço de e-mail, especificar um endereço de e-mail adicional e editar o texto da mensagem. Você também pode selecionar o tipo de telefone do usuário para enviar uma mensagem de SMS, especificar um número de telefone adicional e editar o texto da mensagem de SMS.

     Se o Servidor de SMTP não tiver sido configurado, nenhuma mensagem de e-mail poderá ser enviada aos usuários. Se a notificação de SMS não tiver sido configurada, nenhuma mensagem de SMS pode ser enviada aos usuários.

7. Na página **Resultados**, clique no botão **Concluir** para fechar o assistente.

O pacote de aplicativos móveis do Kaspersky Endpoint Security for Android será automaticamente publicado no Servidor Web do Kaspersky Security Center. O pacote de aplicativos móveis contém o aplicativo, as configurações para conexão do dispositivo móvel com o Servidor de Administração e um certificado. O usuário do dispositivo móvel receberá uma notificação que contém um link para baixar do pacote do Servidor Web. O usuário clica no link. O sistema operacional do dispositivo móvel solicita então que o usuário aceite a instalação do pacote de aplicativos móveis. Se o usuário concordar, o pacote será baixado no dispositivo móvel. Após o pacote ter sido baixado e o dispositivo móvel for sincronizado com o Servidor de Administração, o dispositivo será exibido na pasta **Dispositivos móveis**, que é uma subpasta da pasta **Gerenciamento de Dispositivos Móveis** na árvore do console.

Gerenciamento de dispositivos móveis Exchange ActiveSync

Essa seção descreve funcionalidades avançadas para gerenciamento de dispositivos EAS através do Kaspersky Security Center.

Além do gerenciamento de dispositivos EAS através de comandos, o administrador pode usar as seguintes opções:

- Criar perfis de gerenciamento para dispositivos EAS, atribuí-los a caixas de correio de usuários. *Perfil de gerenciamento de dispositivos EAS* é uma política do Exchange ActiveSync que é usada em um servidor Microsoft Exchange para gerenciar dispositivos EAS. Em um perfil de gerenciamento de dispositivo EAS, você pode configurar os seguintes grupos de configurações:
  - Configurações de gerenciamento da senha do usuário
  - Configurações de sincronização de correio
  - Restrições no uso de recursos do dispositivo móvel
  - Restrições no uso de aplicativos móveis no dispositivo móvel

  Dependendo do modelo do dispositivo móvel, as configurações de um perfil de gerenciamento podem ser aplicadas parcialmente. O status de uma política Exchange ActiveSync que foi aplicada pode ser visualizado nas propriedades do dispositivo.
- Visualizar informações sobre as configurações do gerenciamento do dispositivo EAS. Por exemplo, nas propriedades de um dispositivo móvel, o administrador pode visualizar a hora da última sincronização com um Microsoft Exchange Server, a ID do dispositivo EAS, o nome da política Exchange ActiveSync e o status atual do dispositivo móvel.
- Desconectar dispositivos EAS do gerenciamento se não estiverem sendo usados.
- Defina as configurações da sondagem do Active Directory pelo Servidor de dispositivos móveis Exchange, o qual permite atualizar as informações sobre as caixas de correio e dispositivos móveis de usuários.

Adicionar um perfil de gerenciamento

Para gerenciar dispositivos EAS, você pode criar perfis de gerenciamento de dispositivos EAS e atribuí-los a caixas de correio Microsoft Exchange selecionadas.

Somente um perfil de gerenciamento de dispositivos EAS pode ser atribuído a uma caixa de correio do Microsoft Exchange.

Para adicionar um perfil de gerenciamento de dispositivos EAS para uma caixa de correio do Microsoft Exchange:

1. Na árvore do console, abra a pasta **Gerenciamento de Dispositivos Móveis**.
2. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Servidores de dispositivos móveis**.
3. No espaço de trabalho da pasta **Servidores de dispositivos móveis**, selecione um Servidor de dispositivos móveis Exchange.
4. No menu de contexto do Servidor de dispositivos móveis Exchange, selecione **Propriedades**.

   A janela propriedades do Servidor de dispositivos móveis é aberta.

5. Na janela de propriedades do **Servidor de dispositivos móveis do Exchange**, selecione a seção **Caixas de correio**.

6. Selecione uma caixa de correio e clique no botão **Atribuir perfil**.

   A janela **Perfis de política** se abre.

7. Na janela **Perfis de política**, clique no botão **Adicionar**.

   A janela **Novo perfil** se abre.

8. Configure o perfil nas guias da janela **Novo perfil**.

   - Se você desejar especificar o nome do perfil e o intervalo de atualização, selecione a guia **Geral**.
   - Se você desejar configurar a senha do usuário do dispositivo móvel, selecione a guia **Senha**.
   - Se você desejar configurar a sincronização com o servidor Microsoft Exchange, selecione a guia **Sincronização**.
   - Se você desejar configurar restrições nos recursos do dispositivo móvel, selecione a guia **Restrições de recurso**.
   - Se você desejar configurar a restrição no uso de aplicativos móveis no dispositivo móvel, selecione a guia **Restrições do aplicativo**.

9. Clique em **OK**.

   O novo perfil será exibido na lista de perfis na janela **Perfis de política**.

   Se você desejar que esse perfil seja automaticamente atribuído às novas caixas de correio, assim como para as caixas de correio cujos perfis que foram excluídos, selecione o perfil na lista de perfis e clique no botão **Definir como perfil padrão**.

   > O perfil padrão não pode ser excluído. Para excluir o perfil padrão atual, você deve atribuir o atributo "perfil padrão" a um perfil diferente.

10. Na janela **Perfis de política** clique em **OK**.

    As configurações do perfil de gerenciamento serão aplicadas no dispositivo EAS na próxima sincronização do dispositivo com o Servidor de dispositivos móveis Exchange.

Remover um perfil de gerenciamento

Para remover um perfil de gerenciamento de dispositivos EAS para uma caixa de correio do Microsoft Exchange:

1. Na árvore do console, abra a pasta **Gerenciamento de Dispositivos Móveis**.

2. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Servidores de dispositivos móveis**.

3. No espaço de trabalho da pasta **Servidores de dispositivos móveis**, selecione um Servidor de dispositivos móveis Exchange.

4. No menu de contexto do Servidor de dispositivos móveis Exchange, selecione **Propriedades**.

   A janela propriedades do Servidor de dispositivos móveis é aberta.

5. Na janela de propriedades do Servidor de dispositivos móveis Exchange, selecione a seção **Caixas de correio**.

6. Selecione uma caixa de correio e clique no botão **Alterar perfis**.

   A janela **Perfis da política** abre.

7. Na janela **Perfis da política**, selecione o perfil que você deseja remover e clique no botão vermelho Excluir.

   O perfil selecionado será removido da lista de perfis gerenciados. O perfil padrão atual será aplicado a dispositivos EAS gerenciados pelo perfil que foi removido.

   > Se você desejar remover o perfil padrão atual, atribua novamente a propriedade "perfil padrão" a outro perfil e, a seguir, remova o primeiro.

Tratar as políticas do Exchange ActiveSync

Após você instalar o Servidor de dispositivos móveis Exchange, na seção **Caixas de correio** da janela Propriedades do servidor, você pode exibir informações sobre contas do servidor Microsoft Exchange que foram recuperadas ao amostrar o domínio atual ou o floresta de domínios.

Também, na janela de propriedades do Servidor de dispositivos móveis Exchange, você pode usar os seguintes botões:

- **Alterar perfis** permite você abrir a janela **Perfis da política**, que contém uma lista de políticas recuperadas do servidor Microsoft Exchange. Nesta janela, você pode criar, editar ou excluir políticas do Exchange ActiveSync. A janela **Perfis da política** é quase idêntica à janela de edição da política no Console de Gerenciamento do Exchange.

- **Atribuir perfis a dispositivos móveis** permite atribuir perfis a uma política do Exchange ActiveSync selecionada a uma ou diversas contas.

- **Ativar/Desativar ActiveSync** permite ativar ou desativar o Exchange ActiveSync HTTP para uma ou múltiplas contas.

Configurar o escopo da verificação

Nas propriedades do Servidor de dispositivos móveis Exchange recém instalado, na seção **Configurações**, você pode configurar o escopo da verificação. Por padrão, o escopo da verificação é o domínio atual no qual o Servidor de dispositivos móveis Exchange estiver instalado. Selecionar o valor **Toda a floresta de domínios** expande o escopo da verificação para incluir todo floresta de domínios.

Trabalhar com dispositivos EAS

Os dispositivos recuperados ao verificar o servidor Microsoft Exchange serão adicionados à lista comum de dispositivos, que está localizada no nó **Gerenciamento de Dispositivos Móveis** na pasta **Dispositivos móveis**.

Se você desejar que a pasta **Dispositivos móveis** exiba somente os dispositivos Exchange ActiveSync (doravante designado como dispositivos EAS), filtre a lista de dispositivo clicando no link **Exchange ActiveSync (EAS)** que está localizado acima nesta lista.

Você pode gerenciar os dispositivos EAS através de comandos. Por exemplo, o comando **Redefinir as configurações padrão** permite remover todos os dados de um dispositivo e redefinir as configurações do dispositivo para as configurações de fábrica. Este comando é útil se o dispositivo for perdido ou roubado, quando você tem de impedir que os dados pessoais ou corporativos caiam nas mãos de uma terceira pessoa.

Se todos os dados foram excluídos do dispositivo, eles serão novamente excluídos na próxima vez que o dispositivo se conectar ao Microsoft Exchange Server. O comando será repetido até que o dispositivo seja removido da lista de dispositivos. Este comportamento é causado pelos princípios de operação do servidor Microsoft Exchange.

Para remover um dispositivo EAS da lista, no menu de contexto do dispositivo, selecione **Excluir**. Se a conta do Exchange ActiveSync não for excluída do dispositivo EAS, o último reaparecerá na lista de dispositivos após a próxima sincronização do dispositivo com o servidor Microsoft Exchange.

Exibir informações sobre um dispositivo EAS

Para visualizar informações sobre um dispositivo EAS:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre dispositivos EAS clicando no link **Exchange ActiveSync (EAS)**.

3. No menu de contexto do dispositivo móvel, selecione **Propriedades**.

   A janela Propriedades do dispositivo EAS é aberta.

A janela de propriedades do dispositivo móvel exibe informações sobre o dispositivo EAS conectado.

Desconectar um dispositivo EAS do gerenciamento

Para desconectar um dispositivo EAS do gerenciamento através do Servidor de dispositivos móveis Exchange:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre dispositivos EAS clicando no link **Exchange ActiveSync (EAS)**.

3. Selecione o dispositivo móvel que você desejar desconectar do gerenciamento pelo Servidor de dispositivos móveis Exchange.

4. No menu de contexto do dispositivo móvel, selecione **Excluir**.

O dispositivo EAS é marcado para remoção com um ícone de cruz vermelha. O dispositivo móvel é removido da lista de dispositivos gerenciados após ter sido removido do banco de dados do Exchange ActiveSync Server. Para isso, o administrador deve remover a conta do usuário no servidor Microsoft Exchange.

Direitos do usuário para gerenciar dispositivos móveis Exchange ActiveSync

Para gerenciar dispositivos móveis executados com o protocolo Exchange ActiveSync com Microsoft Exchange Server 2010 ou Microsoft Exchange Server 2013, certifique-se de que o usuário é incluído em um grupo de funções para os quais os seguintes commandlets têm execução permitida:

- Get-CASMailbox
- Set-CASMailbox
- Remove-ActiveSyncDevice
- Clear-ActiveSyncDevice
- Get-ActiveSyncDeviceStatistics
- Get-AcceptedDomain
- Set-AdServerSettings
- Get-ActiveSyncMailboxPolicy
- New-ActiveSyncMailboxPolicy
- Set-ActiveSyncMailboxPolicy
- Remove-ActiveSyncMailboxPolicy

Para gerenciar dispositivos móveis executados com o protocolo Exchange ActiveSync com Microsoft Exchange Server 2007, certifique-se de que o usuário tem direitos de administrador. Se os direitos não forem concedidos, execute os commandlets para atribuir os direitos do administrador ao usuário (consulte a tabela embaixo).

Direitos de administrador requeridos para gerenciamento de dispositivos móveis Exchange ActiveSync em Microsoft Exchange Server 2007

Acesso	Objeto	Cmdlet
Completo	Ramificação "CN=Mobile Mailbox Policies,CN=Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=yourdomain"	`Add-ADPermission -User < Nome de usuário ou grupo > -Identity "CN=Mobile Mailbox Policies,CN=< Nome da organização >,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=< Nome do domínio >" -InheritanceType All -AccessRight GenericAll`
Ler	Ramificação "CN= Your Organization,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC= yourdomain"	`Add-ADPermission -User < Nome do usuário ou grupo > -Identity "CN=< Nome da organização >,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=< Nome do domínio >" -InheritanceType All -AccessRight GenericRead`
Ler/gravar	Propriedades msExchMobileMailboxPolicyLink e msExchOmaAdminWirelessEnable para objetos no Active Directory	`Add-ADPermission -User < Nome do usuário ou grupo > -Identity "DC=< Dome do domínio >" -InheritanceType All -AccessRight ReadProperty,WriteProperty -Properties msExchMobileMailboxPolicyLink, msExchOmaAdminWirelessEnable`
Completo	Repositórios de caixa do correio para ms-Exch-Store-Admin	`Get-MailboxDatabase | Add-ADPermission -User < nome de usuário ou grupo > -ExtendedRights ms-Exch-Store-Admin`

Para informações detalhadas sobre como utilizar os commandlets no console Exchange Management Shell consulte o site de Suporte Técnico do Microsoft Exchange Server.

Gerenciamento de dispositivos MDM do iOS

Essa seção descreve funcionalidades avançadas para gerenciamento de dispositivos MDM do iOS através do Kaspersky Security Center. O aplicativo suporta os seguintes recursos para o gerenciamento de dispositivos MDM do iOS:

- Defina as configurações de dispositivos MDM do iOS gerenciados no modo centralizado e limite os recursos dos dispositivos através de perfis de configuração. Você pode adicionar ou modificar perfis de configuração e instalá-los em dispositivos móveis.
- Instale os aplicativos em dispositivos móveis por meio de perfis de provisionamento, não através da App Store. Por exemplo, você pode usar perfis de provisionamento para a instalação de aplicativos corporativos internos nos dispositivos móveis de usuários. Um perfil de provisionamento contém informações sobre um aplicativo e um dispositivo móvel.
- Instale os aplicativos em um dispositivo MDM do iOS através da App Store. Antes de instalar um aplicativo em um dispositivo MDM do iOS, você deve adicionar aquele aplicativo em um Servidor MDM do iOS.

A cada 24 horas, uma notificação push é enviada para todos os dispositivos móveis MDM do iOS conectados para sincronizar os dados com o Servidor de MDM do iOS.

Para obter informações sobre o perfil de configuração e o perfil de provisionamento, assim como os aplicativos instalados no dispositivo MDM do iOS, consulte a janela Propriedades do dispositivo.

Assinando um perfil MDM do iOS por um certificado

Você pode assinar um perfil MDM do iOS por um certificado. Você pode usar um certificado emitido por você ou pode receber um certificado de autoridades de certificação confiáveis.

Os dispositivos iOS exibem uma isenção de responsabilidade para perfis não assinados e solicitam que o usuário confie no signatário ao instalar o perfil.

Para assinar um perfil de MDM do iOS por um certificado:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.
2. No menu de contexto da pasta **Dispositivos móveis**, selecione **Propriedades**.
3. Na janela de propriedades da pasta, selecione a seção **Configurações de conexão para dispositivos iOS**.
4. Clique no botão **Procurar** abaixo do campo **Selecione o arquivo de certificado**.

   A janela **Certificado**.

5. No campo **Tipo de certificado**, especifique o tipo de certificado público ou privado:

   - Se o valor **Contêiner PKCS#12** for selecionado, especifique o arquivo de certificado e a senha.
   - Se o valor **Certificado X.509** estiver selecionado:

     a. Especifique um arquivo de chave privada (um com a extensão *.prk ou *.pem).

     b. Especifique a senha da chave privada.

     c. Especifique o arquivo de chave pública (com a extensão *.cer).

6. Clique em **OK**.

O perfil MDM do iOS é assinado por um certificado.

Adicionar um perfil de configuração

Para criar um perfil de configuração, você pode usar o Apple Configurator 2, disponível no site da Apple Inc. O Apple Configurator 2 funciona apenas em dispositivos que executam macOS. Se você não tiver esses dispositivos à sua disposição, poderá usar o Utilitário de Configuração do iPhone no dispositivo equipado com o Console de Administração, em vez disso. No entanto, a Apple Inc. não oferece mais compatibilidade para o Utilitário de configuração do iPhone.

Para criar um perfil de configuração usando u Utilitário de Configuração do iPhone e adicioná-lo a um Servidor de MDM do iOS:

1. Na árvore do console, selecione a pasta **Gerenciamento de Dispositivos Móveis**.
2. No espaço de trabalho da pasta **Gerenciamento de Dispositivos Móveis**, selecione a subpasta **Servidores de dispositivos móveis**.
3. No espaço de trabalho da pasta **Servidores de dispositivos móveis**, selecione um Servidor de MDM do iOS.
4. No menu de contexto do servidor MDM do iOS, selecione **Propriedades**.

   A janela propriedades do Servidor de dispositivos móveis é aberta.
5. Na janela de propriedades do Servidor de MDM do iOS, selecione a seção **Perfis de configuração**.
6. Na seção **Perfis de configuração**, clique no botão **Criar**.

   A janela **Novo perfil de configuração** se abre.
7. Na janela **Novo perfil de configuração**, especifique um nome e ID para o perfil.

   O ID do perfil de configuração deve ser único; o valor deve ser especificado em formato Reverse-DNS, por exemplo, *com.companyname.identifier*.
8. Clique em **OK**.

   Se estiver instalado, o Utilitário de Configuração do iPhone é iniciado.
9. Configure novamente o perfil no Utilitário de Configuração do iPhone.

   Para obter uma descrição das configurações do perfil e instruções sobre como configurar o perfil consulte a documentação incluída no Utilitário de Configuração do iPhone.

Após você ter configurado o perfil com o Utilitário de Configuração do iPhone, o novo perfil de configuração será exibido na seção **Perfis de configuração** da janela Propriedades do Servidor de MDM do iOS.

Você pode clicar no botão **Modificar** para modificar o perfil de configuração.

Você pode clicar no botão **Importar** para carregar o perfil de configuração para um programa.

Você pode clicar no botão **Exportar** para salvar o perfil de configuração em um arquivo.

O perfil que você criou deve ser instalado em dispositivos MDM do iOS.

Instalar um perfil de configuração no um dispositivo

Para instalar um perfil de configuração em um dispositivo móvel:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre os dispositivos MDM do iOS por protocolo (*MDM do iOS*).

3. Selecione o dispositivo móvel do usuário onde você deseja instalar um perfil de configuração.

   Você pode selecionar múltiplos dispositivos para instalar neles o perfil em simultâneo.

4. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

5. Na janela **Comandos de gerenciamento de dispositivos móveis**, siga para a seção **Instalar perfil** e clique no botão **Enviar comando**.

   Você pode também enviar o comando para o dispositivo selecionando **Todos os comandos** no menu de contexto do dispositivo móvel e, a seguir, selecionando **Instalar o perfil**.

   A janela **Selecionar perfis** é aberta e exibe uma lista de perfis. Selecione na lista o perfil que você deseja instalar no dispositivo móvel. Você pode selecionar múltiplos perfis para os instalar no dispositivo móvel em simultâneo. Para selecionar o conjunto de perfis, use a tecla **Shift**. Para combinar perfis em um grupo, use a tecla **CTRL**.

6. Clique em **OK** para enviar o comando para o dispositivo móvel.

   Quando o comando é executado, o perfil de configuração selecionado será instalado no dispositivo móvel do usuário. Se o comando for executado com êxito, o status atual do comando no registro de comandos será exibido como *Concluído*.

   Você pode clicar no botão **Reenviar** para enviar novamente o comando para o dispositivo móvel do usuário.

   Você pode clicar no botão **Remover da fila** para cancelar a execução de um comando que foi enviado, se o comando ainda não tenha sido executado.

   A seção **Log de comandos** exibe comandos que foram enviados para o dispositivo móvel, com os respetivos status de execução. Clique em **Atualizar** para atualizar a lista de comandos.

7. Clique em **OK** para fechar a janela **Comandos de gerenciamento de dispositivos móveis**.

Você pode ver o perfil instalado e removê-lo, se necessário.

Remover o perfil de configuração de um dispositivo

Para remover um perfil de configuração de um dispositivo:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre dispositivos MDM do iOS clicando no link **MDM do iOS**.

3. Selecione o dispositivo móvel do usuário a partir do qual você deseja remover o perfil de configuração.

   Você pode selecionar múltiplos dispositivos para remover o perfil neles em simultâneo.

4. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

5. Na janela **Comandos de gerenciamento de dispositivos móveis**, siga para a seção **Remover perfil** e clique no botão **Enviar comando**.

   Você pode também enviar o comando para o dispositivo móvel selecionando **Todos os comandos** no menu de contexto do dispositivo e, a seguir, selecionando **Remover o perfil**.

   A janela **Remover perfis** é aberta e exibe uma lista de perfis.

6. Selecione na lista o perfil que você deseja remover do dispositivo móvel. Você pode selecionar múltiplos perfis para os remover do dispositivo móvel em simultâneo. Para selecionar o conjunto de perfis, use a tecla **Shift**. Para combinar perfis em um grupo, use a tecla **CTRL**.

7. Clique em **OK** para enviar o comando para o dispositivo móvel.

   Quando o comando é executado, o perfil de configuração selecionado será removido do dispositivo móvel do usuário. Se o comando for executado com êxito, o status atual do comando será exibido como *Concluído*.

   Você pode clicar no botão **Reenviar** para enviar novamente o comando para o dispositivo móvel do usuário.

   Você pode clicar no botão **Remover da fila** para cancelar a execução de um comando que foi enviado, se o comando ainda não tenha sido executado.

   A seção **Log de comandos** exibe comandos que foram enviados para o dispositivo móvel, com os respetivos status de execução. Clique em **Atualizar** para atualizar a lista de comandos.

8. Clique em **OK** para fechar a janela **Comandos de gerenciamento de dispositivos móveis**.

Adicionar um novo dispositivo ao publicar um link a um perfil

No Console de Administração, o administrador cria um novo perfil de iOS MDM, usando o Assistente de instalação de certificados. O assistente executa as seguintes ações:

- O perfil MDM iOS é automaticamente publicado no servidor da Web.
- Ao usuário é enviado um link ao perfil de MDM do iOS através de SMS ou por e-mail. Ao receber o link, o usuário instala o perfil de MDM do iOS no dispositivo móvel.
- O dispositivo móvel conecta-se ao Servidor de MDM do iOS.

Devido a uma política de segurança mais estrita introduzida por Apple, você tem de definir as versões do protocolo TLS 1.1 e TLS 1.2 ao conectar um dispositivo móvel executando o iOS 11 a um Servidor de Administração que tenha a integração com a Infraestrutura de Chaves Públicas (PKI) ativada.

Adicionar um novo dispositivo através da instalação do perfil pelo administrador

Para conectar um dispositivo móvel a um Servidor de MDM do iOS ao instalar um perfil de MDM do iOS naquele dispositivo móvel, o administrador deve executar as seguintes ações:

1. No Console de Administração, abra o Assistente de instalação de certificados.
2. Crie o novo perfil de iOS MDM ao marcar a caixa de seleção **Mostrar o certificado após a conclusão do assistente** na janela do assistente.
3. Salvar o perfil de MDM do iOS.
4. Instalar o perfil de MDM do iOS no dispositivo móvel do usuário através do utilitário Configurador da Apple.

   O dispositivo móvel conecta-se ao Servidor de MDM do iOS.

Devido a uma política de segurança mais estrita introduzida por Apple, você tem de definir as versões do protocolo TLS 1.1 e TLS 1.2 ao conectar um dispositivo móvel executando o iOS 11 a um Servidor de Administração que tenha a integração com a Infraestrutura de Chaves Públicas (PKI) ativada.

Adicionar um perfil de provisionamento

Para adicionar um perfil de provisionamento para um Servidor de MDM do iOS:

1. Na árvore do console, abra a pasta **Gerenciamento de Dispositivos Móveis**.
2. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Servidores de dispositivos móveis**.
3. No espaço de trabalho da pasta **Servidores de dispositivos móveis**, selecione um Servidor de MDM do iOS.

4. No menu de contexto do servidor MDM do iOS, selecione **Propriedades**.

   A janela propriedades do Servidor de dispositivos móveis é aberta.

5. Na janela de propriedades do **Servidor de MDM do iOS**, siga para a seção **Perfis de provisionamento**.

6. Na seção **Perfis de provisionamento**, clique no botão **Importar** e especifique o caminho para um arquivo de perfil de provisionamento.

O perfil será adicionado às configurações do Servidor de MDM do iOS.

Você pode clicar no botão **Exportar** para salvar o perfil de provisionamento em um arquivo.

Você pode instalar o perfil de aprovisionamento importado em dispositivos MDM do iOS.

Instalar um perfil de provisionamento em um dispositivo

Para instalar um perfil de provisionamento em um dispositivo móvel:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre os dispositivos MDM do iOS por protocolo (*MDM do iOS*).

3. Selecione o dispositivo móvel do usuário onde você deseja instalar o perfil de provisionamento.

   Você pode selecionar vários dispositivos para instalar o perfil de provisionamento em simultâneo.

4. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

5. Na janela **Comandos de gerenciamento de dispositivos móveis**, siga para a seção **Instalar perfil de provisionamento** e clique no botão **Enviar comando**.

   Você pode também enviar o comando para o dispositivo selecionando **Todos os comandos** no menu de contexto do dispositivo móvel e, a seguir, selecionando **Instalar o perfil de provisionamento**.

   A janela **Selecionar perfis de provisionamento** é aberta e exibe uma lista de perfis de provisionamento. Selecione na lista o perfil de provisionamento que você deseja instalar no dispositivo móvel. Você pode selecionar múltiplos perfis de provisionamento para os instalar no dispositivo móvel em simultâneo. Para selecionar o conjunto de perfis de provisionamento, use a tecla **Shift**. Para combinar perfis de provisionamento em um grupo, use a tecla **Ctrl**.

6. Clique em **OK** para enviar o comando para o dispositivo móvel.

   Quando o comando é executado, o perfil de provisionamento selecionado será instalado no dispositivo móvel do usuário. Se o comando for executado com êxito, o status atual no registro do comando será exibido como *Concluído*.

   Você pode clicar no botão **Reenviar** para enviar novamente o comando para o dispositivo móvel do usuário.

   Você pode clicar no botão **Remover da fila** para cancelar a execução de um comando que foi enviado, se o comando ainda não tenha sido executado.

   A seção **Log de comandos** exibe comandos que foram enviados para o dispositivo móvel, com os respetivos status de execução. Clique em **Atualizar** para atualizar a lista de comandos.

7. Clique em **OK** para fechar a janela **Comandos de gerenciamento de dispositivos móveis**.

Você pode ver o perfil instalado e removê-lo, se necessário.

Remover um perfil de provisionamento de um dispositivo

Para remover um perfil de provisionamento de um dispositivo móvel:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre os dispositivos MDM do iOS por protocolo (*MDM do iOS*).

3. Selecione o dispositivo móvel do usuário a partir do qual você deseja remover o perfil de provisionamento.

   Você pode selecionar múltiplos dispositivos para remover o perfil de provisionamento neles em simultâneo.

4. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

5. Na janela **Comandos de gerenciamento de dispositivos móveis**, siga para a seção **Remover perfil de provisionamento** e clique no botão **Enviar comando**.

   Você pode também enviar o comando para o dispositivo móvel selecionando **Todos os comandos** no menu de contexto e, a seguir, selecionando **Remover perfil de provisionamento**.

   A janela **Remover perfis de provisionamento** é aberta e exibe uma lista de perfis.

6. Selecione na lista o perfil de provisionamento que você deseja remover do dispositivo móvel. Você pode selecionar múltiplos perfis de provisionamento para os remover do dispositivo móvel em simultâneo. Para selecionar o conjunto de perfis de provisionamento, use a tecla **Shift**. Para combinar perfis de provisionamento em um grupo, use a tecla **Ctrl**.

7. Clique em **OK** para enviar o comando para o dispositivo móvel.

   Quando o comando é executado, o perfil de provisionamento selecionado será removido do dispositivo móvel do usuário. Os aplicativos relacionados com o perfil de provisionamento excluído não poderão ser usados. Se o comando for executado com êxito, o status atual do comando será exibido como *Concluído*.

   Você pode clicar no botão **Reenviar** para enviar novamente o comando para o dispositivo móvel do usuário.

   Você pode clicar no botão **Remover da fila** para cancelar a execução de um comando que foi enviado, se o comando ainda não tenha sido executado.

   A seção **Log de comandos** exibe comandos que foram enviados para o dispositivo móvel, com os respetivos status de execução. Clique em **Atualizar** para atualizar a lista de comandos.

8. Clique em **OK** para fechar a janela **Comandos de gerenciamento de dispositivos móveis**.

Adicionar um aplicativo gerenciado

Antes de instalar um aplicativo em um dispositivo MDM do iOS, você deve adicionar aquele aplicativo em um Servidor MDM do iOS. Um aplicativo é considerado como gerenciado se tiver sido instalado em um dispositivo através do Kaspersky Security Center. Um aplicativo gerenciado pode ser gerenciado remotamente através do Kaspersky Security Center.

Para adicionar um aplicativo gerenciado a um Servidor MDM do iOS:

1. Na árvore do console, abra a pasta **Gerenciamento de Dispositivos Móveis**.
2. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Servidores de dispositivos móveis**.
3. No espaço de trabalho da pasta **Servidores de dispositivos móveis**, selecione um Servidor de MDM do iOS.
4. No menu de contexto do servidor MDM do iOS, selecione **Propriedades**.

   Isso abre a janela de propriedades Servidor MDM do iOS.
5. Na janela Propriedades do servidor MDM do iOS, selecione a seção **Aplicativos gerenciados**.
6. Clique no botão **Adicionar** na seção **Aplicativos gerenciados**.

   A janela **Adicionar um aplicativo** se abre.
7. Na janela **Adicionar um aplicativo**, no campo **Nome do aplicativo**, especifique o nome do aplicativo a ser adicionado.
8. No campo **ID da Apple ou link para o arquivo de manifesto**, especifique a Apple ID do aplicativo a ser adicionado ou especifique um link para um arquivo manifest que possa ser usado para baixar o aplicativo.
9. Se você desejar que um aplicativo gerenciado seja removido do dispositivo móvel do usuário junto com o perfil MDM do iOS ao remover esse último, selecione a caixa de seleção **Remover junto com o perfil de MDM do iOS**.
10. Se você desejar bloquear o backup de dados do aplicativo através do iTunes, selecione a caixa de seleção **Bloquear o backup de dados**.
11. Clique em **OK**.

O aplicativo adicionado é exibido na seção **Aplicativos gerenciados** da janela Propriedades do servidor MDM do iOS.

Instalar um aplicativo em um dispositivo móvel

Para instalar um aplicativo em um dispositivo móvel MDM do iOS:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.
2. Selecione o dispositivo MDM do iOS onde você deseja instalar um aplicativo.

   Você pode selecionar múltiplos dispositivos móveis para neles instalar o aplicativo em simultâneo.
3. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

4. Na janela **Comandos de gerenciamento de dispositivos móveis**, siga para a seção **Instalar o aplicativo** e clique no botão **Enviar comando**.

   Você pode também enviar o comando para o dispositivo selecionando **Todos os comandos** no menu de contexto do dispositivo móvel e, a seguir, selecionando **Instalar o aplicativo**.

   A janela **Selecionar os aplicativos** é aberta e exibe uma lista de perfis. Selecione na lista o aplicativo que você deseja instalar no dispositivo móvel. Você pode selecionar múltiplos aplicativos para os instalar no dispositivo móvel em simultâneo. Para selecionar uma faixa de aplicativos, use a tecla **Shift**. Para combinar apps em um grupo, use a tecla **Ctrl**.

5. Clique no **OK** para enviar o comando para o dispositivo móvel.

   Quando o comando é executado, o aplicativo selecionado será instalado no dispositivo móvel do usuário. Se o comando for executado com êxito, o status atual do comando no registro do comando será exibido como *Concluído*.

   Você pode clicar no botão **Reenviar** para enviar novamente o comando para o dispositivo móvel do usuário. Você pode clicar no botão **Remover da fila** para cancelar a execução de um comando que foi enviado, se o comando ainda não tenha sido executado.

   A seção **Log de comandos** exibe comandos que foram enviados para o dispositivo móvel, com os respetivos status de execução. Clique em **Atualizar** para atualizar a lista de comandos.

6. Clique em **OK** para fechar a janela **Comandos de gerenciamento de dispositivos móveis**.

A informação sobre o aplicativo instalado, é exibida nas propriedades do Dispositivo Móvel MDM do iOS. Você pode remover o aplicativo do dispositivo móvel usando o registro de comandos ou o menu de contexto do dispositivo móvel.

Remover um aplicativo de um dispositivo

Para remover um aplicativo de um dispositivo móvel:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre os dispositivos MDM do iOS por protocolo (*MDM do iOS*).

3. Selecione o dispositivo móvel do usuário a partir do qual você deseja remover o aplicativo.

   Você pode selecionar múltiplos dispositivos móveis para remover deles o aplicativo em simultâneo.

4. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

5. Na janela **Comandos de gerenciamento de dispositivos móveis**, siga para a seção **Remover o aplicativo** e clique no botão **Enviar comando**.

   Você pode também enviar o comando para o dispositivo selecionando **Todos os comandos** no menu de contexto do dispositivo móvel e, a seguir, selecionando **Remover o aplicativo**.

   A janela **Remover os aplicativos** é aberta e exibe uma lista de aplicativos.

6. Selecione na lista o perfil que você desejar remover do dispositivo móvel. Você pode selecionar múltiplos aplicativos para removê-los em simultâneo. Para selecionar uma faixa de aplicativos, use a tecla **Shift**. Para combinar apps em um grupo, use a tecla **Ctrl**.

7. Clique em **OK** para enviar o comando para o dispositivo móvel.

   Quando o comando for executado, os aplicativos selecionados serão removidos do dispositivo móvel do usuário. Se o comando for executado com êxito, o status atual do comando será exibido como *Concluído*.

   Você pode clicar no botão **Reenviar** para enviar novamente o comando para o dispositivo móvel do usuário.

   Você pode clicar no botão **Remover da fila** para cancelar a execução de um comando que foi enviado, se o comando ainda não tenha sido executado.

   A seção **Log de comandos** exibe comandos que foram enviados para o dispositivo móvel, com os respetivos status de execução. Clique em **Atualizar** para atualizar a lista de comandos.

8. Clique em **OK** para fechar a janela **Comandos de gerenciamento de dispositivos móveis**.

Configurar o roaming em um dispositivo móvel MDM do iOS

Para configurar o roaming:

1. Na árvore do console, abra a pasta **Gerenciamento de Dispositivos Móveis**.
2. Na pasta **Gerenciamento de Dispositivos Móveis**, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

3. Selecione o dispositivo MDM do iOS de propriedade do usuário para o qual você precisa configurar o roaming.

   Você pode selecionar múltiplos dispositivos móveis para neles configurar o roaming em simultâneo.

4. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.
5. Na janela **Comandos de gerenciamento de dispositivos móveis**, siga para a seção **Configurar o roaming** e clique no botão **Enviar comando**.

   Você também pode enviar o comando ao dispositivo móvel selecionando **Todos os comandos → Configurar o roaming** no menu de contexto do dispositivo.

6. Na janela **Configurações de roaming**, especifique as configurações relevantes:

   - Ativar roaming de dados

     Se essa opção estiver ativada, o roaming de dados é ativado no dispositivo móvel iOS MDM. O usuário do dispositivo móvel iOS MDM pode navegar na Internet em roaming.

     Por padrão, esta opção está desativada.

O roaming é configurado para os dispositivos selecionados.

Exibir informações sobre um dispositivo MDM do iOS

Para visualizar informações sobre um dispositivo MDM do iOS:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre dispositivos MDM do iOS clicando no link **MDM do iOS**.

3. Selecione o dispositivo móvel para o qual você deseja exibir as informações.

4. No menu de contexto do dispositivo móvel, selecione **Propriedades**.

   A janela de propriedades do dispositivo MDM do iOS abre.

A janela de propriedades do dispositivo móvel exibe informações sobre o dispositivo MDM do iOS conectado.

Desconectar um dispositivo MDM do iOS do gerenciamento

Para desconectar um dispositivo MDM do iOS do Servidor de MDM do iOS:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre dispositivos MDM do iOS clicando no link **MDM do iOS**.

3. Selecione o dispositivo móvel que você deseja desconectar.

4. No menu de contexto do dispositivo móvel, selecione **Excluir**.

   O dispositivo MDM do iOS será marcado na lista para remoção. O dispositivo móvel será automaticamente removido da lista de dispositivos gerenciados após ter sido removido do banco de dados do Servidor de MDM do iOS. O dispositivo móvel será removido do banco de dados do Servidor de MDM do iOS dentro de um minuto.

Após o dispositivo MDM do iOS ter sido desconectado do gerenciamento, todos os perfis de configuração, o perfil de MDM do iOS e os aplicativos instalados para os quais a opção **Remover junto com o perfil de MDM do iOS** tiver sido selecionada, serão removidos do dispositivo móvel.

Enviar comandos para um dispositivo

Para enviar um comando para um dispositivo MDM do iOS:

1. No console de administração, abra o nó **Gerenciamento de Dispositivos Móveis**.

2. Selecione a pasta **Dispositivos móveis**.

3. Na pasta **Dispositivos móveis**, selecione o dispositivo móvel ao qual os comandos têm de ser enviados.

4. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

5. Na lista que aparece, selecione o comando a ser enviado ao dispositivo móvel.

Verificar o status de execução de comandos enviados

Para verificar o status de execução de um comando enviado para um dispositivo móvel:

1. No console de administração, abra o nó **Gerenciamento de Dispositivos Móveis**.

2. Selecione a pasta **Dispositivos móveis**.

3. Na pasta **Dispositivos móveis**, selecione o dispositivo móvel no qual o status de execução deve ser verificado para os comandos selecionados.

4. No menu de contexto do dispositivo móvel, selecione **Exibir log de comandos**.

Gerenciar dispositivos KES

No Kaspersky Security Center, você pode gerenciar dispositivos móveis KES das seguintes maneiras:

- Gerencie centralmente dispositivos KES usando comandos.
- Visualize informações sobre as configurações para gerenciamento de dispositivos KES.
- Instalar aplicativos usando pacotes de aplicativos móveis.
- Desconectar dispositivos KES do gerenciamento.

Criar um pacote de aplicativo móvel para dispositivos KES

Uma licença do Kaspersky Endpoint Security for Android é requerida para criar um pacote de aplicativos móveis para dispositivos KES.

Para criar um pacote de aplicativos móveis:

1. Na pasta **Instalação remota** na árvore do console, selecione a subpasta **Pacotes de instalação**.

   A pasta **Instalação remota** é uma subpasta da pasta **Avançado** por padrão.

2. Clique no botão **Ações adicionais** e selecione **Gerenciar pacotes de aplicativos móveis** na lista suspensa.

3. Na janela **Gerenciamento de pacotes de aplicativos móveis**, clique no botão **Novo**.

4. O Assistente de novo pacote inicia. Siga as instruções do Assistente.

O novo pacote de aplicativos móveis criado é exibido na janela **Gerenciamento de pacotes de aplicativos móveis**.

Ativar a autenticação baseada em certificado de dispositivos do KES

Para ativar a autenticação baseada em certificado de um dispositivo do KES:

1. Abra o registro do sistema do dispositivo cliente com o Servidor de Administração instalado (por exemplo, localmente, usando o comando regedit no menu **Iniciar** → **Executar**).
2. Vá ao seguinte hive:
   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\.core\.independent\KLLIM
   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\.core\.independent\
3. Crie uma chave com o nome de LP_MobileMustUseTwoWayAuthOnPort13292.
4. Especifique REG_DWORD como o tipo de chave.
5. Defina o valor da chave como 1.
6. Reinicie o serviço do Servidor de Administração.

A autenticação obrigatória baseada em certificado do dispositivo do KES usando um certificado compartilhado será ativada após a execução do serviço do Servidor de Administração.

> A primeira conexão do dispositivo KES com o Servidor de Administração não requer um certificado.

Por padrão, a autenticação baseada em certificado de dispositivos do KES é desativada.

Visualizar informações sobre um dispositivo KES

Para visualizar informações sobre um dispositivo KES:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.
2. No espaço de trabalho, filtre os dispositivos KES pelo tipo de protocolo *(KES)*.
3. Selecione o dispositivo móvel para o qual você deseja exibir as informações.
4. No menu de contexto do dispositivo móvel, selecione **Propriedades**.

A janela de propriedades do dispositivo KES é aberta.

A janela de propriedades do dispositivo móvel exibe informações sobre o dispositivo KES conectado.

Desconectar um dispositivo KES do gerenciamento

Para desconectar um dispositivo KES do gerenciamento, o usuário deve remover o Agente de Rede do dispositivo móvel. Após o usuário ter removido o Agente de Rede, os detalhes do dispositivo móvel são removidos do banco de dados do Servidor de Administração, e o administrador poderá remover o dispositivo móvel da lista de dispositivos gerenciados.

Para remover um dispositivo KES da lista de dispositivos gerenciados:

1. Na pasta **Gerenciamento de Dispositivos Móveis** da árvore do console, selecione a subpasta **Dispositivos móveis**.

   O espaço de trabalho da pasta exibe uma lista de dispositivos móveis gerenciados.

2. No espaço de trabalho, filtre os dispositivos KES pelo tipo de protocolo *(KES)*.

3. Selecione o dispositivo móvel que você deseja desconectar do gerenciamento.

4. No menu de contexto do dispositivo móvel, selecione **Excluir**.

O dispositivo será removido da lista de dispositivos gerenciados.

Se o Kaspersky Endpoint Security for Android não tiver sido removido do dispositivo móvel, o aquele dispositivo reaparece na lista de dispositivos gerenciados após a sincronização com o Servidor de Administração.

Criptografia e proteção de dados

A criptografia dos dados reduz o risco de vazamentos não intencionais, caso seu notebook, unidade removível ou um disco rígido seja roubado ou perdido, ou por acesso não autorizado por usuários e aplicativos.

O Kaspersky Endpoint Security for Windows fornece a funcionalidade de criptografia. O Kaspersky Endpoint Security for Windows permite criptografar os arquivos armazenados em unidades locais de dispositivos e de unidades removíveis, assim como as unidades removíveis e discos rígidos inteiramente criptografados.

As regras de criptografia são configuradas usando o Kaspersky Security Center, através da definição de políticas. A criptografia e descriptografia, de acordo com as regras existentes, são executadas após a aplicação de uma política.

A disponibilidade da funcionalidade de gerenciamento de criptografia é determinada pelas configurações de interface do usuário.

O administrador pode executar as seguintes ações:

- Configure e execute a criptografia ou descriptografia de arquivo em unidades locais do dispositivo.
- Configure e efetue a criptografia de arquivos nas unidades removíveis.
- Criar regras de acesso para acessar arquivos criptografados por aplicativo.
- Crie e entregue ao usuário um arquivo de chave para acessar arquivos criptografados se a criptografia do arquivo for restrita ao dispositivo do usuário.

- Configurar e executar a criptografia do disco rígido.
- Gerenciar o acesso de usuários a unidades criptografadas e unidades removíveis (gerenciar contas do agente de autenticação, criar e enviar informações a usuários sobre o nome da conta e a restauração da senha, assim como chaves de acesso a dispositivos criptografados).
- Exiba o status da criptografia e os relatórios sobre a criptografia de arquivos.

Estas operações são efetuadas usando ferramentas integradas no Kaspersky Endpoint Security for Windows. Para obter instruções detalhadas sobre como efetuar operações e uma descrição da funcionalidade de criptografia, consulte a Ajuda on-line do Kaspersky Endpoint Security for Windows.

O Kaspersky Security Center é compatível com a funcionalidade de gerenciamento de criptografia para dispositivos que executam sistemas operacionais macOS. A criptografia é configurada usando as ferramentas do Kaspersky Endpoint Security for Mac para as versões do aplicativo que são compatíveis com a funcionalidade de criptografia. Para obter instruções detalhadas sobre como efetuar operações e uma descrição da funcionalidade de criptografia, consulte o *Guia do Administrador do Kaspersky Endpoint Security for Mac*.

Visualização da lista de dispositivos criptografados

Para ver a lista de dispositivos que armazenam informações criptografadas:

1. Na árvore do console do Servidor de Administração, selecione a pasta **Criptografia e proteção de dados**.
2. Abra a lista de dispositivos criptografados usando uma das seguintes formas:
   - Ao clicar no link **Ir para a lista de dispositivos criptografados** na seção **Gerenciar dispositivos criptografados**.
   - Ao selecionar a pasta **Dispositivos criptografados** na árvore do console.

O espaço de trabalho exibe as informações sobre dispositivos na rede que armazenam arquivos criptografados e sobre dispositivos criptografados ao nível da unidade. Após as informações num dispositivo serem descriptografadas, o dispositivo é automaticamente removido da lista.

Você pode ordenar as informações na lista de dispositivos, seja na ordem ascendente ou descendente, em qualquer coluna.

As configurações da interface do usuário determinam se a pasta **Criptografia e proteção de dados** aparece na árvore do console.

Visualização da lista de eventos de criptografia

Ao executar tarefas de criptografia ou descriptografia de dados nos dispositivos, o Kaspersky Endpoint Security for Windows envia ao Kaspersky Security Center informações sobre os eventos dos seguintes tipos:

- Não é possível criptografar ou descriptografar um arquivo, ou criar um arquivo criptografado devido a falta de espaço livre em disco.
- Não é possível criptografar ou descriptografar um arquivo, ou criar um arquivo criptografado devido a problemas com a licença.

- Não é possível criptografar ou descriptografar um arquivo, ou criar um arquivo criptografado devido a ausência de direitos de acesso.
- O aplicativo foi proibido de acessar um arquivo criptografado.
- Erros desconhecidos.

Para exibir uma lista de eventos que ocorreram durante a criptografia os dados nos dispositivos:

1. Na árvore do console do Servidor de Administração, selecione a pasta **Criptografia e proteção de dados**.
2. Abra a lista de eventos que ocorreram durante a criptografia, usando uma das seguintes formas:
   - Ao clicar no link **Ir para lista de erros** na seção **Erros de criptografia de dados**.
   - Ao selecionar a pasta **Dispositivos criptografados** na árvore do console.

O espaço de trabalho exibe as informações sobre os problemas que ocorreram durante a criptografia dos dados nos dispositivos.

Você pode efetuar as seguintes ações na lista de eventos de criptografia:

- Ordenar registros de dados na ordem ascendente ou descendente, em qualquer coluna.
- Execute uma pesquisa rápida para registros (por correspondência de texto com uma subsequência de caracteres em qualquer campo da lista).
- Exportar a lista de eventos para um arquivo de texto.

> As configurações da interface do usuário determinam se a pasta **Criptografia e proteção de dados** aparece na árvore do console.

Exportação da lista de eventos de criptografia para um arquivo de texto

Para exportar a lista de eventos de criptografia para um arquivo de texto:

1. Criar uma lista de eventos de criptografia.
2. No menu de contexto da lista de eventos, selecione **Exportar a lista**.

   A janela **Exportar a lista** abre.
3. Na janela **Exportar a lista**, especifique o nome do arquivo de texto com a lista de eventos, selecione uma para salvá-lo e clique no botão **Salvar**.

   A lista de eventos de criptografia será salva no arquivo que você especificou.

Criação e visualização de relatórios de criptografia

É possível gerar os seguintes relatórios:

- Relatório de status da criptografia dos dispositivos gerenciados. Este relatório fornece detalhes sobre a criptografia de dados de vários dispositivos gerenciados. Por exemplo, o relatório mostra o número de dispositivos aos quais a política com regras de criptografia configuradas se aplica. Além disso, você pode descobrir, por exemplo, quantos dispositivos precisam ser reinicializados. Ele também contém informações sobre a tecnologia de criptografia e o algoritmo para cada dispositivo.

- Relatório de status da criptografia dos dispositivos de armazenamento em massa. Este relatório contém informações semelhantes ao relatório sobre o status de criptografia de dispositivos gerenciados, mas fornece dados apenas para dispositivos de armazenamento em massa e unidades removíveis.

- Relatório de direitos de acesso aos dispositivos criptografados. Este relatório mostra quais contas de usuário têm acesso a unidades criptografadas.

- Relatório de erros na criptografia de arquivos. Este relatório contém informações sobre os erros que ocorreram ao executar as tarefas de criptografia ou a descriptografia dos dados nos dispositivos.

- Relatório de bloqueio de acesso aos arquivos criptografados. Este relatório contém informações sobre como bloquear o acesso dos aplicativos aos arquivos criptografados. Este relatório será útil se um usuário ou aplicativo não autorizado tentar acessar arquivos ou unidades criptografadas.

Para gerar o relatório sobre criptografia de dispositivos:

1. Na árvore do console, selecione a pasta **Criptografia e proteção de dados**.

2. Execute uma das seguintes ações:

   - Para gerar o relatório sobre o status de criptografia dos dispositivos gerenciados, clique no link **Exibir relatório de status da criptografia de dispositivos de armazenamento**.

     Se você ainda não configurou esse relatório, o Assistente de novo modelo de relatório será iniciado. Siga as etapas do Assistente.

   - Para gerar o relatório sobre o status de criptografia dos dispositivos de armazenamento em massa, na árvore do console, selecione a subpasta **Dispositivos criptografados** e, a seguir, clique no botão **Exibir relatório de status da criptografia de dispositivos de armazenamento**.

A geração do relatório começa. O relatório aparece na guia **Relatórios** do nó **Servidor de Administração**.

Para gerar o relatório sobre direitos de acesso a dispositivos criptografados:

1. Na árvore do console, selecione a pasta **Criptografia e proteção de dados**.
2. Execute uma das seguintes ações:
   - Clique no link **Relatório de direitos de acesso aos dispositivos criptografados** na seção **Gerenciar dispositivos criptografados** para iniciar o Assistente de novo modelo de relatório.
   - Selecione a subpasta **Dispositivos criptografados** e, a seguir, clique no botão **Relatório de direitos de acesso aos dispositivos criptografados** para iniciar o Assistente de novo modelo de relatório.
3. Siga as etapas do Assistente de novo modelo de relatório.

A geração do relatório começa. O relatório aparece na guia **Relatórios** do nó **Servidor de Administração**.

Para gerar o relatório sobre erros de criptografia de arquivo:

1. Na árvore do console, selecione a pasta **Criptografia e proteção de dados**.
2. Execute uma das seguintes ações:
   - Clique no link **Visualizar o relatório de erros de criptografia de arquivo** na seção **Erros de criptografia de dados** para iniciar o Assistente de novo modelo de relatório.
   - Selecione a subpasta **Eventos de criptografia** e, a seguir, clique no link **Relatório de erros na criptografia de arquivos** para iniciar o Assistente de novo modelo de relatório.
3. Siga as etapas do Assistente de novo modelo de relatório.

A geração do relatório começa. O relatório aparece na guia **Relatórios** do nó **Servidor de Administração**.

Para gerar o relatório sobre o status da criptografia do dispositivos gerenciados:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Clique no botão **Novo modelo de relatório** para iniciar o Assistente de novo modelo de relatório.
4. Siga as instruções do Assistente de novo modelo de relatório. Na janela **Selecionar o tipo de modelo de relatório**, na seção **Outro**, selecione **Relatório de status de criptografia de dispositivos gerenciados**.

   Após você ter terminado com o Assistente de novo modelo de relatório, um novo modelo de relatório aparece no nó Servidor de Administração na guia **Relatórios**.
5. No nó do Servidor de Administração relevante na guia **Relatórios**, selecione o modelo de relatório que foi criado durante as etapas anteriores das instruções.

A geração do relatório começa. O relatório aparece na guia **Relatórios** do nó **Servidor de Administração**.

Você também pode obter as informações sobre se o status de criptografia dos dispositivos e das unidades removíveis estão em conformidade com a política de criptografia ao exibir os painéis de informações na guia **Estatísticas** do nó Servidor de Administração.

Para gerar o relatório sobre o bloqueio de acesso aos dispositivos criptografados:

1. Na árvore do console, selecione o nó com o nome do Servidor de Administração desejado.
2. No espaço de trabalho do nó, selecione a guia **Relatórios**.
3. Clique no botão **Novo modelo de relatório** para iniciar o Assistente de novo modelo de relatório.
4. Siga as instruções do Assistente de novo modelo de relatório. Na janela **Selecionar o tipo de modelo de relatório**, na seção **Outro**, selecione **Relatório de bloqueio de acesso aos arquivos criptografados**.

   Após a conclusão do Assistente de novo modelo de relatório, um novo modelo de relatório aparece no nó **Servidor de Administração** na pasta **Relatórios**.
5. No nó do **Servidor de Administração** na guia **Relatórios**, selecione o modelo de relatório que foi criado durante as etapas anteriores das instruções.

A geração do relatório começa. O relatório aparece na guia **Relatórios** do nó **Servidor de Administração**.

Transmitindo as chave de criptografia entre Servidores de Administração

Quando o recurso de criptografia de dados for ativado em um dispositivo gerenciado, a chave de criptografia é armazenada no Servidor de Administração. A chave de criptografia é usada para acessar dados criptografados e gerenciar a política de criptografia.

A chave de criptografia deve ser transmitida para outro Servidor de Administração nos seguintes casos:

- Você reconfigura o Agente de Rede em um dispositivo gerenciado para atribuir o dispositivo a outro Servidor de Administração. Se esse dispositivo contiver dados criptografados, a chave de criptografia deverá ser transmitida ao Servidor de Administração de destino. Caso contrário, os dados não poderão ser descriptografados.
- Você criptografa uma unidade removível conectada a um dispositivo D1 gerenciado pelo Servidor de Administração S1 e, em seguida, conecta essa unidade removível a um dispositivo D2 gerenciado pelo Servidor de Administração S2. Para acessar os dados na unidade removível, a chave de criptografia deve ser transmitida do Servidor de Administração S1 para o Servidor de Administração S2.
- Você criptografa um arquivo em um dispositivo D1 gerenciado pelo Servidor de Administração S1 e, em seguida, tenta acessar o arquivo em um dispositivo D2 gerenciado pelo Servidor de Administração S2. Para acessar o arquivo, a chave de criptografia deve ser transmitida do Servidor de Administração S1 para o Servidor de Administração S2.

Você pode transmitir chaves de criptografia das seguintes maneiras:

- Automaticamente, ativando a opção **Usar a hierarquia de Servidores de Administração para obter chaves de criptografia** nas propriedades de dois Servidores de Administração entre os quais uma chave de criptografia deve ser transmitida. Se esta opção estiver desativada para um dos Servidores de Administração, a transmissão automática de chaves de criptografia não será possível.

  Ao ativar a opção **Usar a hierarquia de Servidores de Administração para obter chaves de criptografia** nas propriedades de um Servidor de Administração, o Servidor de Administração envia as chaves de criptografia armazenadas no seu repositório para o Servidor de Administração principal (se houver) um nível acima na hierarquia.

  Quando você tenta acessar dados criptografados, o Servidor de Administração primeiro pesquisa a chave de criptografia em seu próprio repositório. Se a opção **Usar a hierarquia de Servidores de Administração para obter chaves de criptografia** estiver ativada e a chave de criptografia necessária não for encontrada no repositório, o Servidor de Administração envia adicionalmente uma solicitação aos Servidores de Administração principais (se houver) para fornecer a chave de criptografia necessária. A solicitação será enviada a todos os Servidores de Administração principais até o servidor no nível mais alto da hierarquia.

A opção **Usar a hierarquia de Servidores de Administração para obter chaves de criptografia** não está disponível atualmente na interface do Web Console. Se você não tiver acesso ao console de administração baseado em MMC, use o Servidor de Administração principal para gerenciar dispositivos criptografados.

- Manualmente, de um Servidor de Administração para outro, exportando e importando o arquivo que contendo as chaves de criptografia.

  A exportação e a importação de chaves de criptografia são ações incluídas no recurso de gerenciamento da chave de criptografia. Para realizar essas ações, configure os direitos de acesso ao recurso para usuários do Kaspersky Security Center da seguinte forma:

  - Conceda o direito de acesso **Leitura** ao recurso de gerenciamento da chave de criptografia para um usuário que exporte chaves de criptografia do Servidor de Administração secundário.

  - Conceda o direito de acesso de **Gravação** ao recurso de gerenciamento da chave de criptografia para um usuário que importe as chaves de criptografia para o Servidor de Administração de destino.

Para ativar a transmissão automática de chaves de criptografia entre Servidores de Administração dentro da hierarquia:

1. Na árvore do console, selecione o Servidor de Administração para o qual você quer ativar a transmissão automática de chaves de criptografia.

2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.

3. Na janela de propriedades, selecione a seção **Algoritmo de criptografia**.

4. Ative a opção **Usar a hierarquia de Servidores de Administração para obter chaves de criptografia**.

5. Clique em **OK** para aplicar as alterações.

As chaves de criptografia serão transmitidas aos Servidores de Administração principais (se houver) na próxima sincronização (a pulsação). Este Servidor de Administração também fornecerá, mediante solicitação, uma chave de criptografia de seu repositório para um Servidor de Administração secundário.

Para transmitir chaves de criptografia entre Servidores de Administração manualmente:

1. Na árvore do console do Servidor de Administração, selecione o Servidor de Administração secundário do qual você deseja transmitir as chaves de criptografia.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades, selecione a seção **Algoritmo de criptografia**.
4. Clique em **Exportar chaves de criptografia do Servidor de Administração**.

   Certifique-se de que um usuário que exporta chaves de criptografia do Servidor receba o direito de acesso **Leitura** ao recurso de gerenciamento da chave de criptografia.
5. Na janela **Exportar chaves de criptografia**:
   - Clique no botão **Procurar** e especifique onde salvar o arquivo.
   - Especifique uma senha para proteger o arquivo contra acesso não autorizado.

     Memorize a senha. Uma senha perdida não pode ser recuperada. Se a senha for perdida, você deverá repetir o procedimento de exportação. Portanto, anote a senha e mantenha-a à mão.
6. Transmitir o arquivo para outro Servidor de Administração, por exemplo, através de uma pasta compartilhada ou unidade removível.
7. No Servidor de Administração de destino, verifique se o Console de Administração do Kaspersky Security Center está em execução.
8. Na árvore do console do Servidor de Administração, selecione o Servidor de Administração de destino para o qual deseja transmitir chaves de criptografia.
9. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
10. Na janela de propriedades, selecione a seção **Algoritmo de criptografia**.
11. Clique em **Importar chaves de criptografia no Servidor de Administração**.

    Verifique e confirme se um usuário que importa as chaves de criptografia para o Servidor recebeu o direito de acesso de **Gravação** ao recurso de gerenciamento da chave de criptografia.
12. Na janela **Importar chaves de criptografia**:
    - Clique no botão **Procurar** e selecione o arquivo contendo as chaves de criptografia.
    - Especifique a senha.
13. Clique em **OK**.

As chaves de criptografia são transmitidas para o Servidor de Administração de destino.

Repositórios de dados

Esta seção fornece informações sobre os dados armazenados no Servidor de Administração e usados para rastrear a condição de dispositivos cliente e para fazer sua manutenção.

A pasta **Repositórios** da árvore do console exibe os dados usados para rastrear o status de dispositivos cliente.

A pasta **Repositórios** contém os seguintes objetos:

- As atualizações baixadas pelo Servidor de Administração que distribuídas para dispositivos cliente
- Lista de equipamentos detectados na rede
- Chaves de licença detectadas em dispositivos cliente
- Arquivos colocados em pastas de Quarentena em dispositivos por aplicativos de segurança
- Arquivos colocados no backup em dispositivos cliente
- Arquivos adiados para uma verificação posterior por aplicativos de segurança

Exportação de uma lista de objetos no repositório para um arquivo de texto

Você pode exportar a lista de objetos do repositório para um arquivo de texto.

Para exportar a lista de objetos do repositório para um arquivo de texto:

1. Na árvore do console, na pasta **Repositórios** selecione a subpasta do repositório relevante.
2. Na subpasta do repositório, selecione **Exportar a lista** no menu de contexto.

   Isso abrirá a janela **Exportar a lista**, na qual você pode especificar o nome do arquivo de texto e o caminho para a pasta onde a mesma foi colocada.

Pacotes de instalação

O Kaspersky Security Center coloca os pacotes de instalação para aplicativos Kaspersky e de outros fornecedores nos repositórios de dados.

Um *pacote de instalação* é um conjunto de arquivos necessários para instalar um aplicativo. Um pacote de instalação contém as configurações iniciais do aplicativo que está sendo instalado.

Se você desejar instalar um aplicativo em um dispositivo cliente, deverá criar um pacote de instalação para aquele aplicativo ou usar um existente. A lista de pacotes de instalação criados está armazenada na pasta **Instalação remota** da árvore do console, a subpasta **Pacotes de instalação**.

Status principais de arquivos no repositório

Os aplicativos de segurança verificam os arquivos nos dispositivos quanto a vírus conhecidos e outros programas que apresentem uma ameaça, atribuir status aos arquivos e colocar alguns deles no repositório.

Por exemplo, os aplicativos de segurança podem fazer o seguinte:

- Salvar uma cópia de um arquivo no repositório antes da exclusão
- Isolar os arquivos provavelmente infectados no repositório

Os status principais dos arquivos são apresentados na tabela abaixo. Você pode obter informações mais detalhadas sobre as ações a empreender em arquivos nos respetivos sistemas de Ajuda de aplicativos de segurança.

Status de arquivos no repositório

Nome do status	Descrição de status
Infectado	O arquivo tem uma seção do código de um vírus ou outro malware conhecido cujas informações são encontradas nos bancos de dados antivírus da Kaspersky.
Não infectado	Nenhum vírus ou outro malware conhecido foi detectado no arquivo.
Advertência	O arquivo contém um fragmento do código que parcialmente coincide com um fragmento do código de uma ameaça conhecida.
Provavelmente infetado	O arquivo contém o código modificado de um vírus conhecido ou o código que se parece com um vírus que ainda não é conhecido à Kaspersky.
Colocado na pasta pelo usuário	O usuário manualmente colocou o arquivo no repositório porque o comportamento do arquivo deu origem à suspeita de que ele contém ameaças. O usuário pode verificar o arquivo quanto a ameaças usando bancos de dados atualizados.
Falso positivo	Um aplicativo Kaspersky atribuiu o status Infectado a um arquivo não-infectado porque o seu código é semelhante àquele de um vírus. Após uma verificação com bancos de dados atualizados, o arquivo é identificado como não infectado.
Desinfectado	O arquivo foi com desinfectado com êxito.
Excluído	O arquivo foi excluído durante o processamento.
Protegido por senha	O arquivo não pode ser processado porque está protegido com uma senha.

Acionamento de regras no modo de Treinamento inteligente

Esta seção fornece informações sobre as detecções realizadas pelas regras do Controle Adaptativo de Anomalias no Kaspersky Endpoint Security for Windows em dispositivos cliente.

As regras detectam e podem bloquear comportamento anômalo nos dispositivos cliente. Se as regras funcionarem no modo de Treinamento Inteligente, elas detectarão o comportamento anômalo e enviarão relatórios sobre cada ocorrência ao Servidor de Administração do Kaspersky Security Center. Esta informação é armazenada como uma lista na subpasta **Acionamento de regras no estado de Treinamento inteligente** da pasta **Repositórios**. Você pode confirmar que as detecções estão corretas ou adicioná-las como exclusões para que esse tipo do comportamento não seja mais considerado como anômalo.

As informações sobre detecções são armazenadas no log de eventos no Servidor de Administração (junto com outros eventos) e no relatório do Controle Adaptativo de Anomalias.

Para mais informações sobre o Controle Adaptativo de Anomalia, as regras, seus modos e status, consulte a Ajuda do Kaspersky Endpoint Security for Windows Help.

Exibir a lista de detecções executadas usando regras do Controle Adaptativo de Anomalias

Para exibir a lista de detecções executadas usando regras do Controle Adaptativo de Anomalias:

1. Na árvore do console, selecione o nó do Servidor de Administração que você necessita.

2. Selecione a subpasta **Acionamento de regras no estado de Treinamento inteligente** (por padrão é a subpasta de **Avançado** → **Repositórios**).

   A lista exibe as seguintes informações sobre as detecções executadas usando regras do Controle Adaptativo de Anomalias:

   - Grupo de administração

     O nome do grupo de administração ao qual o dispositivo pertence.

   - Nome do dispositivo

     O nome do dispositivo cliente onde a regra foi aplicada.

   - Nome

     O nome da regra aplicada.

   - Status

     Excluir – Se o Administrador processou e adicionou este item como uma exclusão às regras. Este status permanecerá até a próxima sincronização do dispositivo cliente com o Servidor de Administração; após a sincronização, o item desaparecerá da lista.

     Confirmar – Se o Administrador processou e confirmou este item. Este status permanecerá até a próxima sincronização do dispositivo cliente com o Servidor de Administração; após a sincronização, o item desaparecerá da lista.

     Vazio – Se o Administrador não processou este item.

   - Total de vezes em que as regras foram acionadas

     O número de detecções incluídas em uma regra heurística, em um processo e em um dispositivo cliente. Este número é contabilizado pelo Kaspersky Endpoint Security.

   - Nome do usuário

     O nome do usuário de dispositivo cliente que executou o processo que gerou a detecção.

   - Caminho do processo de origem

     Caminho até o processo de origem, isto é, até o processo que executa a ação (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

   - Hash do processo de origem

Hash SHA256 do arquivo do processo de origem (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Caminho do objeto de origem**

  Caminho até o objeto que iniciou o processo (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do objeto de origem**

  Hash SHA256 do arquivo de origem (para mais informações, consulte a ajuda do Kaspersky Endpoint Security).

- **Caminho do processo de destino**

  Caminho até o processo de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do processo de destino**

  Hash SHA256 do processo de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Caminho do objeto de destino**

  Caminho até o objeto de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Hash do objeto de destino**

  Hash SHA256 do processo de destino (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security).

- **Processado**

  Data em que a anomalia foi detectada.

Para exibir propriedades de cada elemento de informação:

1. Na árvore do console, selecione o nó do Servidor de Administração que você necessita.
2. Selecione a subpasta **Acionamento de regras no estado de Treinamento inteligente** (por padrão é a subpasta de **Avançado** → **Repositórios**).

3. No espaço de trabalho **Acionamento de regras no estado de Treinamento inteligente**, selecione o objeto desejado.

4. Execute uma das seguintes ações:

   - Clique no link **Propriedades**, na caixa de informações do lado direito da tela.
   - Clique com o botão direito e, no menu de contexto, selecione **Propriedades**.

   A janela de propriedades do objeto se abre, exibindo as informações sobre o elemento selecionado.

Você pode confirmar ou adicionar às exclusões qualquer elemento na lista de detecções das regras do Controle Adaptativo de Anomalias.

Para confirmar um elemento,

Selecione um elemento (ou vários) na lista de detecções e clique no botão **Confirmar**.

O status do(s) elemento(s) será alterado para **Confirmando**.

A sua confirmação contribuirá com a estatística usada pelas regras (para mais informações, consulte a Ajuda do Kaspersky Endpoint Security 11 for Windows).

Para adicionar um elemento como uma exclusão,

Clique com o botão direito em um elemento (ou em vários) na lista de detecções e selecione **Adicionar a exclusões** no menu de contexto.

O assistente para Adicionar exclusão é iniciado. Siga as instruções do assistente.

Se você rejeitar ou confirmar um elemento, ele será excluído da lista de detecções após a próxima sincronização do dispositivo cliente com o Servidor de Administração e não será mais exibido na lista.

Adicionar exclusões a partir das regras do Controle Adaptativo de Anomalias

O Assistente para adicionar exclusão permite que você adicione exclusões das regras do Controle Adaptativo de Anomalias para o Kaspersky Endpoint Security.

Você pode iniciar o assistente por meio de um dos três procedimentos abaixo.

Para iniciar o assistente para Adicionar exclusão através do Controle Adaptativo de Anomalias:

1. Na árvore do console, selecione o nó do Servidor de Administração desejado.

2. Selecione **Acionamento de regras no estado de Treinamento inteligente** (por padrão, é a subpasta de **Avançado → Repositórios**).

3. No espaço de trabalho, clique com o botão direito em um elemento (ou em vários) na lista de detecções e selecione **Adicionar a exclusões**.

   Você pode adicionar até 1.000 exclusões por vez. Se você selecionar mais elementos e tentar adicioná-los às exclusões, uma mensagem de erro será exibida.

O assistente para Adicionar exclusão é iniciado.

Você pode iniciar o Assistente para adicionar exclusão de outros nós na árvore do console:

- A guia **Eventos** da janela principal do Servidor de Administração (então a opção **Pedidos de usuário** ou a opção **Eventos recentes**).

- **Relatório de estado das regras do Controle Adaptável de Anomalias**, coluna **Contagem de detecções**.

Etapa 1. Selecionar o aplicativo

Esta etapa pode ser ignorada se você tiver só uma versão do Kaspersky Endpoint Security for Windows e não tiver outros aplicativos com suporte às regras do Controle Adaptativo de Anomalias.

O Assistente para adicionar exclusão mostra a lista de aplicativos Kaspersky cujos plugins de gerenciamento lhe permitem adicionar exclusões às políticas para esses aplicativos. Selecione um aplicativo desta lista e clique em **Avançar** para prosseguir até a seleção da política à qual a exclusão será adicionada.

Etapa 2. Selecionar a política (políticas)

O assistente mostra a lista de políticas (com perfis da política) para o Kaspersky Endpoint Security.

Selecionar todas as políticas e perfis aos quais você quer adicionar exclusões e clique em **Avançar**.

Etapa 3. Processamento da política (políticas)

O assistente exibe uma barra de andamento à medida que as políticas são processadas. Você pode interromper o processamento das políticas clicando em **Cancelar**.

As políticas herdadas não podem ser atualizadas. Se você não tiver os direitos de modificar uma política, essa política também não será atualizada.

Quando todas as políticas são processadas (ou se você interromper o processamento), um relatório será exibido. Ele mostra quais políticas foram atualizadas com êxito (ícone verde) e quais políticas não foram atualizadas (ícone vermelho).

Essa é a última etapa do assistente. Clique em **Concluir** para fechar o assistente.

Quarentena e Backup

Os aplicativos de antivírus da Kaspersky instalados em dispositivos cliente podem colocar arquivos em Quarentena ou Backup durante a verificação do dispositivo.

Quarentena é um repositório especial que armazena prováveis arquivos infectados com vírus e arquivos que não podem ser desinfectados no momento que são encontrados.

O *Backup* é designado para armazenar cópias backup dos arquivos que foram excluídos ou modificados durante o processo de desinfecção.

O Kaspersky Security Center cria uma lista resumida dos arquivos colocados em Quarentena ou Backup pelos aplicativos Kaspersky nos dispositivos cliente. Os Agentes de Rede em dispositivos cliente transferem as informações sobre os arquivos em Quarentena e Backup para o Servidor de Administração. Você pode usar o Console de Administração para visualizar as propriedades dos arquivos armazenados em repositórios nos dispositivos, executar a verificação de malwares desses repositórios e excluir os arquivos neles armazenados. Os ícones dos status do arquivo são descritos no Apêndice.

O Kaspersky Endpoint Security é compatível com as operações com de Quarentena e Backup.

O Kaspersky Security Center não copia arquivos de repositórios para o Servidor de Administração. Todos os arquivos são armazenados nos repositórios nos dispositivos. Você pode restaurar um arquivo somente no dispositivo com o aplicativo de antivírus, que colocou aquele arquivo no repositório.

Ativar o gerenciamento remoto para arquivos nos repositórios

Por padrão, você não poderá gerenciar os arquivos colocados nos repositórios dos dispositivos cliente.

Para ativar o gerenciamento remoto de arquivos armazenados nos repositórios nos dispositivos cliente:

1. Na árvore do console, selecione um grupo de administração, para o qual você pretende habilitar o gerenciamento remoto de arquivos no repositório.
2. No espaço de trabalho do grupo, abra a guia **Políticas**.
3. Na guia **Políticas**, selecione a política de um aplicativo de segurança que coloca os arquivos nos repositórios dos dispositivos.
4. Na janela de configurações da política, no grupo de configurações **Transferência de dados para o Servidor de Administração**, selecione as caixas de seleção correspondentes aos repositórios para os quais você pretende habilitar o gerenciamento remoto.

   A localização do grupo de configurações **Transferência de dados para o Servidor de Administração** na janela Propriedades da política e os nomes das caixas de seleção dependem do aplicativo de segurança utilizado.

Visualização de propriedades de um arquivo colocado no repositório

Para visualizar as propriedades de um arquivo em Quarentena ou Backup:

1. Na árvore do console, selecione a pasta **Repositórios**, a pasta **Quarentena** ou a subpasta **Backup**.
2. No espaço de trabalho da pasta **Quarentena** (**Backup**), selecione um arquivo, cujas propriedades o usuário pretende visualizar.
3. Selecionando **Propriedades** no menu de contexto do arquivo.

Excluir os arquivos dos repositórios

Para excluir um arquivo de Quarentena ou Backup:

1. Na árvore do console, na pasta **Repositórios**, selecione a subpasta **Quarentena** ou subpasta **Backup**.
2. No espaço de trabalho da pasta **Quarentena** (ou **Backup**), selecione os arquivos que deseja excluir com o uso das teclas **Shift** e **Ctrl**.
3. Exclua os arquivos numa das seguintes formas:
   - Selecionando **Excluir** no menu dos arquivos.
   - Clicando em **Excluir** (**Excluir** se você desejar excluir um arquivo) na caixa de informações para os arquivos selecionados.

Os aplicativos de segurança que colocaram arquivos nos repositórios em dispositivos cliente excluirão os mesmos arquivos destes repositórios.

Restaurar arquivos dos repositórios

Para restaurar um arquivo de Quarentena ou Backup:

1. Na árvore do console, selecione a pasta **Repositórios**, a pasta **Quarentena** ou a subpasta **Backup**.
2. No espaço de trabalho da pasta **Quarentena** (**Backup**), selecione os arquivos que você pretende restaurar usando as teclas **SHIFT** e **CTRL**.
3. Comece restaurando os arquivos em uma das seguintes formas:
   - Selecionando **Restaurar** no menu de contexto dos arquivos.
   - Clicando no link **Restaurar** na caixa de informações para os arquivos selecionados.

Os aplicativos de segurança que colocaram arquivos nos repositórios em dispositivos cliente restaurarão os mesmos arquivos para suas pastas originais.

Salvar um arquivo dos repositórios para o disco

O Kaspersky Security Center lhe permite salvar em disco as cópias de arquivos que foram colocadas por um aplicativo de segurança em Quarentena ou Backup em um dispositivo cliente. Os arquivos são copiados no dispositivo no qual o Kaspersky Security Center estiver instalado, para a pasta especificada.

Para salvar uma cópia do arquivo da Quarentena ou Backup para o disco rígido:

1. Na árvore do console, selecione a pasta **Repositórios**, a pasta **Quarentena** ou a subpasta **Backup**.
2. No espaço de trabalho da pasta **Quarentena** (**Backup**), selecione um arquivo que você pretende copiar para o disco rígido.
3. Inicie a cópia de uma das seguintes formas:
   - Selecionando **Salvar no disco** no menu de contexto do arquivo.
   - Clicando no link **Salvar no disco** na caixa de informações para o arquivo selecionado.

O aplicativo de segurança que colocou o arquivo em Quarentena no dispositivo cliente salvará uma cópia do arquivo na pasta especificada.

Verificação de arquivos em Quarentena

Para verificar os arquivos em quarentena:

1. Na árvore do console, selecione a pasta **Repositórios**, a subpasta **Quarentena**.
2. No espaço de trabalho da pasta **Quarentena**, selecione os arquivos que pretende verificar usando as teclas **`Shift`** e **`Ctrl`**.
3. Inicie o verificação em uma das seguintes formas:
   - Selecionando **Verificar** no menu de contexto do arquivo.
   - Clicando no link **Verificar** na caixa de informações para os arquivos selecionados.

O aplicativo executa a tarefa de verificação sob demanda para os aplicativos de segurança que colocaram os arquivos selecionados na Quarentena nos dispositivos onde esses arquivos estão armazenados.

Ameaças ativas

As informações sobre arquivos não processados encontrados nos dispositivos cliente são armazenadas na pasta **Repositórios**, subpasta **Ameaças ativas**.

O processamento e a desinfeção adiados são executados pelo aplicativo de segurança quando da solicitação ou após que um evento especificado ocorra. Você pode configurar o processamento adiado.

Desinfeção de um arquivo não processado

Para iniciar a desinfeção de um arquivo não processado:

1. Na árvore do console, na pasta **Repositórios** selecione a subpasta **Ameaças ativas**.
2. No espaço de trabalho da pasta **Ameaças ativas**, selecione o arquivo que você tiver desinfectado.
3. Comece desinfectando o arquivo em uma das seguintes formas:
   - Selecionando **Desinfectar** no menu de contexto do arquivo.
   - Clicando no link **Desinfectar** na caixa de informações para o arquivo selecionado.

   A tentativa de desinfetar este arquivo é então realizada.

Se o arquivo estiver desinfectado, o aplicativo de segurança instalado no dispositivo cliente o restaura para sua pasta original. O registro do arquivo é removido da lista na pasta **Ameaças ativas**. Se o arquivo não puder ser desinfectado, o aplicativo de segurança instalado no dispositivo o exclui daquele dispositivo. O registro do arquivo é removido da lista na pasta **Ameaças ativas**.

O recurso de desinfecção e exclusão de arquivos pode variar dependendo de qual aplicativo de segurança está instalado, sua versão e configurações.

Salvar um arquivo não processado no disco

O Kaspersky Security Center permite salvar para o disco as cópias de arquivos não processados encontrados em dispositivos cliente. Os arquivos são copiados no dispositivo no qual o Kaspersky Security Center estiver instalado, para a pasta especificada.

Será possível salvar cópias de arquivos nos seguintes casos:

- Os arquivos foram excluídos ou modificados durante a desinfecção e suas cópias ficaram guardadas no armazenamento do Kaspersky Endpoint Security for Windows no dispositivo gerenciado.
- A opção **Somente registro** está selecionada para o parâmetro **Ação na detecção de ameaças** (**Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**) na política do Kaspersky Endpoint Security.

Para salvar uma cópia de um arquivo não processado para o disco:

1. Na árvore do console, na pasta **Repositórios** selecione a subpasta **Ameaças ativas**.
2. No espaço de trabalho da pasta **Ameaças ativas**, selecione os arquivos que você precisa copiar no disco rígido.
3. Inicie a cópia de uma das seguintes formas:
   - Selecionando **Salvar no disco** no menu de contexto do arquivo.
   - Clicando no link **Salvar no disco** na caixa de informações para o arquivo selecionado.

O aplicativo de segurança instalado no dispositivo cliente, no qual foi encontrado um arquivo não processado, salva uma cópia do arquivo na pasta especificada.

Para excluir um arquivo da pasta "Ameaças ativas"

*Para excluir um arquivo da pasta **Ameaças ativas**:*

1. Na árvore do console, na pasta **Repositórios** selecione a subpasta **Ameaças ativas**.
2. No espaço de trabalho da pasta **Ameaças ativas**, selecione os arquivos que pretende excluir usando as teclas **Shift** e **Ctrl**.
3. Exclua os arquivos numa das seguintes formas:
   - Selecionando **Excluir** no menu dos arquivos.
   - Clicando em **Excluir** (**Excluir** se você desejar excluir um arquivo) na caixa de informações para os arquivos selecionados.

Os aplicativos de segurança que colocaram arquivos nos repositórios em dispositivos cliente excluirão os mesmos arquivos destes repositórios. Os registros do arquivos são removidos da lista na pasta **Ameaças ativas**.

Kaspersky Security Network (KSN)

Essa seção descreve como usar uma infraestrutura de serviços on-line, denominada Kaspersky Security Network (KSN). A seção fornece os detalhes sobre a KSN, assim como instruções sobre como ativar a KSN, configurar o acesso à KSN e visualizar as estatísticas sobre o uso do Servidor proxy da KSN.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Sobre a KSN

A Kaspersky Security Network (KSN) é uma infraestrutura de serviços on-line que fornece o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software. O uso de dados a partir da Kaspersky Security Network garante uma resposta mais rápida dos aplicativos Kaspersky a ameaças, melhora a efetividade de alguns componentes de proteção e reduz o risco de falsos positivos. A KSN permite usar os bancos de dados de reputação da Kaspersky para obter informações sobre os aplicativos instalados nos dispositivos gerenciados.

O Kaspersky Security Center oferece suporte às seguintes soluções de infraestrutura KSN:

- *KSN Global* é uma solução que permite trocar informações com a Kaspersky Security Network. Se você participar da KSN, você concorda em enviar informações à Kaspersky, no modo automático, sobre a operação dos aplicativos Kaspersky instalados nos dispositivos cliente gerenciados por meio do Kaspersky Security Center. As informações são transferidas de acordo com as configurações de acesso da KSN atuais. Os analistas da Kaspersky também averiguam as informações recebidas e as incluem nos bancos de dados estatísticos e de reputação da Kaspersky Security Network. O Kaspersky Security Center usa essa solução por padrão.

- A *KSN Privada* é uma solução que permite aos usuários de dispositivos com aplicativos Kaspersky instalados obter acesso aos bancos de dados de reputação da Kaspersky Security Network, bem como a outros dados estatísticos, sem enviar dados para a KSN de seus próprios computadores. A Kaspersky Private Security Network (KSN Privada) foi projetada para clientes corporativos que não podem participar do Kaspersky Security Network por algum dos seguintes motivos:

  - Os dispositivos do usuário não estão conectados à Internet.

  - A transmissão de quaisquer dados fora do país ou fora da LAN corporativa é proibida pela lei ou limitada por políticas de segurança corporativas.

  Você pode definir configurações de acesso da Kaspersky Private Security Network na seção **Configurações de Proxy da KSN** da janela de propriedades do Servidor de Administração.

O aplicativo solicita a você participar da KSN durante a execução do Assistente de Início Rápido. Você pode iniciar ou parar de usar a KSN em qualquer momento durante o uso do aplicativo.

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração KSN for atualizada, a nova versão será exibida ao atualizar ou fazer upgrade do Servidor de Administração. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Se recusar, continuará usando a KSN de acordo com a versão Declaração KSN aceita anteriormente.

Quando o KSN está habilitado, o Kaspersky Security Center verifica se os servidores da KSN estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos. Isso é necessário para garantir que o nível de segurança seja mantido para os dispositivos gerenciados.

Os dispositivos cliente gerenciados pelo Servidor de Administração interagem com a KSN por meio do servidor proxy da KSN. O servidor proxy da KSN fornece os seguintes recursos:

- Os dispositivos cliente podem enviar solicitações à KSN e transferir informações para a KSN mesmo que não tenham acesso direto à Internet.

- O servidor proxy KSN armazena em cache os dados processados, o que reduz a carga de trabalho no canal de saída e o período de tempo despendido para aguardar por informações solicitadas por um dispositivo cliente.

Você pode configurar o Servidor Proxy KSN na seção **Configurações de Proxy da KSN** da janela Propriedades do Servidor de Administração.

Configurar acesso ao Kaspersky Security Network

Você pode configurar o acesso ao Kaspersky Security Network (KSN) no Servidor de Administração e em um ponto de distribuição.

Para configurar o acesso do Servidor de Administração ao Kaspersky Security Network (KSN):

1. Na árvore do console, selecione o Servidor de Administração para o qual você deseja configurar o acesso à KSN.

2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.

3. Na janela de propriedades do Servidor de Administração, no painel **Seções**, selecione **Proxy da KSN** → **Configurações de Proxy da KSN**.

4. No espaço de trabalho, ative a opção **Usar Servidor de Administração como servidor proxy** para usar o serviço de proxy da KSN.

   Os dados são enviados dos dispositivos cliente para a KSN de acordo com a política do Kaspersky Endpoint Security que estiver ativa naqueles dispositivos cliente. Se essa caixa de seleção estiver desmarcada, nenhum dado será serão enviado a KSN do Servidor de Administração e de dispositivos cliente através do Kaspersky Security Center. No entanto, os dispositivos cliente podem enviar dados para a KSN diretamente (evitando o Kaspersky Security Center), de acordo com suas respectivas configurações. A política do Kaspersky Endpoint Security for Windows, que está ativa nos dispositivos cliente, determina quais dados serão enviados diretamente (evitando o Kaspersky Security Center) pelos dispositivos para a KSN.

5. Ative a opção **Concordo em usar a Kaspersky Security Network**.

   Se essa opção estiver ativada, os dispositivos cliente enviarão os resultados da instalação de patches para a Kaspersky. Ao ativar esta opção, certifique-se de ler e aceitar os termos da Declaração da KSN.

   Se estiver usando a KSN Privada, ative a opção **Configurar KSN Privada** e clique no botão **Selecionar arquivo com config. de proxy da KSN** para baixar as configurações da KSN Privada (arquivos com as extensões pkcs7 e pem). Após as configurações serem baixadas, a interface exibe o nome do provedor e os contatos, assim como a data de criação do arquivo com as configurações da KSN Privada.

   > Ao ativar a KSN Privada, preste atenção aos pontos de distribuição configurados para enviar solicitações da KSN diretamente ao Cloud KSN. Os pontos de distribuição que possuem o Agente de Rede versão 11 (ou anterior) instalado continuarão a enviar solicitações da KSN ao Cloud KSN. Para reconfigurar os pontos de distribuição para enviar solicitações da KSN à KSN Privada, ative a opção **Encaminhar solicitações da KSN para o Servidor de Administração** para cada ponto de distribuição. Você pode ativar esta opção nas propriedades do ponto de distribuição ou na política do Agente de Rede.

   Quando você seleciona a caixa de seleção **Configurar KSN Privada**, uma mensagem aparece com detalhes sobre a KSN Privada.

   Os seguintes aplicativos Kaspersky são compatíveis com a KSN privada:

   - Kaspersky Security Center
   - Kaspersky Endpoint Security for Windows
   - Service Pack 2 do Kaspersky Security for Virtualization 3.0 Agentless
   - Service Pack 1 do Kaspersky Security for Virtualization 3.0 Light Agent

   Se você ativar a opção **Configurar KSN Privada** no Kaspersky Security Center, esses aplicativos receberão informações sobre o suporte na KSN Privada. Na janela de configurações do aplicativo, na subsecção **Kaspersky Security Network** da seção **Proteção Avançada Contra Ameaças**, **Provedor da KSN: KSN Privada** é exibido. Caso contrário, **Provedor da KSN: KSN Global** será exibido.

   > Se você usa versões do aplicativo anteriores ao Service Pack 2 do Kaspersky Security for Virtualization 3.0 Agentless ou anteriores ao Service Pack 1 do Kaspersky Security for Virtualization 3.0 Light Agent ao executar a KSN Privada, recomendamos que você use Servidores de Administração secundários para os quais o uso da KSN Privada não foi ativado.

   > O Kaspersky Security Center não enviará nenhum dado estatístico à Kaspersky Security Network se a KSN Privada estiver configurada na seção **Proxy da KSN → Configurações de Proxy da KSN** da janela Propriedades do Servidor de Administração.

   Se você tiver as configurações do servidor proxy definidas nas propriedades do Servidor de Administração, mas sua arquitetura de rede requer o uso direto da KSN Privada, ative a opção **Ignorar configurações do Servidor Proxy ao conectar à KSN Privada**. Caso contrário, as solicitações dos aplicativos gerenciados não alcançarão a KSN Privada.

6. Configure a conexão do Servidor de Administração ao serviço de proxy da KSN:

   - Em **Configurações de conexão**, para a **Porta TCP**, especifique o número da porta TCP que será usada para se conectar ao Servidor proxy da KSN. A porta padrão para conectar-se ao servidor proxy da KSN é 13111.

   - Se desejar que o Servidor de Administração seja conectado ao servidor proxy da KSN por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de porta para **Porta UDP**. Por padrão, esta opção está desativada e a porta TCP é usada. Se essa opção estiver ativada, a porta UDP padrão para se conectar ao servidor proxy da KSN será 15111.

   - Se quiser que o Servidor de Administração se conecte com o servidor proxy da KSN por meio de uma porta HTTPS, ative a opção **Usar HTTPS via porta** e especifique um número de porta. Por padrão, esta opção está desativada e a porta TCP é usada. Se essa opção estiver ativada, a porta HTTPS padrão para se conectar ao servidor proxy da KSN será 17111.

7. Ative a opção **Conectar Servidores de Administração secundários à KSN através do Servidor de Administração principal**.

   Caso essa opção esteja ativada, os Servidores de Administração secundários de quaisquer níveis de hierarquia usarão o Servidor de Administração principal como servidor proxy da KSN. Se esta opção estiver desativada, os Servidores de Administração secundários conectam-se à KSN por conta própria. Neste caso, os dispositivos gerenciados usam Servidores de Administração secundários como servidores proxy KSN.

   > Os Servidores de Administração secundários usam o Servidor de Administração principal como servidor proxy se, no painel direito da seção **Configurações de Proxy da KSN** nas propriedades do Servidores de Administração secundários, a caixa de seleção **Usar Servidor de Administração como um servidor proxy** estiver marcada.

8. Clique em **OK**.

As configurações de acesso à KSN serão salvas.

Você também pode configurar o acesso ao ponto de distribuição à KSN, por exemplo, se quiser reduzir a carga no Servidor de Administração. O ponto de distribuição que atua como um servidor proxy da KSN envia solicitações da KSN de dispositivos gerenciados para a Kaspersky diretamente, sem usar o Servidor de Administração.

Para configurar o acesso dos pontos de distribuição ao Kaspersky Security Network (KSN):

1. Certifique-se de que o ponto de distribuição seja atribuído manualmente.

2. Na árvore do console, selecione o nó do **Servidor de Administração**.

3. No menu de contexto do Servidor de Administração, selecione **Propriedades**.

4. Na janela de propriedades do Servidor de Administração, selecione a seção **Pontos de distribuição**.

5. Selecione o ponto de distribuição a lista e clique no botão **Propriedades** para abrir sua janela Propriedades.

6. Na janela de propriedades do ponto de distribuição, na seção **Proxy da KSN**, selecione **Acessar a KSN Cloud/KSN Privada diretamente pela internet**.

7. Clique em **OK**.

O ponto de distribuição atuará como um servidor proxy da KSN.

Ativar e desativar a KSN

Para ativar a KSN:

1. Na árvore do console, selecione o Servidor de Administração para o qual você deseja ativar a KSN.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, na seção **Proxy da KSN**, selecione a subseção **Configurações de Proxy da KSN**.
4. Selecione o **Usar Servidor de Administração como um servidor proxy**.

   O serviço de Proxy da KSN será ativado.
5. Marque a caixa de seleção **Concordo em usar a Kaspersky Security Network**.

   A KSN será ativada.

   Se essa caixa de seleção estiver marcada, os dispositivos cliente enviarão os resultados da instalação de patches para a Kaspersky. Ao selecionar essa caixa de seleção, você deve ler e aceitar os termos da Declaração da KSN.
6. Clique em **OK**.

Para desativar a KSN:

1. Na árvore do console, selecione o Servidor de Administração para o qual você deseja ativar a KSN.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, na seção **Proxy da KSN**, selecione a subseção **Configurações de Proxy da KSN**.
4. Desmarque a caixa de seleção **Usar Servidor de Administração como servidor proxy** para desativar o serviço de proxy da KSN ou desmarque a caixa de seleção **Concordo em usar a Kaspersky Security Network**.

   Se essa caixa de seleção estiver desmarcada, os dispositivos cliente não enviarão resultados da instalação de patches para a Kaspersky.

   Se estiver você usando a KSN Privada, desmarque a caixa de seleção **Configurar KSN Privada**.

   A KSN será desativada.
5. Clique em **OK**.

Visualizando a Declaração da KSN aceita

Ao ativar o Kaspersky Security Network (KSN), você deve ler e aceitar a Declaração da KSN. Você pode ver a Declaração da KSN aceita a qualquer momento.

Para visualizar a declaração KSN aceita:

1. Na árvore do console, selecione o Servidor de Administração para o qual você ativou a KSN.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, na seção **Proxy da KSN**, selecione a subseção **Configurações de Proxy da KSN**.
4. Clique no link **Ver declaração da KSN aceita**.

Na janela aberta, você pode ver o texto da Declaração KSN aceita.

Visualizar as estatísticas do Servidor Proxy KSN

O *servidor proxy da KSN* é um serviço que garante a interação entre a infraestrutura da Kaspersky Security Network e os dispositivos cliente gerenciados através do Servidor de Administração.

O uso de um servidor proxy da KSN lhe fornece os seguintes recursos:

- Os dispositivos cliente podem enviar solicitações à KSN e transferir informações para a KSN mesmo que não tenham acesso direto à Internet.
- O servidor proxy KSN armazena em cache os dados processados, o que reduz a carga de trabalho no canal de saída e o período de tempo despendido para aguardar por informações solicitadas por um dispositivo cliente.

Na janela de propriedades do Servidor de Administração, você pode configurar o servidor proxy da KSN e visualizar as estatísticas sobre a utilização do servidor proxy da KSN.

Para visualizar as estatísticas do Servidor proxy da KSN:

1. Na árvore do console, selecione o Servidor de Administração para o qual você deseja visualizar as estatísticas da KSN.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de propriedades do Servidor de Administração, na seção **Proxy da KSN**, selecione a subseção **Estatísticas do Proxy da KSN**.

   Esta seção exibe as estatísticas reais da operação do servidor proxy da KSN (o número de registros de cache, pacotes processados no cache e pacotes recebidos). Além disso, caso o Servidor de Administração esteja conectado à KSN, as mensagens informativas correspondentes serão exibidas.

   Se necessário, execute estas ações adicionais:

   - Clique em **Atualizar** para atualizar as estatísticas sobre o uso do servidor proxy da KSN.
   - Clique no botão **Exportar para arquivo** para exportar as estatísticas para um arquivo CSV.
   - Clique no botão **Verificar conexão do KSN** para verificar se o Servidor de Administração está no momento conectado à KSN.
4. Clique no botão **OK** para fechar a janela Propriedades do Servidor de Administração.

Aceitando uma declaração da KSN atualizada

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração KSN for atualizada, a nova versão será exibida ao atualizar ou fazer upgrade do Servidor de Administração. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Se você recusar a declaração, continuará usando a KSN de acordo com a versão Declaração da KSN aceita anteriormente.

Após atualizar ou atualizar o Servidor de Administração, a declaração da KSN atualizada é exibida automaticamente. Se você recusar a declaração da KSN atualizada, você ainda poderá vê-la e aceitá-la posteriormente.

Para visualizar e aceitar ou recusar uma Declaração da KSN atualizada:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. Na guia **Monitoramento**, na seção **Monitoramento**, clique no link **A Declaração da Kaspersky Security Network é obsoleta**.

   A janela **Declaração da KSN** é aberta.
3. Leia atentamente a Declaração da KSN e, em seguida, faça sua escolha. Se aceitar a declaração da KSN atualizada, clique no botão **Eu aceito os termos do Contrato de Licença**. Se recusar a declaração da KSN atualizada, clique no botão **Cancelar**.

Dependendo da sua escolha, a KSN continuará funcionando de acordo com os termos da Declaração da KSN em vigor ou atualizada. Você pode ver o texto da Declaração da KSN aceita nas propriedades do Servidor de Administração a qualquer momento.

Proteção avançada com a Kaspersky Security Network

A Kaspersky oferece uma camada extra de proteção aos usuários através do Kaspersky Security Network. Esse método de proteção foi concebido para combater as ameaças persistentes e ataques de dia zero. As tecnologias de nuvem integradas e a perícia dos analistas de vírus da Kaspersky fazem do Kaspersky Endpoint Security a escolha perfeita para proteção contra as ameaças de rede mais sofisticadas.

Os detalhes sobre a proteção avançada do Kaspersky Endpoint Security estão disponíveis no site da Kaspersky.

Verificar se o ponto de distribuição funciona como servidor proxy da KSN

Em um dispositivo gerenciado atribuído como ponto de distribuição é possível ativar o servidor proxy da KSN. Um dispositivo gerenciado funciona como servidor proxy da KSN quando o serviço ksnproxy está sendo executado no dispositivo. É possível verificar, ativar ou desativar esse serviço localmente no dispositivo.

Você pode atribuir um dispositivo baseado em Windows ou Linux como um ponto de distribuição. O método de verificação do ponto de distribuição depende de seu sistema operacional.

Para verificar se o ponto de distribuição baseado em Windows funciona como servidor proxy da KSN:

1. No dispositivo de ponto de distribuição, no Windows, abra **Serviços** (**Todos os programas → Ferramentas administrativas → Serviços**).

2. Na lista de serviços, verifique se o serviço ksnproxy está sendo executado.

   Se o serviço ksnproxy estiver em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Se desejar, você pode desativar o serviço ksnproxy. Nesse caso, o Agente de Rede no ponto de distribuição para de participar da Kaspersky Security Network. Isso requer direitos de administrador local.

Para verificar se o ponto de distribuição baseado em Linux funciona como servidor proxy da KSN:

1. No dispositivo do ponto de distribuição, exiba a lista de processos em execução.

2. Na lista de processos em execução, verifique se o processo `/opt/kaspersky/ksc64/sbin/ksnproxy` está em execução.

Caso o processo `/opt/kaspersky/ksc64/sbin/ksnproxy` esteja em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Alternando entre Ajuda On-line e Ajuda Offline

Caso não tenha acesso à Internet, é possível usar a Ajuda offline.

Para alternar entre a ajuda on-line e a ajuda offline:

1. Na janela principal do Kaspersky Security Center, na árvore do console, selecione **Kaspersky Security Center 14.2**.

2. Clique no link **Configurações da interface global**.

   A janela de configurações será aberta.

3. Na janela de configurações, clique em **Usar ajuda offline**.

4. Clique em **OK**.

As configurações são aplicadas e salvas. Caso queira, é possível alterar as configurações e começar a usar a Ajuda on-line a qualquer momento.

Exportação de eventos para os sistemas SIEM

Esta seção explica como exportar eventos registrados pelo Kaspersky Security Center aos sistemas externos de Security Information and Event Management (SIEM).

Configuração da exportação de eventos para sistemas SIEM

O Kaspersky Security Center permite a configuração por um dos seguintes métodos: exportação para qualquer sistema SIEM que use o formato Syslog, exportação para sistemas QRadar, Splunk, ArcSight SIEM que usam formatos LEEF e CEF ou exportação de eventos para sistemas SIEM diretamente do banco de dados do Kaspersky Security Center. Ao concluir este cenário, o Servidor de Administração envia eventos ao sistema SIEM automaticamente.

Pré-requisitos

Antes de iniciar a exportação de configuração de eventos no Kaspersky Security Center:

- Saiba mais sobre os métodos de exportação de eventos.
- Certifique-se de que tem conhecimento dos os valores das configurações do sistema.

> Você pode executar as etapas deste cenário em qualquer ordem.

O processo de exportação de eventos para o sistema SIEM consiste nos seguintes passos:

- **Configurando o sistema SIEM para receber eventos do Kaspersky Security Center**

  Instruções: Configurando a exportação de eventos em um sistema SIEM

- **Selecionando os eventos que deseja exportar para o sistema SIEM:**

  Instruções de como proceder:

  - Console de Administração: Marcando eventos de um aplicativo Kaspersky para exportação em formato Syslog, Marcando eventos gerais para exportação em formato Syslog
  - Kaspersky Security Center Web Console: Marcando eventos de um aplicativo Kaspersky para exportação em formato Syslog, Marcando eventos gerais para exportação em formato Syslog

- **Configurando a exportação de eventos para o sistema SIEM usando um dos seguintes métodos:**

  - Usando TCP/IP, UDP ou TLS via protocolos TCP.

    Instruções de como proceder:

    - Console de Administração: configurando a exportação de eventos para sistemas SIEM
    - Kaspersky Security Center Web Console: configurando a exportação de eventos para sistemas SIEM

  - Usando a exportação de eventos diretamente do banco de dados do Kaspersky Security Center (um conjunto de visualizações públicas é fornecido no banco de dados do Kaspersky Security Center e é possível encontrar a descrição dessas visualizações públicas no documento klakdb.chm).

Resultados

Após configurar a exportação de eventos para o sistema SIEM, você pode ver os resultados de exportação se tiver selecionado eventos que deseja exportar.

Antes de iniciar

Ao configurar uma exportação automática de eventos no Kaspersky Security Center, você deve especificar algumas das configurações do sistema SIEM. Recomenda-se que você verifique estas configurações com antecedência para preparar-se para configurar o Kaspersky Security Center.

Para configurar com êxito o envio automático de eventos a um sistema SIEM, você deve conhecer as seguintes configurações:

- **Endereço do servidor do sistema SIEM**

  O endereço IP do servidor onde o sistema SIEM atualmente usado está instalado. Verifique este valor nas suas configurações de sistema SIEM.

- **Porta do servidor do sistema SIEM**

  O número da porta usada para estabelecer a conexão entre o Kaspersky Security Center e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center e nas configurações do receptor do seu sistema SIEM.

- **Protocolo**

  Protocolo usado para transferir mensagens do Kaspersky Security Center ao seu sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center e nas configurações do receptor do seu sistema SIEM.

Sobre eventos no Kaspersky Security Center

O Kaspersky Security Center lhe permite receber informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nestes dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração. É possível exportar estas informações para sistemas SIEM externos. Exportar informações sobre o evento aos sistemas SIEM externos permite que os administradores de sistemas SIEM respondam prontamente aos eventos de sistema de segurança que ocorrem em dispositivos gerenciados ou em grupos de administração.

Tipos de eventos

No Kaspersky Security Center, há os seguintes tipos de eventos:

- Eventos gerais. Esses eventos ocorrem em todos os aplicativos Kaspersky gerenciados. Um exemplo de um evento geral é um Surto de vírus. Eventos gerais têm sintaxe e semântica estritamente definidas. Eventos gerais são usados, por exemplo, em relatórios e painéis.

- Eventos gerenciados específicos de aplicativos Kaspersky. Cada aplicativo Kaspersky gerenciado tem o seu próprio conjunto de eventos.

Fontes de eventos

Os eventos podem ser gerados pelos seguintes aplicativos:

- Componentes do Kaspersky Security Center:
  - Servidor de Administração
  - Agente de Rede
  - Servidor MDM do iOS
  - Servidor de dispositivos móveis Exchange
- Aplicativos gerenciados pela Kaspersky

  Para obter detalhes sobre os eventos gerados pelos aplicativos gerenciados pela Kaspersky, consulte a documentação do aplicativo correspondente.

É possível visualizar a lista completa dos eventos que podem ser gerados por um aplicativo na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar a lista de eventos nas propriedades do Servidor de Administração.

Nível de importância dos eventos

Cada evento tem o seu próprio nível de importância. Dependendo das condições da sua ocorrência, a um evento pode ser atribuídos diversos níveis de importância. Há quatro níveis de importância de eventos:

- Um *evento crítico* é um evento que indica a ocorrência de um problema crítico que pode levar à perda de dados, um funcionamento operacional ruim ou um erro crítico.

- Uma *falha funcional* é um evento que indica a ocorrência de um problema sério, erro ou funcionamento incorreto que ocorreu durante a operação do aplicativo ou ao executar um procedimento.

- Um *aviso* é um evento que não necessariamente é sério, mas no entanto indica um problema potencial no futuro. A maior parte de eventos são indicados como avisos se o aplicativo puder ser restaurado sem perda dos dados ou capacidades funcionais após a ocorrência de tais eventos.

- Um evento *de informação* é um evento que ocorre para fins de informar sobre conclusão bem sucedida de uma operação, funcionamento apropriado do aplicativo ou conclusão de um procedimento.

Cada evento tem um prazo de armazenamento definido, durante o qual você pode exibi-lo ou modificá-lo no Kaspersky Security Center. Alguns eventos não são salvos no banco de dados do Servidor de Administração por padrão porque o seu prazo de armazenamento definido é zero. Somente os eventos que serão armazenados no banco de dados do Servidor de Administração por ao menos um dia podem ser exportados aos sistemas externos.

Sobre a exportação de evento

Você pode usar a exportação de evento dentro de sistemas centralizados que tratam de questões de segurança em nível organizacional e técnico, que fornecem serviços de monitoramento da segurança e consolidam informações de diferentes soluções. Estes são sistemas SIEM, que fornecem a análise em tempo real de alertas de segurança e eventos gerados por hardware de rede e aplicativos ou Centros de Operação de Segurança (SOCs).

Estes sistemas recebem dados de muitas fontes, incluindo redes, segurança, servidores, bancos de dados e aplicativos. Os sistemas de SIEM também fornecem a funcionalidade para consolidar os dados monitorados para ajudá-lo a evitar faltar a eventos críticos. Além disso, os sistemas executam a análise automatizada de eventos correlacionados e alertas para notificar os administradores de problemas de segurança imediatos. Um alerta pode ser implementado através de um painel ou pode ser enviado por canais de terceiros, tal como por um e-mail.

O processo de exportar eventos do Kaspersky Security Center para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center) e um receptor do evento (sistema SIEM). Para exportar com sucesso eventos, é necessário configurar isso no seu sistema SIEM e no Kaspersky Security Center. Não importa que lado você configura primeiro. Você pode configurar a transmissão de eventos no Kaspersky Security Center e depois configurar o recebimento de eventos pelo sistema SIEM, ou vice-versa.

Métodos para enviar eventos do Kaspersky Security Center

Há três métodos para enviar eventos do Kaspersky Security Center aos sistemas externos:

- Enviando eventos sob o protocolo Syslog à qualquer sistema SIEM

  Usando o protocolo Syslog, você pode encaminhar qualquer evento que ocorre no Servidor de Administração do Kaspersky Security Center e em aplicativos Kaspersky que são instalados em dispositivos gerenciados. O protocolo Syslog é um protocolo de registro de mensagem padrão. É possível usá-lo para exportar os eventos para qualquer sistema SIEM.

  Para isso, é preciso marcar os eventos que deseja retransmitir ao sistema SIEM. É possível marcar os eventos no console de administração ou no Kaspersky Security Center Web Console. Apenas os eventos marcados serão retransmitidos para o sistema SIEM. Caso não tenha marcado nada, nenhum evento será retransmitido.

- Enviando eventos sobre os protocolos CEF e LEEF para os sistemas QRadar, Splunk e ArcSight

  Você pode usar os protocolos CEF e LEEF para exportar eventos gerais. Ao exportar eventos sobre os protocolos CEF e LEEF, você não tem a capacidade de selecionar eventos específicos para exportar. Em vez disso, todos os eventos gerais são exportados. Para converter eventos do Kaspersky Security Center em eventos no formato CEF e LEEF, você precisa usar o arquivo siem_conversion_rules.xml. Esse arquivo contém a lista de atributos de eventos do Kaspersky Security Center e atributos correspondentes de eventos nos formatos CEF e LEEF. Além disso, o arquivo siem_conversion_rules.xml contém as regras para gerar mensagens correspondentes aos eventos. Esse arquivo está incluído no kit de distribuição do Kaspersky Security Center.

  Diferentemente do protocolo Syslog, os protocolos CEF e LEEF não são universais. CEF e LEEF são destinados para os sistemas SIEM apropriados (QRadar, Splunk e ArcSight). Portanto, quando você escolhe exportar eventos através de um desses protocolos, você usa o analisador necessário no sistema SIEM.

- Diretamente do banco de dados do Kaspersky Security Center para qualquer sistema SIEM

  Este método de exportar eventos pode ser usado para receber eventos diretamente das vistas públicas do banco de dados por meio de consultas SQL. Os resultados de uma consulta são salvos em um arquivo XML que pode ser usado como dados de entrada para um sistema externo. Somente os eventos disponíveis nas vistas públicas podem ser exportados diretamente do banco de dados.

Recebimento de eventos pelo sistema SIEM

O sistema SIEM deve receber e corretamente analisar os eventos recebidos do Kaspersky Security Center. Para estes propósitos, você deve configurar apropriadamente o sistema SIEM. A configuração depende do sistema SIEM específico utilizado. No entanto, há um número de etapas gerais na configuração de todos os sistemas SIEM, tal como a configuração do receptor e do analisador.

Sobre a configuração de exportação de eventos em um sistema SIEM

O processo de exportar eventos do Kaspersky Security Center para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center) e um receptor do evento (sistema SIEM). Você deve configurar a exportação de eventos no seu sistema SIEM e no Kaspersky Security Center.

As configurações especificadas no sistema SIEM dependem de qual sistema que você estiver usando. Normalmente, para todos os sistemas SIEM você deve definir um receptor e, opcionalmente, um analisador de mensagem para analisar os eventos recebidos.

Configurar o receptor

Para poder receber eventos enviados pelo Kaspersky Security Center, configure o receptor no seu sistema SIEM. Em geral, as seguintes configurações devem ser especificadas no sistema SIEM:

- **Protocolo para exportar ou tipo de entrada**

  É o protocolo de transferência de mensagem, TCP/IP ou UDP. Este protocolo deve ser o mesmo protocolo que você especificou no Kaspersky Security Center.

- **Porta**

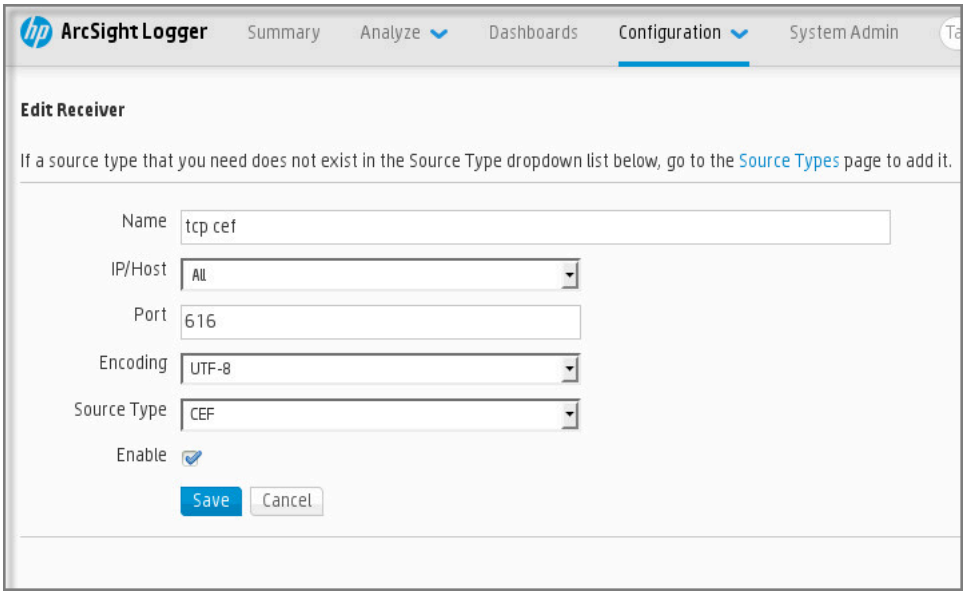
  Número da porta para conectar-se ao Kaspersky Security Center. Esta porta deve ser a mesma que a porta que você especificou no Kaspersky Security Center.

- **Protocolo de mensagem ou tipo de origem**

  O protocolo usado para exportar eventos ao sistema SIEM. Pode ser um dos protocolos padrão: Syslog, CEF ou LEEF. O sistema SIEM seleciona o analisador de mensagem de acordo com o protocolo que você especifica.

Dependendo do sistema SIEM usado, você pode ter que especificar algumas configurações adicionais de receptor.

A figura abaixo mostra tela de configuração de receptor no ArcSight.



Configuração do receptor no ArcSight

Analisador de mensagem

Os eventos exportados são passados aos sistemas SIEM como mensagens. Estas mensagens devem ser apropriadamente analisadas para que as informações nos eventos possam ser usadas pelo sistema SIEM. Os analisadores de mensagem são uma parte do sistema SIEM; eles são usados para dividir o conteúdo da mensagem em campos relevantes, como ID do evento, gravidade, descrição e parâmetros. Isto ativa o sistema SIEM para processar eventos recebidos do Kaspersky Security Center para que eles possam ser armazenados no banco de dados do sistema SIEM.

Marcando eventos para exportação para sistemas SIEM em formato Syslog

Após ativar a exportação automática de eventos, você deve selecionar quais eventos serão exportados ao sistema SIEM externo.

Você pode configurar a exportação de eventos em formato Syslog para um sistema externo com base em uma das seguintes condições:

- Marcando eventos gerais. Se você marcar eventos para exportar em uma política, nas configurações de um evento ou no Servidor de Administração, o sistema SIEM receberá os eventos marcados que ocorreram em todos os aplicativos gerenciados pela política específica. Se os eventos exportados foram selecionados na política, você não será capaz de redefini-los para um aplicativo individual gerenciado por esta política.

- Marcando eventos para um aplicativo individual. Se você marcar eventos para exportar para um aplicativo gerenciado instalado em um dispositivo gerenciado, o sistema SIEM somente receberá os eventos que ocorreram neste aplicativo.

Sobre a marcação de eventos para exportação para o sistema SIEM no formato Syslog

Após ativar a exportação automática de eventos, você deve selecionar quais eventos serão exportados ao sistema SIEM externo.

Você pode configurar a exportação de eventos em formato Syslog para um sistema externo com base em uma das seguintes condições:

- Marcando eventos gerais. Se você marcar eventos para exportar em uma política, nas configurações de um evento ou no Servidor de Administração, o sistema SIEM receberá os eventos marcados que ocorreram em todos os aplicativos gerenciados pela política específica. Se os eventos exportados foram selecionados na política, você não será capaz de redefini-los para um aplicativo individual gerenciado por esta política.

- Marcando eventos para um aplicativo individual. Se você marcar eventos para exportar para um aplicativo gerenciado instalado em um dispositivo gerenciado, o sistema SIEM somente receberá os eventos que ocorreram neste aplicativo.

Marcando eventos de um aplicativo Kaspersky para exportação em formato Syslog

Se desejar exportar eventos ocorridos em um aplicativo gerenciado individual instalado em um dispositivo gerenciado, marque os eventos para exportar para o aplicativo. Se os eventos anteriormente exportados foram marcados na política, você não será capaz de redefinir os eventos marcados de um aplicativo individual gerenciado por esta política.

Para marcar os eventos para exportação para um aplicativo gerenciado individual:

1. Na árvore do console do Kaspersky Security Center, selecione o nó **Dispositivos gerenciados** e siga para a guia **Dispositivos**.

2. Clique com o botão direito do mouse para abrir o menu de contexto do dispositivo relevante e selecione **Propriedades**.

3. Na janela de propriedades do dispositivo que será aberta, selecione a seção **Aplicativos**.

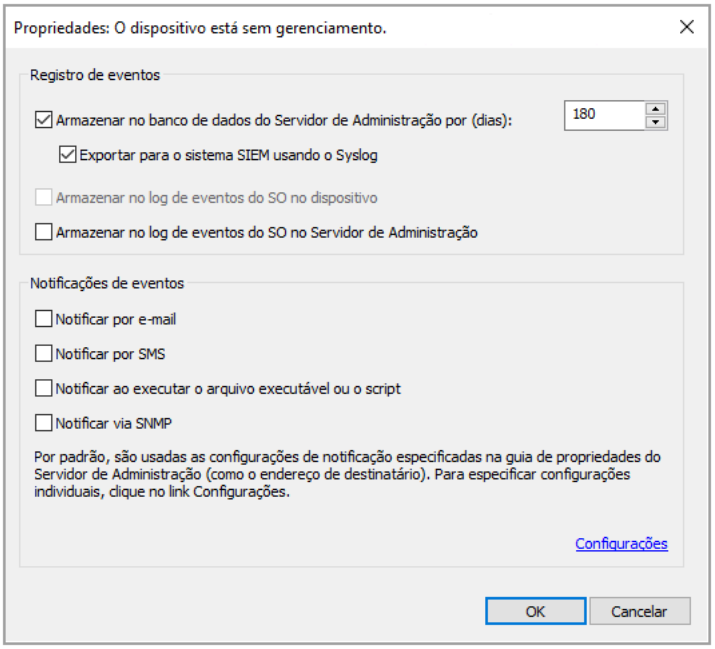
4. Na lista de aplicativos que aparece, selecione o aplicativo cujos eventos você precisa exportar e clique no botão **Propriedades**.

5. Na janela de propriedades do aplicativo, selecione a seção **Configuração de eventos**.

6. Na lista de eventos que aparece, selecione um ou diversos eventos que têm de ser exportados ao sistema SIEM, e clique no botão **Propriedades**.

7. Na janela de propriedades do evento, selecione a caixa de seleção **Exportar para o sistema SIEM usando o Syslog** para marcar os eventos selecionados para exportação no formato Syslog. Desmarque a caixa de seleção **Exportar para o sistema SIEM usando o Syslog** para desmarcar os eventos selecionados para exportação no formato Syslog.

   Se as propriedades do evento forem definidas em uma política, os campos desta janela não podem ser editados.



Janela Propriedades de evento

8. Clique em **OK** para salvar as alterações.

9. Clique em **OK** na janela Propriedades do aplicativo e na janela Propriedades do dispositivo.

Os eventos marcados serão enviados ao sistema SIEM através do formato Syslog. Os eventos para os quais você desmarcou a caixa de seleção **Exportar para o sistema SIEM usando o Syslog** não serão exportados para um sistema SIEM. A exportação iniciará imediatamente após a ativação da exportação automática e selecionar os eventos para exportar. Configure o sistema SIEM para assegurar que ele possa receber eventos do Kaspersky Security Center.

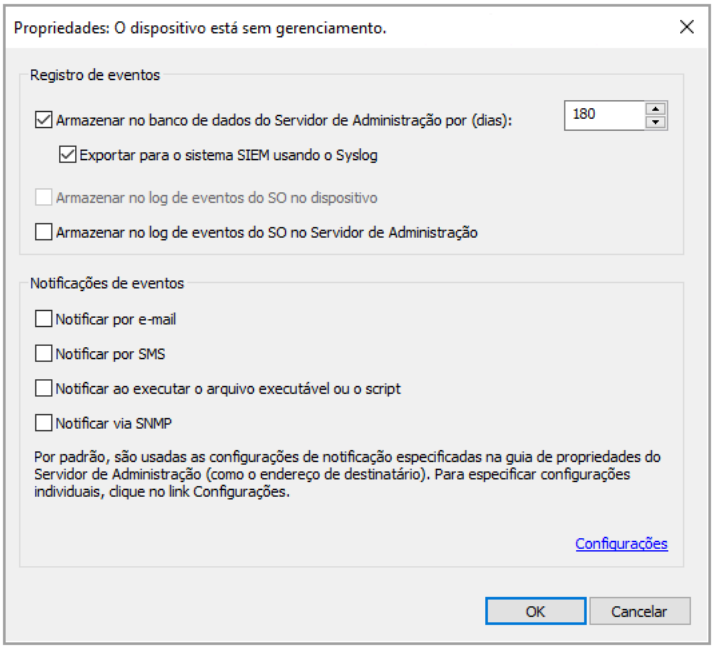
Marcando eventos gerais para exportação no formato Syslog

Se desejar exportar eventos que ocorreram em todos os aplicativos gerenciados por uma política específica, marque os eventos para exportar na política. Neste caso, você não poderá marcar eventos para um aplicativo gerenciado individual.

Para configurar eventos gerais para um sistema SIEM:

1. No árvore do console do Kaspersky Security Center, selecione o nó **Políticas**.
2. Clique com o botão direito do mouse para abrir o menu de contexto da política relevante e selecione **Propriedades**.
3. Na janela de propriedades da política que se abre, selecione a seção **Configuração de eventos**.
4. Na lista de eventos que aparece, selecione um ou diversos eventos que têm de ser exportados ao sistema SIEM, e clique no botão **Propriedades**.

   Se você precisar selecionar todos os eventos, clique no botão **Selecionar tudo**.
5. Na janela de propriedades do evento, selecione a caixa de seleção **Exportar para o sistema SIEM usando o Syslog** para marcar os eventos selecionados para exportação no formato Syslog. Desmarque a caixa de seleção **Exportar para o sistema SIEM usando o Syslog** para desmarcar os eventos selecionados para exportação no formato Syslog.



Janela Propriedades do evento do Servidor de Administração

6. Clique em **OK** para salvar as alterações.
7. Na janela de propriedades da política, clique em **OK**.

Os eventos marcados serão enviados ao sistema SIEM através do formato Syslog. Os eventos para os quais você desmarcou a caixa de seleção **Exportar para o sistema SIEM usando o Syslog** não serão exportados para um sistema SIEM. A exportação iniciará imediatamente após a ativação da exportação automática e selecionar os eventos para exportar. Configure o sistema SIEM para assegurar que ele possa receber eventos do Kaspersky Security Center.

Sobre a exportação de eventos usando o formato Syslog

Você pode usar o formato Syslog para exportar aos sistemas SIEM os eventos que ocorrem no Servidor de Administração e em outros aplicativos Kaspersky instalados em dispositivos gerenciados.

Syslog é um padrão para o protocolo de registro da mensagem. Isso permite a separação do software que gera mensagens, o sistema que as armazena e o software que os reporta e os analisa. Cada mensagem é legendada com um código de instalação, indicando o tipo de software que gera a mensagem e à mesma é atribuído um nível de gravidade.

O formato Syslog é definido por documentos de Solicitação de Comentários (RFC) publicados pela Internet Engineering Task Force (padrões da Internet). O padrão RFC 5424 é usado para exportar os eventos do Kaspersky Security Center aos sistemas externos.

No Kaspersky Security Center, você pode configurar a exportação dos eventos aos sistemas externos usando o formato Syslog.

O processo de exportação consistem em duas etapas:

1. Ativar a exportação automática do evento. Nesta etapa, o Kaspersky Security Center é configurado para que ele envie eventos ao sistema SIEM. O Kaspersky Security Center começa a enviar eventos imediatamente após você ativar a exportação automática.

2. Selecionar os eventos a ser exportados ao sistema externo. Nesta etapa, você seleciona qual evento exportar ao sistema SIEM.

Sobre a exportação de eventos usando formatos CEF e LEEF

Você pode usar os formatos CEF e LEEF para exportar eventos gerais, bem como eventos transferidos pelos aplicativos Kaspersky para o Servidor de Administração. O conjunto de eventos exportado é predefinido, e você não pode selecionar os eventos a ser exportados. Antes de enviar eventos para o sistema SIEM (QRadar, ArcSight ou Splunk), é necessário interpretar os eventos do Kaspersky Security Center para eventos no formato CEF e LEEF com o uso das regras especificadas no arquivo siem_conversion_rules.xml.

Selecione o formato de exportação com base no sistema SIEM usado. A tabela abaixo mostra os sistemas SIEM e os formatos de exportação correspondentes.

Formatos da exportação de eventos para um sistema SIEM

SIEM system	Formato de exportação
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Formato Estendido de Evento de Log) – Um formato de evento customizado para o IBM Security QRadar SIEM. O QRadar pode integrar, identificar e processar eventos LEEF. Os eventos de LEEF devem usar a codificação de caractere UTF-8. Você pode encontrar as informações detalhadas sobre o protocolo LEEF no IBM Knowledge Center.

- CEF (Formato de Evento Comum) – Um padrão de gerenciamento de registro aberto que aprimora a interoperabilidade da informação relativa a segurança de diferentes dispositivos de segurança e de rede e aplicativos. O CEF lhe permite usar um formato de registro de evento comum para que os dados possam ser facilmente integrados e agregados para a análise por um sistema de gerenciamento corporativo. Os eventos de CEF devem usar a codificação de caractere UTF-8.

A exportação automática significa que o Kaspersky Security Center envie eventos gerais ao sistema SIEM. A exportação automática de eventos inicia imediatamente após você a ativar. Esta seção explica detalhadamente como ativar a exportação automática de eventos.

Conversão de eventos para o formato CEF ou LEEF

Antes de enviar eventos para o sistema SIEM (QRadar, ArcSight ou Splunk), é necessário interpretar os eventos do Kaspersky Security Center para eventos no formato CEF e LEEF com o uso das regras especificadas no arquivo siem_conversion_rules.xml. Esse arquivo está incluído no kit de distribuição do Kaspersky Security Center.

O arquivo siem_conversion_rules.xml contém as regras de interpretação predefinidas para converter eventos para o formato CEF e LEEF. Caso queira usar regras adicionais de interpretação de eventos, é possível adicioná-las manualmente ao arquivo.

O arquivo siem_conversion_rules.xml inclui as seções `<product name="SP_QRADAR" vendor="IBM">` e `<product name="SP_QRADAR" vendor="IBM">`. A seção `<product name="SP_QRADAR" vendor="IBM">` contém regras para gerar eventos no formato LEEF que podem ser exportados para o sistema QRadar SIEM. A seção `<product name="SP_ARCSIGHT" vendor="HP">` contém regras para gerar eventos no formato CEF que podem ser exportados para o sistema ArcSight ou Splunk SIEM.

Cada seção tem a subseção `<comum>`, na qual estão localizados os atributos de eventos da Kaspersky Security Center e os atributos correspondentes dos eventos no formato LEEF. Esses atributos comuns são usados para todos os tipos de eventos que podem ser exportados.

Além disso, cada seção tem subseções `<event>`. Cada subseção de `<evento>` contém atributos adicionais que são adicionados àqueles listados na seção `<comum>`.

É possível adicionar manualmente uma nova regra de geração de eventos ao arquivo siem_conversion_rules.xml.

Para adicionar uma nova regra de geração de eventos:

1. Adicionar uma nova subseção `<event>` na seção `<product name="SP_QRADAR" vendor="IBM">` ou `<product name="SP_QRADAR" vendor="IBM">` e, em seguida, especifique os atributos de evento adicionais, caso necessário.

2. Caso um evento consista apenas em atributos comuns, a subseção `<evento>` estará vazia.

siem_conversion_rules.xml

```
<conversion_rules>
    <product name="SP_QRADAR" vendor="IBM">
        <common> <!-- Common Kaspersky Security Center event attributes and corresponding LEEF event attributes --
>
            <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"> <!-- Regra de geração para o evento GNRL_EV_VIRUS_FOUND com atributos
adicionais -->
            <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> <!-- Atributos comuns de eventos do Kaspersky Security Center e atributos de eventos LEEF
correspondentes -->
            <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>
```

Configurando o Kaspersky Security Center para exportação de eventos para o sistema SIEM

Você pode ativar a exportação automática de eventos no Kaspersky Security Center.

Somente os eventos gerais podem ser exportados de aplicativos gerenciados através dos formatos CEF e LEEF. As regras de interpretação usadas para converter eventos nos formatos CEF e LEEF são especificadas no arquivo siem_conversion_rules.xml incluído no kit de distribuição do Kaspersky Security Center. Os eventos específicos para um aplicativo não podem ser exportados de aplicativos gerenciados através dos formatos CEF e LEEF. Se tiver de exportar eventos de aplicativos gerenciados ou de um conjunto personalizado de eventos configurado usando as políticas de aplicativos gerenciados, exporte os eventos através do formato Syslog.

Para ativar a exportação automática de eventos:

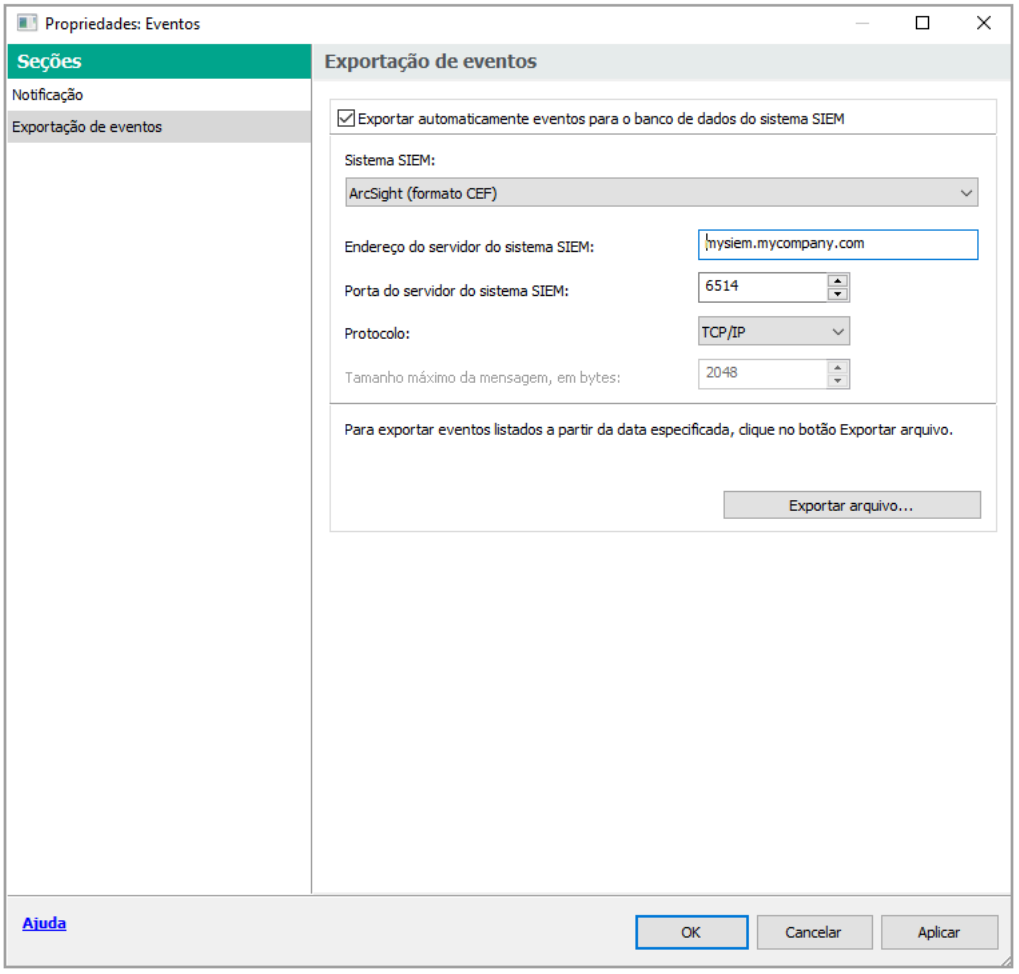
1. Na árvore do console do Kaspersky Security Center, selecione o Servidor de Administração cujos eventos você quer exportar.

2. No espaço de trabalho do Servidor de Administração selecionado, clique na guia **Eventos**.

3. Clique na seta suspensa junto ao link **Configurar notificações e exportação de eventos** e selecione **Configurar a exportação para o sistema SIEM** na lista suspensa.

   A janela Propriedades de eventos é aberta, exibindo a seção **Exportação de eventos**.

4. Na seção **Exportação de eventos**, especifique as seguintes configurações de exportação:



Seção Exportação de eventos da janela Propriedades do evento

- **Exportar automaticamente eventos para o banco de dados do sistema SIEM**

  Selecione esta caixa de seleção para ativar a exportação automática de eventos para sistemas SIEM. A seleção desta caixa de seleção ativa todos os campos na seção **Exportando eventos**.

- **Sistema SIEM**

  Selecione o sistema SIEM para exportar eventos: QRadar (formato LEEF), ArcSight (formato CEF), Splunk (formato CEF) e formato Syslog (RFC 5424).

  Se selecionar o formato Syslog, você deve especificar:

  Tamanho máximo da mensagem, em bytes

  Especifique o tamanho máximo (em bytes) de uma mensagem encaminhada ao sistema SIEM. Cada evento é encaminhado em uma mensagem. Se o comprimento real de uma mensagem exceder o valor especificado, a mensagem é truncada e os dados podem ser perdidos. O tamanho padrão é de 2.048 bytes. Este campo somente está disponível se você selecionou o formato Syslog no campo **Sistema SIEM**.

- **Endereço do servidor do sistema SIEM**

Especifique o endereço do servidor do sistema SIEM. O endereço pode ser especificado como um nome DNS ou NetBIOS ou como um endereço IP.

- **Porta do servidor do sistema SIEM**

  Especifique o número da porta usada para conectar-se ao servidor do sistema SIEM. Este número de porta deve ser o mesmo que este, que o seu sistema SIEM usa para receber os eventos (consulte a seção Configuração de um sistema SIEM para obter detalhes).

- **Protocolo**

Selecione o protocolo a ser usado para transferir mensagens para o sistema SIEM. Você pode selecionar o TCP/IP, UDP ou TLS sobre protocolo TCP.

Especifique as seguintes configurações de TLS se selecionar o protocolo TLS sobre TCP:

- **Autenticação do servidor SIEM**

  Escolha uma das seguintes maneiras de autenticar o servidor do sistema SIEM:

  - **Ao usar certificados CA**. Você pode receber um arquivo com uma lista de certificados de uma autoridade de certificação (CA) confiável e carregá-lo para o Kaspersky Security Center. O Kaspersky Security Center verifica se o certificado do servidor do sistema SIEM também é assinado por uma CA confiável.

    Para adicionar um certificado confiável, clique no botão **Procurar** e, em seguida, carregue o certificado.

    Se você selecionar a opção **Ao usar certificados CA**, você poderá especificar nomes de assunto no campo **Assuntos dos certificados do servidor (opcional)**. *Nome do assunto* é um nome de domínio para o qual o certificado foi recebido. O Kaspersky Security Center não pode se conectar ao servidor do sistema SIEM se o nome de domínio do servidor do sistema SIEM não corresponder ao nome da entidade do certificado do servidor do sistema SIEM. No entanto, o servidor do sistema SIEM poderá alterar seu nome de domínio se você mudar o nome do assunto no certificado. Para fazer isso, especifique os nomes dos assuntos no campo **Assuntos dos certificados do servidor (opcional)**. Se qualquer um dos nomes de assunto especificados corresponder ao nome do assunto do certificado do sistema SIEM, o Kaspersky Security Center valida o certificado do servidor do sistema SIEM.

  - **Ao usar impressões& digitais SHA-1 dos certificados do servidor**. Você pode especificar as impressões digitais SHA-1 dos certificados do sistema SIEM no Kaspersky Security Center. Para adicionar uma impressão digital SHA-1, insira-a no campo abaixo da opção.

- **Autenticação do cliente**

  Para autenticação de cliente, você pode inserir o seu certificado ou gerá-lo no Kaspersky Security Center.

  - **Inserir certificado**. Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer CA confiável. Para inserir um certificado existente, clique no botão **Procurar por certificado**. Na janela aberta **Certificado**, escolha um dos seguintes tipos de certificado e especifique o certificado e sua chave privada:

    - **Certificado X.509**. Carregue um arquivo com uma chave privada no campo **Chave privada (*.prk, *.pem)** e um arquivo com um certificado no campo **Certificado (*.cer)**. Para fazer isso, clique no botão **Procurar** à direita do campo correspondente e, em seguida, adicione o arquivo necessário. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Depois de carregar ambos os arquivos, especifique a senha para decodificar a chave privada no campo **Senha**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

    - **Contêiner PKCS#12**. Carregue um único arquivo que contenha um certificado e sua chave privada no campo **Arquivo de certificado**. Para fazer isso, clique no botão **Procurar** à direita do campo e, em seguida, adicione o arquivo necessário. Depois de carregar o arquivo, especifique a senha para decodificar a chave privada no campo **Senha**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

  - **Gerar chave**. Você pode gerar um certificado autoassinado no Kaspersky Security Center. Clique no botão **Gerar certificado** e, em seguida, digite um nome de assunto no campo **Assunto**. O certificado do cliente é gerado para este nome de assunto e a impressão digital SHA-1 deste certificado é exibida no campo **Impressão digital SHA-1 do certificado do cliente**. Como resultado, o Kaspersky Security Center armazena o certificado autoassinado gerado e você pode passar a parte pública do certificado ou a impressão digital SHA-1 para o sistema SIEM.

5. Se você desejar exportar ao banco de dados do sistema SIEM os eventos que ocorreram após uma data especificada no passado, clique no botão **Exportar arquivo** e especifique a data inicial para a exportação do evento. Por padrão, a exportação do evento inicia imediatamente após você ativá-la.

6. Clique em **OK**.

A exportação automática dos eventos está ativada.

Após ativar a exportação automática de eventos, você deve selecionar quais eventos serão exportados ao sistema SIEM.

Exportando eventos diretamente do banco de dados

Você pode recuperar eventos diretamente do banco de dados do Kaspersky Security Center sem ter necessidade de usar a interface Kaspersky Security Center. Você pode consultar as vistas públicas diretamente e recuperar os dados de evento, ou ainda criar as suas próprias vistas com base em vistas públicas existentes e endereçá-las para receber os dados de que precisa.

Vistas públicas

Para a sua conveniência, um conjunto de vistas públicas é fornecido no banco de dados do Kaspersky Security Center. Você pode encontrar a descrição dessas visualizações públicas no documento klakdb.chm.

A vista pública v_akpub_ev_event contém um conjunto de campos que representa os parâmetros de evento no banco de dados. No documento klakdb.chm você também pode encontrar informações sobre vistas públicas que correspondem a outras entidades do Kaspersky Security Center, por exemplo, dispositivos, aplicativos ou usuários. Você pode usar estas informações nas suas consultas.

Esta seção contém instruções para executar uma consulta SQL por meio do utilitário klsql2 e um exemplo de consulta.

Para criar consultas SQL ou vistas do banco de dados, você também pode usar qualquer outro programa para trabalhar com bancos de dados. As informações sobre como exibir os parâmetros para conectar-se ao banco de dados do Kaspersky Security Center, como o nome da instância e o nome do banco de dados, são fornecidas na seção correspondente.

Executar uma consulta SQL usando o utilitário klsql2

Este artigo descreve como baixar e usar o utilitário klsql2 e como executar uma consulta SQL usando esse utilitário.

Para usar o utilitário klsql2:

1. Localize o utilitário klsql2 na pasta de instalação do Kaspersky Security Center. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Não use versões do utilitário klsql2 destinadas a versões mais antigas do Kaspersky Security Center.

2. Crie um arquivo com a extensão .sql em qualquer editor de texto e coloque o arquivo na mesma pasta do utilitário.

3. No arquivo .sql criado, digite a consulta SQL desejada e salve o arquivo.

4. No dispositivo com o Servidor de Administração do Kaspersky Security Center instalado, na linha de comando, digite o seguinte comando para executar a consulta SQL do arquivo .sql e salve os resultados no arquivo result.xml:

   ```
   klsql2 -i src.sql -u <nome de usuário> -p <senha> -o result.xml
   ```

   onde `<nome de usuário>` e `<senha>` são as credenciais da conta de usuário que tem acesso ao banco de dados.

5. Caso seja necessário, digite o login e a senha da conta de usuário que tem acesso ao banco de dados.

6. Abra os arquivos result.xml criados recentemente para exibir os resultados da consulta SQL.

É possível editar o arquivo .sql e criar qualquer consulta SQL para as visualizações públicas. Então, a partir da linha de comando, execute a consulta SQL e salve os resultados em um arquivo.

Exemplo de uma consulta SQL no utilitário klsql2

Esta seção mostra um exemplo de uma consulta SQL, executada por meio do utilitário klsql2.

O exemplo a seguir ilustra a recuperação dos eventos que ocorreram em dispositivos durante os últimos sete dias e exibe os eventos ordenados pelo horário em que ocorreram. Os eventos mais recentes são exibidos primeiro.

Exemplo:

```
SELECT

/* identificador do evento */
e.nId,

/* hora em que o evento ocorreu */
e.tmRiseTime,

/* nome interno do tipo de evento */
e.strEventType,

/* nome exibido do evento */
e.wstrEventTypeDisplayName,

/* descrição do evento exibida */
e.wstrDescription,

/* nome do grupo onde o dispositivo está localizado */
e.wstrGroupName,

/* nome exibido do dispositivo no qual o evento ocorreu */
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)) + '.' +

/* endereço IP do dispositivo no qual o evento ocorreu */
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
```

Exibir o nome de banco de dados do Kaspersky Security Center

Pode ser útil saber o nome de um banco de dados se você precisar, por exemplo, enviar uma consulta SQL e conectar-se ao banco de dados de seu editor de script SQL.

Para exibir o nome do banco de dados do Kaspersky Security Center:

1. Na árvore do console do Kaspersky Security Center, abra o menu de contexto da pasta **Servidor de Administração** e selecione **Propriedades**.

2. Na janela de propriedades do Servidor de Administração, no painel Seções, selecione **Avançado** e, a seguir, **Detalhes do banco de dados atual**.

3. Na seção **Detalhes do banco de dados atual**, observe as seguintes propriedades do banco de dados (veja a figura abaixo):

- **Nome de instância**

  Nome da instância atual do banco de dados do Kaspersky Security Center. O valor padrão é *.\KAV_CS_ADMIN_KIT*.

- **Nome do banco de dados**

  Nome do banco de dados SQL do Kaspersky Security Center. O valor padrão é *KAV*.

- **Espaço alocado para o banco de dados do Kaspersky Security Center**

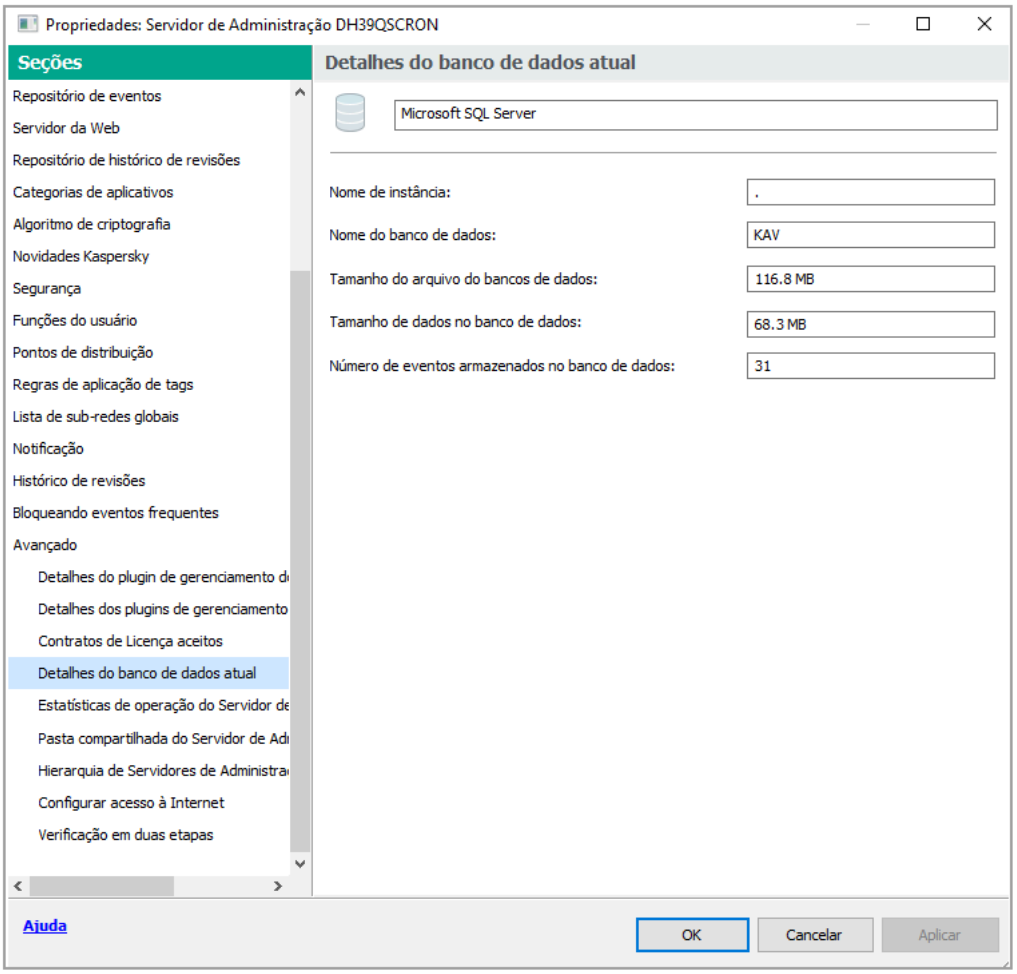
  O tamanho do arquivo do banco de dados. Se quiser limpar dados desnecessários, configure a compactação do banco de dados usando a tarefa *Manutenção do Servidor de Administração*.

- **Tamanho dos dados no banco de dados inteiro**

  O tamanho real dos dados usados atualmente no DBMS. O artigo a seguir descreve como diagnosticar o DBMS: O tamanho do banco de dados excede o limite.

- **Número de eventos armazenados no banco de dados**

O número de eventos atualmente armazenados no DBMS. Consulte o artigo a seguir para obter detalhes: Processamento e armazenamento de eventos.



Seção com informações sobre o banco de dados de Servidor de administração atual

4. Clique no botão **OK** para fechar a janela Propriedades do Servidor de Administração.

Use o nome do banco de dados para endereçar o banco de dados nas suas consultas SQL.

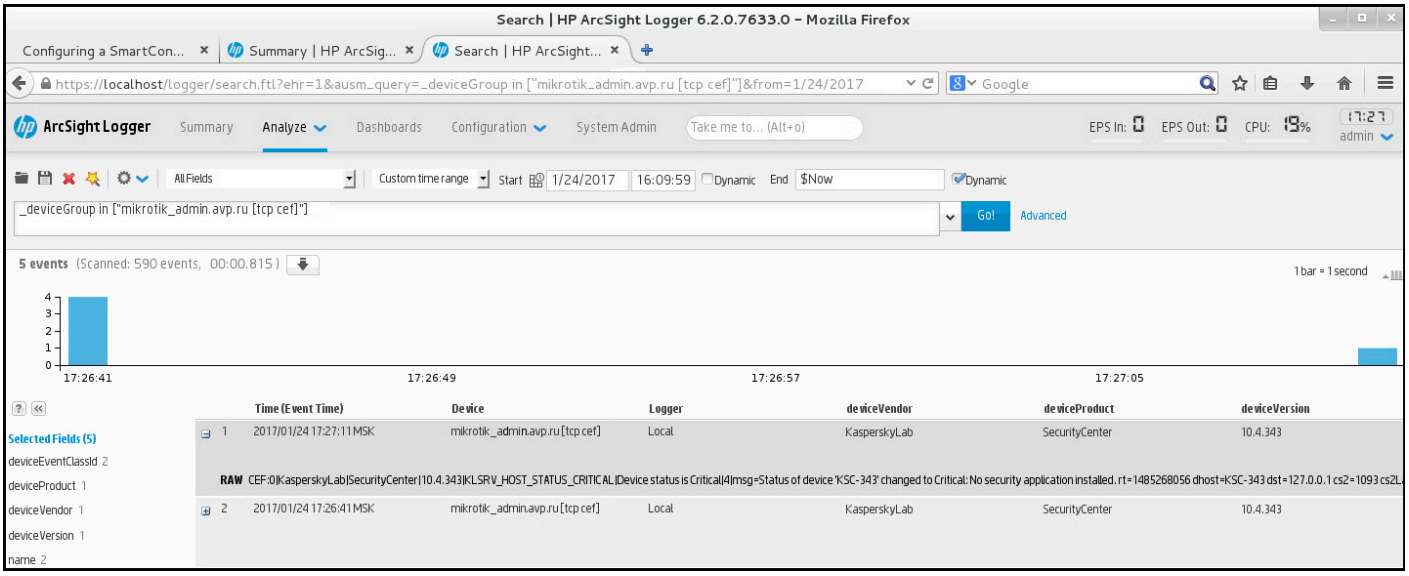
Exibir os resultados da exportação

Você pode controlar para a conclusão bem-sucedida do procedimento de exportação de eventos. Para fazer isto, verifique se as mensagens com eventos exportados são recebidas pelo seu sistema SIEM.

Se os eventos enviados do Kaspersky Security Center forem recebidos e apropriadamente analisados pelo seu sistema SIEM, a configuração nos dois lados foi feita apropriadamente. De outra forma, verifique as configurações que você especificou no Kaspersky Security Center contra a configuração no seu sistema SIEM.

A figura abaixo mostra os eventos exportados ao ArcSight. Por exemplo, o primeiro evento é crítico do Servidor de Administração: "*Status do dispositivo é crítico*".

A representação da exportação de eventos no sistema SIEM varia de acordo com o sistema SIEM que você usa.



Exemplo de eventos

Usando SNMP para enviar estatísticas para aplicativos de terceiros

Esta seção descreve como obter informações do Servidor de Administração usando o Protocolo de Gerenciamento de Rede Simples (SNMP) no Windows. O Kaspersky Security Center contém o agente SNMP, que transfere estatísticas de desempenho do Servidor de Administração para aplicativos secundários usando OIDs.

Esta seção também contém informações sobre como solucionar problemas que você pode encontrar ao usar SNMP para Kaspersky Security Center.

Configuração do serviço SNMP para uso com o Kaspersky Security Center

Esta seção descreve como configurar o serviço SNMP no Windows para obter informações do Servidor de Administração com o uso do Protocolo de Gerenciamento de Rede Simples (SNMP).

O suporte ao SNMP está desativado por padrão no Windows.

Para ativar a compatibilidade do SNMP no Windows:

1. Navegue até **o painel de controle**.
2. Abra o menu **Adicionar ou Remover Programas**.
3. Clique em **Ativar ou desativar recursos do Windows**.
4. Na lista de recursos do Windows, navegue até o recurso SNMP e clique em **OK**.
5. Navegue até **Painel de Controle** → **Ferramentas Administrativas** → **Serviços**.

6. Escolha o **serviço SNMP** e execute-o.

7. Verifique se a escuta funciona ao testá-la com `netstat` para uma porta UPD padrão.

O suporte SNMP está ativado no Windows.

Para configurar os serviços SNMP no Windows:

1. Verifique e confirme se o componente do **Agente SNMP** do Kaspersky Security Center foi instalado por meio de instalação normal ou silenciosa.

2. Verifique e confirme se os serviços do Windows **SNMP Service** e **SNMP Trap** estão em execução.

3. Verifique e confirme se o ManageEngine MIB Browser está instalado no seu sistema.

4. Nas propriedades do serviço **SNMP Service**, na guia **Segurança**, adicione duas comunidades com os seguintes direitos:

Comunidade	Direitos
`kaspersky`	`NOTIFY`
`public`	`READ WRITE`

5. No campo **Aceitar pacotes SNMP desses hosts**, adicione o endereço IP do dispositivo no qual o ManageEngine MIB Browser está instalado, por exemplo, 10.10.10.105.

6. Na guia **Traps**, digite `kaspersky` no campo **Nome da comunidade**.

7. Clique em **OK** para salvar as alterações e fechar a janela propriedades do serviço.

8. No ManageEngine MIB Browser, carregue o arquivo adminkit.mib a partir da pasta de instalação do Kaspersky Security Center. Por padrão, o arquivo adminkit.mib está na pasta <Disco>:\Program Files\Kaspersky Lab\Kaspersky Security Center\snmp.

9. No campo **Host** da janela ManageEngine MIB Browser, adicione o endereço IP do dispositivo no qual o Servidor de Administração do Kaspersky Security Center está instalado.

O serviço SNMP é configurado para obter informações do Servidor de Administração com o uso do Protocolo de Gerenciamento de Rede Simples (SNMP).

Agente SNMP e identificadores de objetos

Para o Kaspersky Security Center, o agente SNMP é implementado como uma biblioteca dinâmica `klsnmpag.dll`, que é registrada pelo instalador durante a instalação do Servidor de Administração. O agente SNMP funciona dentro do processo `snmp.exe` (que é um serviço do Windows). Os aplicativos de terceiros usam SNMP para receber estatísticas na forma de contadores sobre o desempenho do Servidor de Administração.

Cada contador possui um identificador de *objeto identificador* exclusivo (também chamado como OID). Um identificador de objeto é uma sequência de números dividida por pontos. Os identificadores de objeto do Servidor de Administração começam com o prefixo 1.3.6.1.4.1.23668.1093. O OID do contador é uma concatenação desse prefixo com um sufixo que descreve o contador. Por exemplo, o contador com o valor OID de 1.3.6.1.4.1.23668.1093.1.1.4 tem o sufixo com valor 1.1.4.

Você pode usar um cliente SNMP (como Zabbix) para monitorar o estado do sistema. Para obter as informações, você pode pesquisar um valor de OID que corresponda às informações e inserir esse valor no cliente SNMP. Em seguida, o cliente SNMP retornará a você outro valor que caracteriza o status do seu sistema.

A lista de contadores e tipos de contadores está no arquivo `adminkit.mib` no Servidor de Administração. *MIB* significa Base de Informações de Gerenciamento. Você pode importar e analisar arquivos `.mib` por meio do aplicativo MIB Viewer, que é projetado para solicitar e exibir os valores do contador.

Obtendo uma string do nome de contador de um identificador de objeto

Para usar um identificador de objeto (OID) para transferir informações para aplicativos de terceiros, pode ser necessário obter um nome de contador de string desse OID.

Para obter um nome de contador de string de um OID:

1. Abra o arquivo `adminkit.mib`, localizado no Servidor de Administração em um editor de texto.
2. Localize o namespace que descreve o primeiro valor (da esquerda para a direita).

   Por exemplo, para o sufixo 1.1.4 OID, será `"counters" (::= { kladminkit 1 })`.
3. Localize o namespace que descreve o segundo valor.

   Por exemplo, para o sufixo 1.1.4 OID, será os `counters 1`, que significa `deployment`.
4. Localize o namespace que descreve o terceiro valor.

   Por exemplo, para o sufixo 1.1.4 OID, isso será `deployment 4`, que significa `hostsWithAntivirus`.

O nome do contador da strings é a concatenação desses valores, por exemplo, `<MIB base namespace>.counters.deployment.hostsWithAntivirus`, que corresponde ao OID com o valor de 1.3.6.1.4.1.23668.1093.1.1.4.

Valores de identificadores de objetos para SNMP

A tabela abaixo mostra os valores e descrições dos identificadores de objetos (também chamados de OIDs), usados para transferir informações sobre o desempenho do Servidor de Administração para aplicativos de terceiros.

Valores e descrições de identificadores de objetos para SNMP

Valor do identificador de objeto	Tipo de dados numérico	OID	Descrição
deploymentStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.1.1	Status de implementação. O status pode ser um dos seguintes: • **Informação**. A licença não é mais válida para N dispositivos. • **Advertência**. Um dos seguintes: Há M dispositivos com aplicativos Kaspersky instalados em um total de N dispositivos nos grupos do Servidor de Administração (N > M). A licença L irá expirar em N dispositivos em M dias. A tarefa T de instalação de aplicativos foi concluída com êxito nos dispositivos N, é necessário reinicializar para M dispositivos. • **Crítico**. Licença expirada para N dispositivos. • **OK**. Nenhuma das opções acima.
noAntivirusSoftware	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.1	O motivo `deploymentStatus` mostra que o grupo do Servidor de Administração contém muitos dispositivos sem aplicativos gerenciados. O valor é igual a 1 se alguns dispositivos sejam encontrados sem aplicativos gerenciados e 0, caso contrário.
remoteInstallTaskFailed	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.2	O motivo `deploymentStatus` mostra que a tarefa da instalação remota falhou em alguns dispositivos. O número desses dispositivos pode ser obtido via `hostsRemoteInstallFailed`.
licenceExpiring	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.3	O motivo `deploymentStatus` mostra que há alguns dispositivos com uma licença que expira nos próximos 7 dias. O número desses dispositivos pode ser obtido via `hostsLicenseExpiring`.
licenceExpired	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.1.2.4	O motivo `deploymentStatus` mostra que há alguns dispositivos com uma licença expirada. Você pode obter a quantidade desses dispositivos via `hostsLicenseExpired`.
hostsInGroups	Counter32	.1.3.6.1.4.1.23668.1093.1.1.3	Número de dispositivos nos grupos do Servidor de Administração.
hostsWithAntivirus	Counter32	.1.3.6.1.4.1.23668.1093.1.1.4	Número de dispositivos nos grupos do Servidor de Administração com aplicativos gerenciados instalados.
hostsRemoteInstallFailed	Counter32	.1.3.6.1.4.1.23668.1093.1.1.5	Número de dispositivos nos quais a tarefa de instalação remota falhou.
licenceExpiringSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.6	ID de uma chave de licença que expira em breve (em menos de 7 dias).
licenceExpiredSerial	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.1.7	ID da chave de licença expirada.
licenceExpiringDays	Unsigned32	.1.3.6.1.4.1.23668.1093.1.1.8	Número de dias antes do término de uma licença. Para esse parâmetro, o período da licença é considerado expirado caso haja menos de 7 dias restantes até a data de término. Caso haja mais de 7 dias restantes até a data de término, o valor será 0.
hostsLicenceExpiring	Counter32	.1.3.6.1.4.1.23668.1093.1.1.9	Número de dispositivos com uma licença que expira em breve (em menos de 7 dias).
hostsLicenceExpired	Counter32	.1.3.6.1.4.1.23668.1093.1.1.10	Número de dispositivos com uma licença expirada.

Valor do identificador de objeto	Tipo de dados numérico	OID	Descrição
updatesStatus	INTEGER { ok(0), info(1), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.2.1	Status atual da atualização das bases de antivírus. O status pode ser um dos seguintes: • **Informação**. As bases de antivírus no Servidor de Administração ou nos dispositivos não foram atualizadas por mais de um dia, e menos de um dia se passou desde a instalação do aplicativo. • **Advertência**. As bases de antivírus no Servidor de Administração ou nos dispositivos não foram atualizadas por mais de 3 dias. Esse valor pode ser alterado nas configurações do grupo. • **Crítico**. As bases de antivírus no Servidor de Administração ou nos dispositivos não foram atualizadas por mais de 7 dias. Esse valor pode ser alterado nas configurações do grupo. • **OK**. Nenhuma das opções acima.
serverNotUpdated	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.1	Este motivo mostra que o Servidor de Administração não foi atualizado por um tempo de registro. A quantidade de tempo considerada longa é especificada em updatesStatus.
notUpdatedHosts	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.2.2.2	Este motivo mostra que alguns dispositivos não foram atualizados por um longo tempo (por padrão, 7 dias ou mais para **Crítico** e 3 dias para **Advertência**). Você pode obter a quantidade desses dispositivos via hostsNotUpdated.
lastServerUpdateTime	OCTET STRING	.1.3.6.1.4.1.23668.1093.1.2.3	Última vez em que os bancos de Antivirus foram atualizadas no Servidor de Administração.
hostsNotUpdated	Counter32	.1.3.6.1.4.1.23668.1093.1.2.4	Número de dispositivos que contêm bases de antivírus que não são atualizadas há muito tempo (por padrão, 7 dias ou mais para **Crítico** e 3 dias para **Advertência**). Se houver dispositivos com o status de atualização **Crítico**, somente esses dispositivos serão contabilizados. Você pode obter o status de atualização via updatesStatus.
protectionStatus	INTEGER { ok(0), warning(2), critical(3) }	.1.3.6.1.4.1.23668.1093.1.3.1	Status da proteção em tempo real. Um dos seguintes: • **Advertência**. Um dos seguintes: Uma violação de segurança é detectada em um dispositivo que pertence ao grupo do Servidor de Administração. Erros de criptografia provocaram a alteração de status de proteção de alguns dispositivos. Verificação completa não foi executada há muito tempo. • **Crítico**. A proteção Antivírus não está funcionando em alguns dispositivos nos grupos do Servidor de Administração. • **OK**. Nenhuma das opções acima.
antivirusNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.1	Esse motivo mostra que o aplicativo de segurança não está sendo executado em alguns dispositivos. Você pode obter o número desses dispositivos via hostsAntivirusNotRunning.
realtimeNotRunning	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.2	Esse motivo mostra que a proteção em tempo real não está sendo executada em alguns dispositivos. Você pode obter o número desses dispositivos via hostsRealtimeNotRunning.
notCuredFound	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.4	Este motivo mostra que há alguns dispositivos contendo objetos não desinfectados. Você pode obter a quantidade desses dispositivos via hostsNotCuredObject.
tooManyThreats	INTEGER { off(0), on(1) }	.1.3.6.1.4.1.23668.1093.1.3.2.5	Esse motivo mostra que foram encontradas ameaças em alguns dispositivos. Você pode obter a quantidade desses dispositivos via hostsTooManyThreats.

Valor do identificador de objeto	Tipo de dados numérico	OID	Descrição
`virusOutbreak`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.3.2.6	Esse motivo mostra o status de surto de vírus do sistema. O valor é igual a 1 se uma determinada quantidade de vírus foi encontrada durante um determinado período de tempo e 0, caso contrário. A quantidade de vírus e o tempo são especificados no Servidor de Administração, usando as configurações de `Virus attack`.
`hostsAntivirusNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.3	Quantidade de dispositivos sem aplicativos de segurança sendo executados.
`hostsRealtimeNotRunning`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.4	Quantidade de dispositivos sem proteção em tempo real sendo executados.
`hostsRealtimeLevelChanged`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.5	Quantidade de dispositivos com proteção em tempo real inaceitável.
`hostsNotCuredObject`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.6	Quantidade de dispositivos contendo objetos não desinfectados.
`hostsTooManyThreats`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.3.7	Quantidade de dispositivos contendo ameaças.
`fullscanStatus`	`INTEGER { ok(0), info(1), warning(2), critical(3) }`	.1.3.6.1.4.1.23668.1093.1.4.1	Status da verificação completa do Antivírus. Um dos seguintes: • **Informação**. Menos 7 dias se passaram desde a instalação do aplicativo. • **Advertência**. A verificação completa do Antivírus não foi realizada por mais de 7 dias desde a instalação do aplicativo. • **Crítico**. A verificação completa do Antivírus não foi realizada por mais de 14 dias desde a instalação do aplicativo. • **OK**. Nenhuma das opções acima.
`notScannedLately`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.4.2.1	Esse motivo mostra que alguns dispositivos não foram verificados por um determinado período. Você pode obter a quantidade desses dispositivos via `hostsNotScannedLately`. A quantidade de tempo é especificada em `fullScanStatus`.
`hostsNotScannedLately`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.4.3	Quantidade de dispositivos que não foram verificados por um determinado período. A quantidade de tempo é especificada em `fullScanStatus`.
`logicalNetworkStatus`	`INTEGER { ok(0), warning(1), critical(2) }`	.1.3.6.1.4.1.23668.1093.1.5.1	Status da rede lógica do Servidor de Administração. Um dos seguintes: • **Advertência**. Se houver dispositivos com status de aviso que não podem ser acessados ou se houver dispositivos que não pertençam a nenhum grupo do Servidor de Administração. • **Crítico**. Se houver dispositivos cujo controle foi perdido pelo Servidor de Administração ou se houver dispositivos com um status crítico e que não podem ser acessados. • **OK**. Nenhuma das opções acima.
`notConnectedLongTime`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.1	Este motivo mostra que alguns dispositivos não foram conectados ao Servidor de Administração por um longo tempo (7 dias ou mais para um dispositivo com status de **Advertência** e 4 dias para um dispositivo com status **Crítico**). Você pode obter a quantidade desses dispositivos via `hostsNotConnectedLongTime`.
`controlLost`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.5.2.2	Este motivo mostra que há dispositivos cujo controle foi perdido pelo Servidor de Administração. Você pode obter a quantidade desses dispositivos via `hostsControlLost`.
`hostsFound`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.3	Quantidade de dispositivos encontrados pelo Servidor de Administração que não pertencem a nenhum grupo do Servidor de Administração.
`groupsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.4	Quantidade de grupos no Servidor de Administração.

Valor do identificador de objeto	Tipo de dados numérico	OID	Descrição
`hostsNotConnectedLongTime`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.5	Quantidade de dispositivos que não estão conectados ao Servidor de Administração há muito tempo. A quantidade de tempo considerada longa é especificada em `notConnectedLongTime`.
`hostsControlLost`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.5.6	Quantidade de dispositivos que não controlados pelo Servidor de Administração.
`eventsStatus`	`INTEGER { ok(0), warning(1), critical(2) }`	.1.3.6.1.4.1.23668.1093.1.6.1	Status do subsistema de eventos. Um dos seguintes: • **Advertência**. Um dos seguintes: Dispositivos do grupo do Servidor de Administração não procuraram por atualizações do Windows há muito tempo. Há dispositivos com problemas de status. • **Crítico**. Um dos seguintes: Há um evento com nível de gravidade "crítico" em pelo menos um dispositivo. Há um evento com nível de gravidade "erro" em pelo menos um dispositivo. Há um evento de conclusão de tarefa sem sucesso em pelo menos um dispositivo. Dispositivos do grupo do Servidor de Administração não procuraram por atualizações do Windows há muito tempo. Há dispositivos com problemas de status. • **OK**. Nenhuma das opções acima.
`criticalEventOccured`	`INTEGER { off(0), on(1) }`	.1.3.6.1.4.1.23668.1093.1.6.2.1	O motivo `eventsStatus` mostra que existem alguns eventos críticos no Servidor de Administração. Você pode obter a quantidade desses eventos via `criticalEventsCount`. O valor é igual a 1 se houver pelo menos um evento crítico em qualquer dispositivo e 0, caso contrário.
`criticalEventsCount`	`Counter32`	.1.3.6.1.4.1.23668.1093.1.6.3	Número de eventos críticos no Servidor de Administração.

Solução de problemas

Esta seção lista soluções para alguns problemas típicos que você pode encontrar ao usar o serviço SNMP.

O aplicativo de terceiros não consegue se conectar ao serviço SNMP

Verifique e confirme se o serviço SNMP está instalado e configurado conforme a descrição da seção Configuração do serviço SNMP para uso com o Kaspersky Security Center.

O serviço SNMP está funcionando, mas o aplicativo de terceiros não obtém nenhum valor

Permita o rastreamento do agente SNMP e certifique-se de que um arquivo não vazio seja criado. Isso significa que o agente SNMP está devidamente registrado e funcionando. Depois disso, permita conexões do serviço SNMP nas configurações do serviço secundário. Se um serviço secundário opera no mesmo host que o agente SNMP, a lista de endereços IP deve conter o endereço IP desse host ou o `loopback 127.0.0.1`.

Um serviço SNMP que se comunica com os agentes deve estar em execução no Windows. Você pode especificar os caminhos para os agentes SNMP no Registro do Windows via regedit.

- Para Windows 10:
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents
- Para Windows Vista e Windows Server 2008:
  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SNMP\Parameters\ExtensionAgents

Você também pode permitir o rastreamento do agente SNMP via regedit.

- Para sistemas de 32 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Debug
- Para sistemas de 64 bits:
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\SNMP\Deb
  "TraceLevel"=dword:00000004
  "TraceDir"="C:\\"

Os valores não correspondem aos status do Console de Administração

Para reduzir a carga no Servidor de Administração, o cache de valores é implementado para o agente SNMP. A latência entre o cache sendo atualizado e os valores sendo alterados no Servidor de Administração pode causar incompatibilidades entre os valores retornados pelo agente SNMP e os reais. Ao trabalhar com aplicativos de terceiros, você deve considerar essa possível latência.

Trabalhando em um ambiente nuvem

Esta seção fornece informações sobre a implementação e a manutenção do Kaspersky Security Center em ambientes detecção, como o Amazon Web Services e o Microsoft Azure.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Sobre o trabalho em um ambiente de nuvem

O Kaspersky Security Center 14.2 não só trabalha com dispositivos locais, mas também oferece recursos especiais para trabalhar em um ambiente de nuvem. O Kaspersky Security Center funciona nas seguintes maquinas:

- Instâncias da Amazon EC2 (a qual, também e referido as *instances*). Uma instância do Amazon EC2 é uma máquina virtual criada com base na plataforma Amazon Web Services (AWS). O Kaspersky Security Center usa AWS, *API* (Interface da Programação do Aplicativo).
- Maquinas virtuais do Microsoft Azure. O Kaspersky Security Center usa o Azure API.
- Instâncias das maquinas virtuas do Google Cloud. O Kaspersky Security Center usa o Google API.

Você pode implementar o Kaspersky Security Center em uma instância ou em uma máquina virtual para gerenciar a proteção dos dispositivos em um ambiente de nuvem e para usar recursos especiais do Kaspersky Security Center para trabalhar em um ambiente de nuvem. Esses recursos incluem:

- Use as ferramentas API para sondagem de dispositivos em um ambiente de nuvem
- Usar ferramentas de API para instalar o Agente de rede e aplicativos de segurança em dispositivos em um ambiente de nuvem
- Pesquisar por dispositivos com base em se eles pertencem a um segmento da nuvem específico

Você também pode usar uma instância ou uma máquina virtual que tenha um Servidor de Administração do Kaspersky Security Center nela implementado para proteger dispositivos locais (por exemplo, se você descobrir ser mais fácil fornecer serviços e manutenção em um servidor detecção do que em um servidor físico). Se este for o caso, você trabalha com o Servidor de Administração da mesma forma como faria se o Servidor de Administração estivesse instalado em um dispositivo local.

Em um Kaspersky Security Center que foi implementado a partir de uma Imagem de máquina da Amazon (AMI, Amazon Machine Image) paga (no AWS) ou um SKU com base no uso e faturamento mensal (no Azure), o Gerenciamento de patches e vulnerabilidades (incluindo a integração com sistemas SIEM) é automaticamente ativada; o Gerenciamento de Dispositivos Móveis não pode ser ativado.

O Servidor de Administração é instalado em conjunto com o Console de Administração. O Kaspersky Security for Windows Server também é automaticamente instalado no dispositivo no qual o Servidor de Administração está instalado.

É possível configurar o Kaspersky Security Center com o assistente Configurar ambiente em nuvem, levando em consideração as especificidades de trabalhar em um ambiente de nuvem.

Cenário: implementação para o ambiente em nuvem

Esta seção descreve a implementação do Kaspersky Security Center para trabalhar nos ambiente de nuvem da Amazon Web Services, Microsoft Azure e Google Cloud.

Após a conclusão do cenário de implementação, o Servidor de Administração do Kaspersky Security Center e o Console de Administração serão iniciados e configurados com os parâmetros padrão. A proteção antivírus gerenciada pelo Kaspersky Security Center será implementada nas instâncias do Amazon EC2 selecionadas ou máquinas virtuais do Microsoft Azure. Você então pode efetuar o ajuste fino da configuração do Kaspersky Security Center, criar uma estrutura complexa de grupos de administração e criar diversas políticas e tarefas para grupos.

A implementação do Kaspersky Security Center para trabalho em ambientes em nuvem consiste nas seguintes partes:

1. Trabalho de preparação
2. Distribuir o Servidor de Administração
3. Instalar os aplicativos antivírus da Kaspersky em dispositivos virtuais que têm de ser protegidos
4. Definir as configurações de download de atualizações
5. Definir as configurações para gerenciar relatórios sobre o status de proteção de dispositivos

O assistente Configurar o ambiente em nuvem é destinado para a execução da configuração inicial. Ele é iniciado automaticamente na primeira vez que o Kaspersky Security Center é implementado a partir de uma imagem pronta para uso. É possível iniciar o assistente manualmente a qualquer momento. Além disso, é possível executar manualmente todas as ações que o ambiente executa.

Recomendamos reservar ao menos uma hora para a implementação do Servidor de Administração do Kaspersky Security Center no ambiente de nuvem e pelo menos um dia útil para a implementação da proteção no ambiente de nuvem.

A implementação do Kaspersky Security Center no ambiente de nuvem prossegue em estágios:

1. **Planejar a configuração de segmentos da nuvem**

   Aprenda como o Kaspersky Security Center funciona em um ambiente de nuvem. Planeje onde o Servidor de Administração será implementado: (fora ou dentro do ambiente de nuvem); determine também quantos segmentos da nuvem planeja proteger. Caso esteja planejando implementar o Servidor de Administração fora do ambiente de nuvem, ou se estiver planejando proteger mais de 5.000 dispositivos, será necessário instalar o Servidor de Administração manualmente.

   Para uso com o Google Cloud, você só pode instalar Servidor de Administração manualmente.

2. **Planejar os recursos**

   Assegure-se de ter tudo o que for necessário para a implementação.

3. **Assinatura do Kaspersky Security Center como uma imagem**

   Selecione uma das AMIs prontas para usar no AWS Marketplace ou selecione uma SKU de faturamento mensal no Azure Marketplace, efetue o pagamento de acordo com as condições do marketplace, se necessário (ou use o modelo BYOL), e use a imagem para implementar uma instância do Amazon EC2/máquina virtual do Microsoft Azure com o Kaspersky Security Center instalado.

   Este estágio somente é necessário se você planejar implementar o Servidor de Administração em uma instância / máquina virtual dentro de um ambiente de nuvem e também planeja implementar a proteção de não mais do que 5.000 dispositivos. Caso contrário, este estágio não será necessário; em vez disso, será necessário instalar manualmente o Servidor de Administração, o Console de Administração e o DBMS.

   Esta etapa não esta disponível para o Google Cloud.

4. **Determinar a localização do DBMS**

Determine onde o seu DBMS ficará.

Caso deseje usar um banco de dados fora do ambiente de nuvem, certifique-se de que ele esteja funcionando.

Caso planeje usar o Amazon Relational Database Service (RDS), crie um banco de dados com RDS no ambiente de nuvem AWS.

Caso planeje usar o Microsoft Azure SQL DBMS, crie um banco de dados com o serviço de Banco de Dados do Azure no ambiente de nuvem do Microsoft Azure.

Se você planeja usar o Google MySQL, crie um banco de dados no Google Cloud (consulte https://cloud.google.com/sql/docs/mysql para obter detalhes).

5. **Instalar o Servidor de Administração e o Console de Administração (com base no Console de Gerenciamento Microsoft e/ou no Console baseado na Web) em dispositivos selecionados manualmente**

   Instale o Servidor de Administração, o Console de Administração e o DBMS nos dispositivos selecionados indicados pelo cenário de instalação principal do Kaspersky Security Center.

   Este estágio é necessário se você planeja colocar o Servidor de Administração fora do ambiente de nuvem ou implementar a proteção para mais de 5.000 dispositivos. Depois, certifique-se de que seu Servidor de Administração atende aos requisitos de hardware. Caso contrário, esta fase não será necessária e uma assinatura do Kaspersky Security Center como uma imagem pronta para uso no AWS Marketplace, no Azure Marketplace ou Google Cloud é suficiente.

6. **Certificando-se de que o Servidor de Administração tem as permissões para uso com as APIs de nuvem**

   No AWS, siga até Console de Gerenciamento AWS e crie uma função do IAM ou uma conta de Usuário IAM. A função do IAM criada (ou a conta de usuário IAM) permitirá que o Kaspersky Security Center trabalhe com AWS API: obtendo sondagem dos segmentos da nuvem e a implementando a proteção.

   No Azure, crie uma assinatura e um ID do aplicativo com senha. O Kaspersky Security Center usa essas credenciais para uso com a Azure API: obtendo sondagem dos segmentos da nuvem e a implementando a proteção.

   No Google Cloud, registre um projeto, receba o ID do projeto e uma chave exclusiva. O Kaspersky Security Center usa essas credencias para obter a sondagem de segmentos da nuvem usando o Google API.

7. **Criar uma função do IAM para instâncias protegidas (somente para AWS)**

   No Console de Gerenciamento AWS, crie uma função do IAM que define o conjunto de permissões para a execução das solicitações no AWS. Esta função recentemente criada será subsequentemente atribuída às novas instâncias. A função do IAM é necessária para poder usar o Kaspersky Security Center para instalar aplicativos em instâncias.

8. **Preparar um banco de dados usando Amazon Relational Database Service ou Microsoft Azure SQL**

   Se você planeja usar Amazon Relational Database Service (RDS), crie uma instância de banco de dados do Amazon RDS e um S3 bucket no qual o backup de banco de dados será armazenado. Você pode ignorar esse estágio se deseja ter um banco de dados na mesma instância do EC2 onde o Servidor de Administração está instalado ou que o banco de dados fique localizado em outro lugar.

   Se você planeja usar o Microsoft Azure SQL, crie uma conta de armazenamento e um banco de dados no Microsoft Azure.

   Se você planeja usar o Google MySQL, configure o banco de dados no Google Cloud (consulte https://cloud.google.com/sql/docs/mysql para obter detalhes).

9. **Licenciamento do Kaspersky Security Center para trabalhar no ambiente de nuvem**

   Assegure-se de que você licenciou o Kaspersky Security Center para trabalhar no ambiente de nuvem AWS e forneça um código de ativação ou um arquivo chave para que o aplicativo possa adicioná-lo ao armazenamento da licença. Esta etapa pode ser concluída durante a configuração do ambiente em nuvem.

Este estágio é necessário se você estiver usando o Kaspersky Security Center instalado a partir de um AMI pronto para uso e gratuito com base no modelo BYOL ou se estiver instalando manualmente o Kaspersky Security Center sem o uso de AMIs. Em cada um desses casos, você precisará de uma licença do Kaspersky Security for Virtualization ou uma licença do Kaspersky Hybrid Cloud Security para ativar o Kaspersky Security Center.

Caso esteja usando o Kaspersky Security Center instalado a partir de uma imagem pronta para usar, esta etapa não é necessária, e a janela correspondente do assistente Configurar o ambiente em nuvem não será exibida.

10. **Autorização no ambiente de nuvem**

    Forneça ao Kaspersky Security Center as suas credenciais do AWS, Azure ou Google Cloud para que o Kaspersky Security Center opere com as permissões necessárias. Esta etapa pode ser concluída durante a autorização no ambiente em nuvem.

11. **Obter a sondagem do segmento da nuvem para que o Servidor de Administração possa receber informações sobre os dispositivos no segmento da nuvem**

    Inicie a sondagem do segmento da nuvem. No ambiente AWS, o Kaspersky Security Center receberá os endereços e nomes de todas as instâncias que podem ser acessadas com base nas permissões da função do IAM ou do usuário do IAM. No ambiente do Microsoft Azure, o Kaspersky Security Center receberá os endereços e nomes de todas as máquinas virtuais que podem ser acessadas com base nas permissões de função do Leitor.

    Você então pode usar o Kaspersky Security Center para instalar aplicativos Kaspersky e software de outros fornecedores nas instâncias ou máquinas virtuais detectadas.

    O Kaspersky Security Center regularmente inicia uma sondagem, o que significa que os novas instâncias ou máquinas virtuais são automaticamente detectadas.

12. **Combinando todos os dispositivos na rede no grupo de administração Nuvem**

    Mova todas as instâncias ou máquinas virtuais descobertas para o grupo de administração **Dispositivos gerenciados\Nuvem** para que elas possam ficar disponíveis para o gerenciamento centralizado. Se você desejar atribuir dispositivos aos subgrupos, por exemplo, dependendo de qual o sistema operacional esteja neles instalado, poderá criar diversos grupos de administração dentro do grupo **Dispositivos gerenciados\Nuvem**. Você pode ativar o movimento automático de todos os dispositivos que serão detectados durante as sondagens de rotina ao grupo **Dispositivos gerenciados\Cloud**.

13. **Usar o Agente de Rede para conectar dispositivos na rede ao Servidor de Administração**

    Instale o Agente de Rede nas instâncias. O Agente de Rede é o componente do Kaspersky Security Center que fornece os meios para a comunicação entre os dispositivos e o Servidor de Administração. As configurações do Agente de Rede são definidas automaticamente por padrão.

    Você pode instalar o Agente de Rede em cada dispositivo localmente. Você também pode instalar o Agente de Rede em dispositivos remotamente usando o Kaspersky Security Center. Ou você pode ignorar esse estágio e instalar o Agente de Rede em conjunto com as versões mais recentes dos aplicativos de segurança.

14. **Instalar as versões mais recentes de aplicativos de segurança nos dispositivos em rede**

    Selecione os dispositivos nos quais deseja instalar os aplicativos de segurança e, então, instale as versões mais recentes dos aplicativos de segurança nesses dispositivos. É possível executar a instalação remotamente, utilizando o Kaspersky Security Center em um Servidor de Administração, ou localmente.

    Você pode ter que criar pacotes de instalação para esses programas manualmente.

    O Kaspersky Endpoint Security de Linux é destinado para instâncias e máquinas virtuais sendo executadas no Linux.

    O Kaspersky Security for Windows Server é destinado para instâncias e máquinas virtuais sendo executadas no Windows.

15. **Definir as configurações da atualização**

A tarefa **Localização de vulnerabilidades e atualizações necessárias** é criada automaticamente quando o assistente de configuração de ambiente em nuvem é iniciado. Você também pode criar a tarefa manualmente. Esta tarefa automaticamente encontra e baixa as atualizações de aplicativo necessárias para a instalação subsequente em dispositivos na rede usando as ferramentas do Kaspersky Security Center.

Recomenda-se finalizar a seguinte etapa após a conclusão da configuração de ambiente em nuvem:

1. **Configurando gerenciamento de relatórios**

   Você pode exibir relatórios na guia **Monitoramento** no espaço de trabalho do nó do **Servidor de Administração**. Você também pode receber relatórios por e-mail. Os relatórios na guia **Monitoramento** estão disponíveis por padrão. Para configurar o recebimento de relatórios por e-mail, especifique os endereços de e-mail que devem receber os relatórios e, então, configure o formato dos relatórios.

Resultados

Após a conclusão do cenário, assegure-se de que a configuração inicial teve êxito:

- É possível conectar-se ao Servidor de Administração por meio do Console de Administração ou do Kaspersky Security Center Web Console.
- A versão mais recentes dos aplicativos de segurança da Kaspersky estão instaladas e sendo executadas nos dispositivos gerenciados.
- Que o Kaspersky Security Center tenha criado as políticas e tarefas padrão para todos os dispositivos gerenciados.

Prerrequisitos para implementar o Kaspersky Security Center em um ambiente de nuvem

Antes de iniciar a implementação do Kaspersky Security Center no Amazon Web Services ou no ambiente de nuvem do Microsoft Azure, certifique-se de ter o seguinte:

- Acesso à Internet
- Uma das seguintes contas:
  - Conta Amazon Web Services (para uso com a AWS)
  - Conta da Microsoft (para uso com o Azure)
  - Conta do Google (para uso com o Google Cloud)

- Um dos seguintes:
  - Licença do Kaspersky Security for Virtualization
  - Licença do Kaspersky Hybrid Cloud Security
  - Fundos para comprar a licença (Kaspersky Security for Virtualization ou Kaspersky Hybrid Cloud Security)
  - Fundos para pagar por uma imagem pronta para uso no Azure Marketplace
- Guias das versões mais recentes do Kaspersky Endpoint Security for Linux e Kaspersky Security for Windows Server

Requisitos de hardware para o Servidor de Administração no ambiente de nuvem

Para implementação em ambientes de nuvem, os requisitos do Servidor de Administração e do servidor de banco de dados são idênticos aos requisitos do Servidor de Administração físico (dependendo de quantos dispositivos você deseja gerenciar). Consulte a documentação dos ambientes na nuvem para obter mais detalhes.

Opções de licenciamento em um ambiente em nuvem

O trabalho no ambiente de nuvem está fora da funcionalidade básica do Kaspersky Security Center e, portanto requer uma licença dedicada.

Duas opções de licenciamento do Kaspersky Security Center estão disponíveis para o trabalho em ambiente de nuvem:

- AMI paga (no Amazon Web Services) ou SKU com base no uso e faturamento mensal (no Microsoft Azure).

  Isso dá direito a uma licença do Kaspersky Security Center, bem como a licenças do Kaspersky Endpoint Security for Linux e do Kaspersky Security for Windows Server. Você deve pagar de acordo com as regras do ambiente de nuvem usado.

  Este modelo permite que você tenha até 200 dispositivos cliente para um Servidor de Administração.

- Uma imagem gratuita pronta para uso com uma licença proprietária, segundo o modelo Bring Your Own License (BYOL).

  Para o licenciamento do Kaspersky Security Center no AWS ou Azure, você deve ter uma licença para um dos seguintes aplicativos:

  - Kaspersky Security for Virtualization
  - Kaspersky Hybrid Cloud Security

  O modelo BYOL permite que você tenha até 100.000 dispositivos cliente para um Servidor de Administração. Este modelo também permite gerenciar dispositivos fora do ambiente de nuvem do AWS, Azure ou Google.

  Você pode escolher o modelo BYOL em quaisquer dos seguintes casos:

  - Você já tem uma licença válida do Kaspersky Security for Virtualization.
  - Você já tem uma licença válida do Kaspersky Hybrid Cloud Security.
  - Você deseja comprar uma licença imediatamente antes da implementação do Kaspersky Security Center.

  Na etapa da configuração inicial, Kaspersky Security Center o solicitará a fornecer um código de ativação ou um arquivo de chave.

  Se você escolher BYOL, não terá de pagar pelo Kaspersky Security Center através do Azure Marketplace ou AWS Marketplace.

Em ambos os casos, o Gerenciamento de patches e vulnerabilidades é automaticamente ativado, e o Gerenciamento de Dispositivos Móveis não pode ser ativado.

Se um erro ocorrer ao tentar ativar o recurso de Suporte do ambiente em nuvem usando a licença do Kaspersky Hybrid Cloud Security, use o arquivo de chave.

Ao fazer uma assinatura do Kaspersky Security Center, você recebe uma instância do Amazon Elastic Compute Cloud (Amazon EC2) ou uma máquina virtual do Microsoft Azure com o Servidor de Administração do Kaspersky Security Center. Os pacotes de instalação do Kaspersky Security for Windows Server e do Kaspersky Endpoint Security for Linux estão disponíveis no Servidor de Administração. Você pode instalar esses aplicativos nos dispositivos no ambiente de nuvem. Você não precisa licenciar esses aplicativos.

Se um dispositivo gerenciado não ficar visível para o Servidor de Administração por mais de uma semana, o aplicativo (Kaspersky Security for Windows Server ou Kaspersky Endpoint Security for Linux) no dispositivo será alterado para o Modo de funcionalidade limitada. Para ativar o aplicativo novamente, você precisa tornar o dispositivo no qual o aplicativo está instalado novamente visível para o Servidor de Administração.

Opções de banco de dados para trabalhar em um ambiente de nuvem

Você precisa ter um banco de dados para uso com o Kaspersky Security Center. Quando for implementar o Kaspersky Security Center no AWS ou no Microsoft Azure, você tem três opções:

- Criar um banco de dados local no mesmo dispositivo com o Servidor de Administração. O Kaspersky Security Center vem com um banco de dados SQL Server Express que aceita até 5.000 dispositivos gerenciados. Escolha esta opção se o SQL Server Express Edition for suficiente para as suas necessidades.

- Criar um banco de dados com o Relational Database Service (RDS) no ambiente de nuvem do AWS ou com o serviço Azure Database no ambiente de nuvem do Microsoft Azure. Selecione esta opção se você quiser ter um DBMS diferente do SQL Express. Seus dados serão transferidos para o ambiente de nuvem, onde permanecerão, e você não terá nenhuma despesa extra. Se você já trabalha com o Kaspersky Security Center local e existirem alguns dados no banco de dados, você poderá transferi-los para o novo banco de dados.

  Para funcionar no Google Cloud Platform, você só pode usar o Cloud SQL for MySQL.

- Usar um servidor de banco de dados existente. Escolha esta opção se você já tiver um servidor de banco de dados e quiser usá-lo para o Kaspersky Security Center. Se esse servidor estiver fora do ambiente de nuvem, os dados serão transferidos pela Internet, o que pode resultar em despesas extras.

O procedimento de implementação do Kaspersky Security Center no ambiente de nuvem tem uma etapa especial para criar (escolher) um banco de dados.

Trabalhando no ambiente de nuvem Amazon Web Services

Esta seção informa a você como preparar-se para uso com o Kaspersky Security Center no Amazon Web Services.

> Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Sobre o trabalho no ambiente na nuvem de Amazon Web Services

Você pode comprar o Kaspersky Security Center no AWS Marketplace na forma de uma imagem de máquina da Amazon (AMI), que é uma imagem pronta para usar de uma máquina virtual pré-configurada. Você pode assinar um AMI ou BYOL AMI pago e, com base naquela imagem, criar uma instância do Amazon EC2 com o Servidor de Administração do Kaspersky Security Center instalado.

Para uso com a plataforma AWS e, em particular, comprar aplicativos no AWS Marketplace e criar instâncias, você necessita de uma conta de Amazon Web Services. Você pode criar uma conta gratuita em https://aws.amazon.com. Você também pode usar uma conta existente da Amazon.

Se você assinou por uma AMI disponível no AWS Marketplace, receberá uma instância com o seu Kaspersky Security Center pronto para uso. Você mesmo não tem que instalar o aplicativo. Neste caso, o Servidor de Administração do Kaspersky Security Center é instalado na instância sem o seu envolvimento. Após a instalação, você pode iniciar o Console de Administração e conectar-se ao Servidor de Administração para começar a trabalhar com o Kaspersky Security Center.

Para saber mais sobre uma AMI e como funciona o AWS Marketplace, visite a página de Ajuda do AWS Marketplace. Para obter mais informações sobre o trabalho com a plataforma de AWS, usando instâncias e conceitos relacionados, consulte a documentação de Amazon Web Services.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Criar funções do IAM e contas de Usuário do IAM para instâncias do Amazon EC2

Esta seção descreve as ações que devem ser realizadas para assegurar a operação correta do Servidor de Administração. Estas ações incluem trabalhar com as contas de usuário e funções do AWS Identity And Access Management (IAM). Também estão descritas as ações que devem ser tomadas nos dispositivos cliente para instalar o Agente de Rede nos dispositivos e instalar o Kaspersky Security for Windows Server e o Kaspersky Endpoint Security for Linux.

Assegurar que o Servidor de Administração do Kaspersky Security Center tenha as permissões para trabalhar com AWS

Os padrões para operar no ambiente em nuvem de Amazon Web Services prescrevem que uma função do IAM especial seja atribuída à instância do Servidor de Administração para uso com os serviços AWS. Uma função do IAM é uma entidade IAM que define o conjunto de permissões para a execução das solicitações de serviços IAM. A função do IAM fornece as permissões para a sondagem do segmento da nuvem e a instalação de aplicativos nas instâncias.

Após você criar uma função do IAM e atribui-la ao Servidor de Administração, será capaz de implementar a proteção de instâncias usando esta função, sem fornecer qualquer informação adicional ao Kaspersky Security Center.

No entanto, pode ser aconselhável não criar uma função do IAM para o Servidor de Administração nos seguintes casos:

- Os dispositivos cuja proteção você planeja gerenciar, são instâncias EC2 dentro do ambiente de nuvem de Amazon Web Services, mas o Servidor de Administração está fora do ambiente.
- Você planeja gerenciar a proteção de instâncias não somente dentro de seu segmento da nuvem, mas também dentro de outros segmentos da nuvem que foram criados sob uma conta diferente no AWS. Neste caso, você precisará de uma função do IAM somente para a proteção do seu segmento da nuvem. Uma função do IAM não será necessária para proteger outro segmento da nuvem.

Nestes casos, em vez de criar uma função do IAM você precisará criar uma *Conta de Usuário do IAM* que será usada pelo Kaspersky Security Center para uso com os serviços AWS. Antes de começar a trabalhar com o Servidor de Administração, crie uma conta de Usuário do IAM com uma *chave de acesso AWS IAM* correspondente (aqui também referida como *chave de acesso IAM*).

A criação de uma função do IAM ou Conta de usuário IAM requer o Console de Gerenciamento AWS. Para uso com o Console de Gerenciamento AWS, você precisará de um nome do usuário e senha de uma conta no AWS.

Criar uma função do IAM para o Servidor de Administração

Antes que você implemente o Servidor de Administração, no Console de Gerenciamento AWS crie uma função do IAM com as permissões necessárias para a instalação de aplicativos nas instâncias. Para obter mais detalhes, consulte as seções de Ajuda do AWS sobre funções do IAM.

Para criar uma função do IAM para o Servidor de Administração:

1. Abra o Console de Gerenciamento AWS e efetue o login sob sua conta AWS.
2. Na seção **Funções**, crie uma função com as seguintes permissões:
   - **AmazonEC2ReadOnlyAccess**, se você planeja somente executar a sondagem do segmento da nuvem e não planeja instalar aplicativos em instâncias EC2 usando a AWS API.
   - **AmazonEC2ReadOnlyAccess** and **AmazonSSMFullAccess** se você planeja executar a sondagem do segmento da nuvem e instalar aplicativos em instâncias EC2 usando a AWS API. Neste caso, você também precisará atribuir uma função do IAM com a permissão AmazonEC2RoleforSSM das instâncias EC2 protegidas.

Você precisará atribuir esta função à instância EC2 que usará como Servidor de Administração.

A função recentemente criada está disponível para todos os aplicativos no Servidor de Administração. Portanto, qualquer aplicativo que executa no Servidor de Administração tem a capacidade de amostrar os segmentos da nuvem ou instalar aplicativos em instâncias EC2 dentro de um segmento da nuvem.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Criar uma conta de Usuário do IAM para trabalhar com o Kaspersky Security Center

Uma conta de Usuário do IAM é necessária para uso com o Servidor de Administração do Kaspersky Security Center não tem atribuída uma função do IAM com as permissões para a descoberta de dispositivos e para a instalação de aplicativos em instâncias não tiver sido atribuída ao Servidor de Administração. A mesma conta ou uma conta diferente, também é necessária para o backup da tarefa de dados do Servidor de Administração caso você utilize um S3 bucket. Você pode criar uma conta de usuário IAM com todas as permissões necessárias, ou pode criar duas contas de usuário separadas.

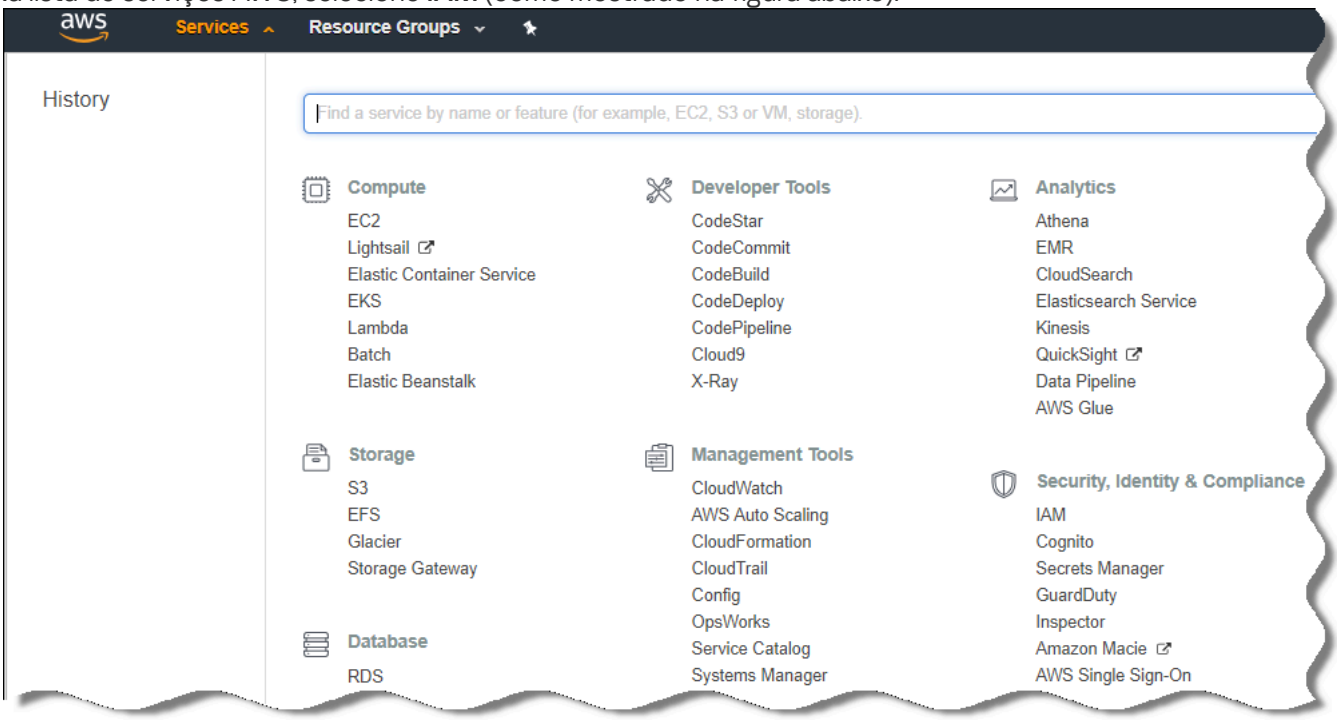
Uma *chave de acesso IAM* que você terá que fornecer ao Kaspersky Security Center durante a configuração inicial é automaticamente criada para o Usuário IAM. Uma chave de acesso IAM consiste em uma ID da chave de acesso e uma chave secreta. Para obter mais detalhes sobre mim o serviço IAM, consulte as seguintes páginas de referência AWS:

- http://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html.
- https://docs.aws.amazon.com/pt_br/IAM/latest/UserGuide/IAM_UseCases.html#UseCase_EC2.

Para criar uma conta de usuário IAM com as permissões necessárias:

1. Abra o Console de Gerenciamento AWS e efetue o login na sua conta.

2. Na lista de serviços AWS, selecione **IAM** (como mostrado na figura abaixo).



Lista de serviços em o Console de Gerenciamento AWS

Uma janela é aberta contendo uma lista de nomes de usuários e um menu que permite a você trabalhar com a ferramenta.

3. Navegue pelas áreas do console processando as contas de usuário e adicione um novo nome de usuário ou mais.

4. Para o(s) usuário(s) você adicionar, especifique as seguintes propriedades do AWS:

   - Tipo de acesso: **Acesso programático**.
   - Limite de permissões não definido.
   - Permissões:
     - **ReadOnlyAccess** – Se você planeja executar somente a sondagem do segmento da nuvem e não planeja instalar aplicativos em instâncias EC2 usando o AWS API.
     - **ReadOnlyAccess** e **AmazonSSMFullAccess** – Se você planeja executar a sondagem do segmento da nuvem e instalar aplicativos em instâncias EC2 usando AWS API. Neste caso, você deve atribuir uma função do IAM com a permissão AmazonEC2RoleforSSM das instâncias EC2 protegidas.

   Depois que você adicionar as permissões, visualize-as para confirmar a exatidão. Em caso de uma seleção por engano, volte à tela anterior e faça a seleção novamente.

5. Após criar a conta de usuário, uma tabela será exibida contendo a chave de acesso IAM do novo Usuário do IAM. A ID da chave de acesso é exibida na coluna **ID da chave de acesso**. A chave secreta é exibida como asteriscos na coluna **Chave de acesso secreta**. Para visualizar a chave secreta, clique em **Exibir**.

A conta recentemente criada é exibida na lista de contas de usuários IAM que correspondem à sua conta no AWS.

Ao implementar o Kaspersky Security Center em um segmento da nuvem, você deve especificar que está usando uma conta de Usuário IAM e fornecer uma ID da chave de acesso e a chave de acesso secreta para o Kaspersky Security Center.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Criar uma função do IAM para a instalação de aplicativos em instâncias do Amazon EC2

Antes que você inicie a implementação de proteção nas instâncias EC2 usando o Kaspersky Security Center, crie no Console de Gerenciamento AWS uma função do IAM com permissões necessárias para a instalação de aplicativos nas instâncias. Para obter mais detalhes, consulte as seções de Ajuda do AWS sobre funções do IAM.

A função do IAM é necessária para que você possa atribuí-la à todas as instâncias EC2 nas quais você planeja instalar aplicativos de segurança usando o Kaspersky Security Center. Se você não atribuir uma instância da função do IAM com as permissões necessárias, a instalação de aplicativos nesta instância usando as ferramentas AWS API resultará em um erro.

Para uso com o Console de Gerenciamento AWS, você precisará de um nome do usuário e senha de uma conta no AWS.

Para criar uma função do IAM para a instalação de aplicativos em instâncias:

1. Abra o Console de Gerenciamento AWS e efetue o login sob sua conta AWS.
2. No menu à esquerda, selecione **Roles**.
3. Clique no botão **Create Role**.
4. Na lista de serviços que aparece, selecione **EC2** e, a seguir, na lista **Select Your Use Case** selecione **EC2** novamente.
5. Clique no botão **Next: Permissions**.
6. Na lista que se abre, selecione a caixa seleção junto a **AmazonEC2RoleforSSM**.
7. Clique no botão **Next: Review**.
8. Insira um nome e uma descrição para a função do IAM e clique no botão **Create role**.

   A função que você criou aparece na lista de funções com o nome e descrição inseridos.

Depois disto, você pode usar a função do IAM recentemente criada para criar novas instâncias EC2 que pretende proteger através do Kaspersky Security Center, assim como associá-lo com as instâncias existentes.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Trabalhar com Amazon RDS

Esta seção descreve quais ações devem ser tomadas para preparar um banco de dados do Amazon Relational Database Service (RDS) para Kaspersky Security Center, colocá-lo em um grupo de opções, criar uma função do IAM para uso com um banco de dados RDS, preparar um S3 bucket para armazenamento e migrar um banco de dados existente para RDS.

O Amazon RDS é um serviço Web que ajuda usuários do AWS a configurar, operar e dimensionar um banco de dados relacional no ambiente de nuvem do AWS. Se desejar, você pode usar um banco de dados do Amazon RDS para uso com o Kaspersky Security Center.

É possível trabalhar com os seguintes bancos de dados:

- Microsoft SQL Server
- SQL Express Edition
- Aurora MySQL 5.7
- Standard MySQL 5.7

Criar uma instância Amazon RDS

Se você quiser usar o Amazon RDS como DBMS, precisará criar uma instância de banco de dados do Amazon RDS. Esta seção descreve como selecionar o SQL Express Edition. Caso deseje trabalhar com o Aurora MySQL ou Standard MySQL (versões 5.7, 8.0) é necessário selecionar um desses mecanismos.

Para criar uma instância de banco de dados do Amazon RDS:

1. Abra o Console de Gerenciamento AWS no https://console.aws.amazon.com e efetue o login sob sua conta.
2. Usando a interface AWS, crie um banco de dados com as seguintes configurações:

   - Mecanismo: Microsoft SQL Server, SQL Express Edition
   - Versão do mecanismo de BD: SQL Server 2014 12.00.5546.0v1
   - Classe da instância de BD: db.t2.medium
   - Tipo de armazenamento: finalidade geral
   - Armazenamento alocado: mínimo de 50 GiB
   - Grupo de segurança: o mesmo grupo onde a instância EC2 com o Servidor de Administração do Kaspersky Security Center será localizada

   Crie um identificador, nome de usuário e senha para a sua instância RDS.

   Você pode deixar as configurações padrão em todos os outros campos. Ou modifique as configurações padrão se você deseja personalizar sua instância do Amazon RDS. Para obter ajuda, consulte as páginas de informações do AWS.
3. Na última etapa, o AWS exibe os resultados do processo. Caso queira visualizar os detalhes da sua instância do Amazon RDS, clique em **Visualizar detalhes da instância do BD**. Se você quiser prosseguir para a próxima ação, comece a criar um grupo de opções da sua instância do Amazon RDS.

A criação de uma nova instância do Amazon RDS pode demorar vários minutos. Depois que a instância é criada, você pode usá-la para uso com dados do Kaspersky Security Center.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Criar grupo de opções para instância do Amazon RDS

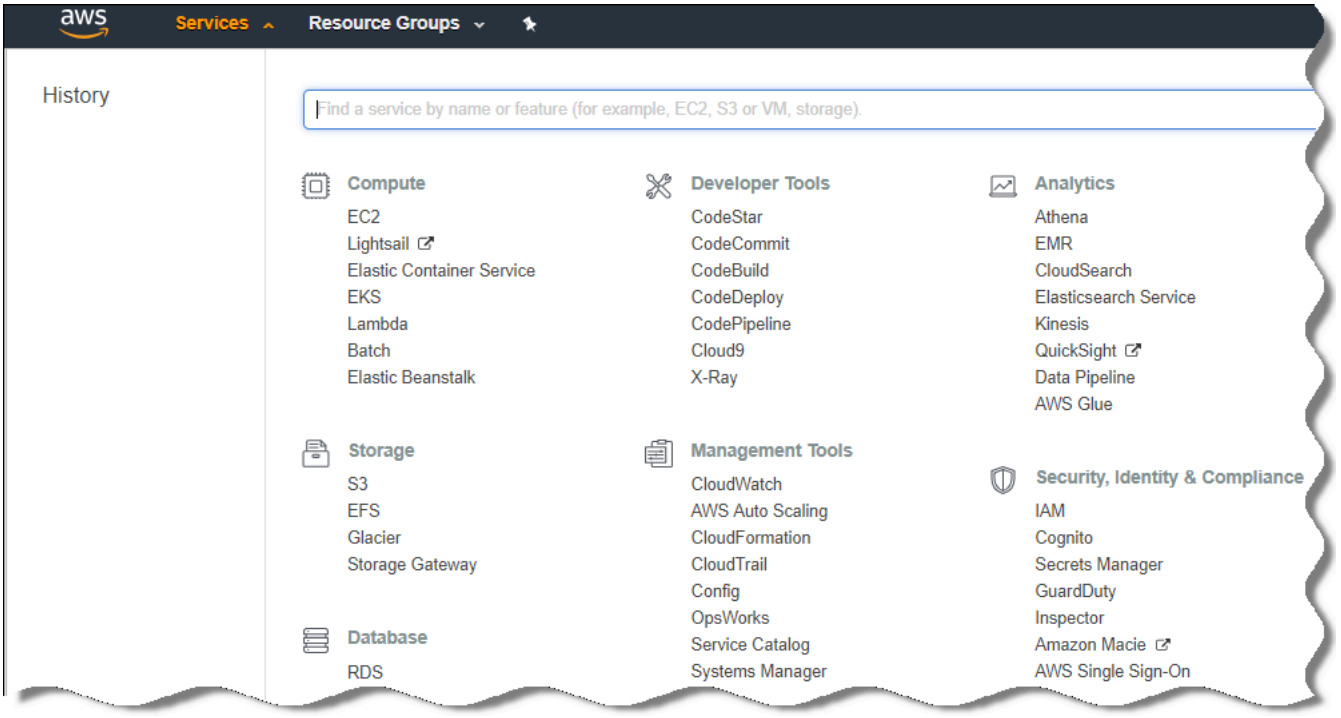
Você precisa colocar sua instância do Amazon RDS em um grupo de opções.

Para criar grupo de opções para a sua instância do Amazon RDS:

1. Assegure-se de que você está no Console de Gerenciamento AWS (https://console.aws.amazon.com) e efetuou login com sua conta.

2. Na linha de menu, clique em **Serviços**.

   A lista de serviços disponíveis é exibida (consulte a figura abaixo).



Lista de serviços em o Console de Gerenciamento AWS

3. Na lista, clique em **RDS**.

4. No painel esquerdo, clique em **Grupos de opções**.

5. Clique no botão **Create group**.

6. Crie um grupo de opções com as seguintes configurações, se você escolheu o SQL Server na etapa para criar a instância do Amazon RDS:

   - Mecanismo: SQLserver-ex
   - Versão do mecanismo principal: 12.00

   Se você selecionou um banco de dados SQL diferente na etapa de criação da instância do Amazon RDS, escolha um mecanismo correspondente.

O grupo é criado e exibido na lista de grupos.

Depois de criar o grupo de opções, coloque as instâncias do Amazon RDS nesse grupo de opções.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Modificar o grupo de opções

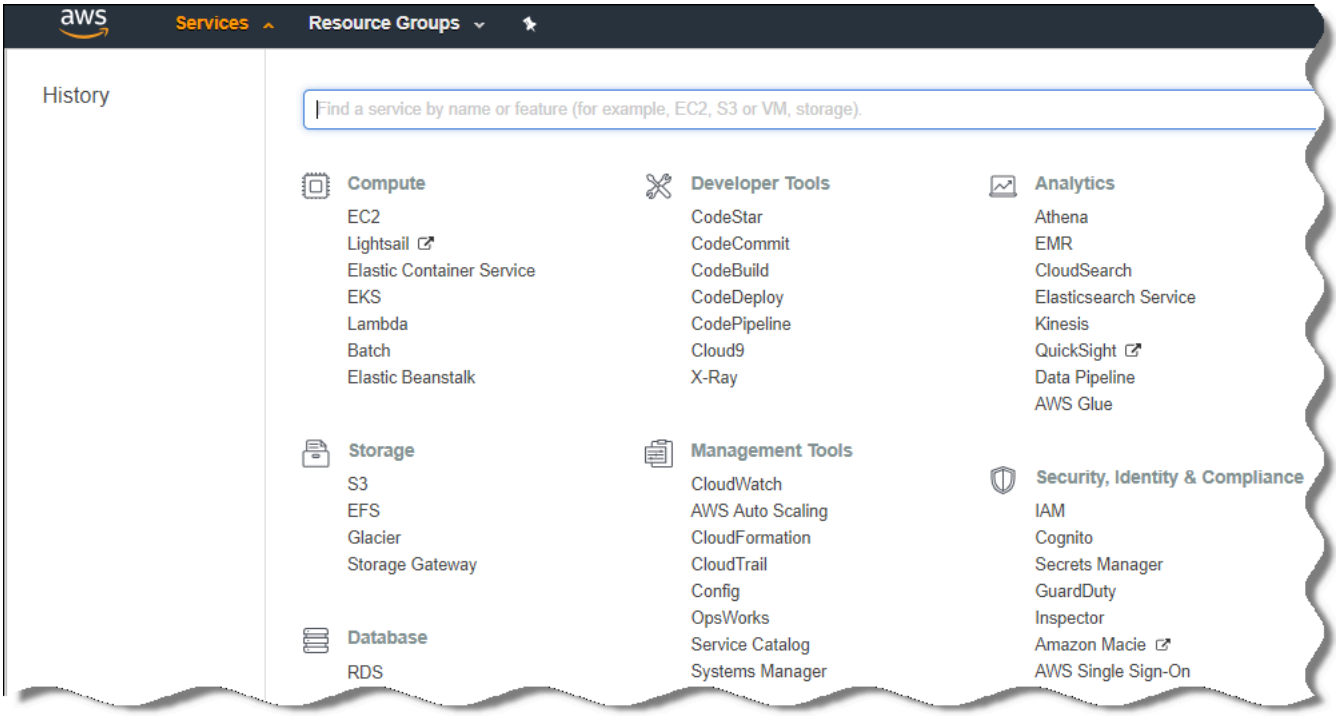
A configuração padrão do grupo de opções no qual você colocou a instância do Amazon RDS não é suficiente para uso com o banco de dados do Kaspersky Security Center. Você precisa adicionar opções para o grupo de opções e criar uma nova função do IAM para uso com o banco de dados.

Para modificar o grupo de opções e criar uma nova função do IAM:

1. Assegure-se de que você está no Console de Gerenciamento AWS (https://console.aws.amazon.com) e efetuou login com sua conta.

2. Na linha de menu, clique em **Serviços**.

   A lista de serviços disponíveis é exibida (consulte a figura abaixo).



Lista de serviços em o Console de Gerenciamento AWS

3. Na lista, selecione RDS.

4. No painel esquerdo, clique em **Grupos de opções**.

   A lista de grupos de opções é exibida.

5. Selecione o grupo de opção no qual você colocou a instância do Amazon RDS e clique no botão **Adicionar opção**.

   A janela **Add option** abre.

6. Na seção da função do IAM, selecione a opção **Criar uma nova função** / **Sim** e digite um nome para a nova função do IAM.

   A função é criada com um conjunto padrão de permissões. Mais tarde, você precisará alterar as permissões.

7. Na seção S3 bucket, realize uma das seguintes ações:

   - Se você não criou uma instância do Amazon S3 bucket para o backup de dados, selecione o link **Criar um novo S3 bucket** e crie um novo S3 bucket usando a interface AWS.

   - Se você já tiver criado uma instância do bucket do Amazon S3 para a tarefa de backup de dados do Servidor de Administração, selecione seu bucket do S3 no menu suspenso.

8. Terminar de adicionar opções clicando no botão após o botão **Adicionar opção** na parte inferior da página.

Você modificou o grupo de opções e criou uma nova função do IAM para uso com o banco de dados RDS.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Modificar permissões para função do IAM para instância de banco de dados do Amazon RDS

Depois de adicionar opções ao grupo de opções, você deve atribuir as permissões necessárias à função do IAM que criou para uso com a instância de banco de dados do Amazon RDS.

Para atribuir as permissões necessárias à função do IAM que você criou para uso com a instância de banco de dados do Amazon RDS:

1. Assegure-se de que você está no Console de Gerenciamento AWS (https://console.aws.amazon.com) e efetuou login com sua conta.

2. Na lista de serviços, selecione **IAM**.

   Uma janela é aberta contendo uma lista de nomes de usuários e um menu que permite a você trabalhar com a ferramenta.

3. No menu, selecione **Roles**.

4. Na lista de funções do IAM exibida no espaço de trabalho, selecione a função que você criou ao adicionar opção ao grupo de opções.

5. Usando a interface AWS, exclua a política **sqlNativeBackup-<date>**.

6. Usando a interface AWS, anexe a política **AmazonS3FullAccess** à função.

As função do IAM é atribuída com as permissões necessárias para uso com o Amazon RDS.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Preparar o Amazon S3 bucket para o banco de dados

Se você planeja usar o banco de dados Amazon Relational Database System (Amazon RDS), precisa criar uma instância do Amazon Simple Storage Service (Amazon S3) bucket onde o Backup regular do banco de dados será armazenado. Para informações sobre o Amazon S3 e sobre S3 buckets, consulte as páginas da Ajuda da Amazon. Para mais informações sobre como criar uma instância do Amazon S3, consulte a página da Ajuda do Amazon S3.

Para criar um Amazon S3 bucket:

1. Verifique e confirme se o Console de Gerenciamento AWS está aberto e se você está conectado com a sua conta.
2. Na lista de serviços AWS, selecione S3.
3. Navegue pelo console para criar um bucket seguindo as instruções do Assistente.
4. Selecione a mesma região em que o seu Servidor de Administração está localizado (ou será localizado).
5. Quando o Assistente finalizar, assegure-se de que o novo bucket aparece na lista de buckets.

Um novo S3 bucket é criado e aparece na lista de buckets. Você tem que especificar esse bucket quando adicionar opções ao grupo de opções. Você também deverá especificar o endereço do S3 bucket no Kaspersky Security Center quando o Kaspersky Security Center criar a tarefa *Backup de dados do Servidor de Administração*.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Migrar o banco de dados para o Amazon RDS

Você pode migrar seu banco de dados do Kaspersky Security Center de um dispositivo local para uma instância do Amazon S3 com suporte ao Amazon RDS. Para fazer isso, você precisa de um S3 bucket para um Banco de dados RDS e de uma Conta de Usuário IAM com a permissão AmazonS3FullAccess para o S3 bucket.

Para executar a migração do banco de dados:

1. Assegure-se de que você criou uma instância do RDS (consulte as páginas de referência do Amazon RDS para mais informações).
2. Em seu Servidor de Administração físico (local), execute o utilitário de Backup da Kaspersky para fazer backup dos dados do Servidor de Administração.

   Você deve certificar-se de que o nome do arquivo é backup.zip.
3. Copie o arquivo de backup.zip para a instância do EC2 na qual o Servidor de Administração está instalado.

Assegure-se de que você tem espaço em disco suficiente na instância do EC2 na qual o Servidor de Administração está instalado. No ambiente AWS, você pode adicionar espaço disponível à sua instância para acomodar o processo de migração do banco de dados.

4. No Servidor de Administração do AWS, inicie novamente o utilitário de Backup da Kaspersky no modo interativo.

   O Assistente de backup e restauração é iniciado.

5. Na etapa **Selecionar ação**, selecione **Restaurar dados do Servidor de Administração** e clique em **Avançar**.

6. Na etapa **Restaurar configurações**, clique no botão **Procurar**, ao lado da **Pasta para armazenamento das cópias de backup**.

7. Na janela **Entrar no Armazenamento Online** exibida, preencha os seguintes campos e clique em **OK**:

   - **Nome do bucket S3**

     O nome do seu S3 bucket.

   - **Pasta de backup**

     Especifique o local da pasta de armazenamento destinada ao backup.

   - **ID da chave de acesso**

     ID da Chave de acesso AWS IAM pertencente ao usuário do IAM que tem as permissões para usar o S3 bucket (a permissão AmazonS3FullAccess).

   - **Chave secreta**

     Chave secreta do IAM AWS pertencente ao usuário do IAM que tem as permissões para usar o S3 bucket (a permissão AmazonS3FullAccess).

8. Selecione a opção **Migrar do backup local**. O botão **Procurar** fica disponível.

9. Clique no botão **Procurar** para escolher a pasta no Servidor de Administração no AWS para a qual você copiou o arquivo de backup.

10. Clique em **Avançar** e conclua o procedimento.

Os seus dados serão restaurados ao Banco de dados RDS usando o S3 bucket. Você pode usar esse banco de dados para trabalho adicional com o Kaspersky Security Center no ambiente AWS.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Trabalhando no ambiente de nuvem Microsoft Azure

Esta seção fornece informações sobre a implementação e manutenção do Kaspersky Security Center em um ambiente de nuvem fornecido por Microsoft Azure, assim como detalhes da implementação da proteção em máquinas virtuais neste ambiente de nuvem.

Em um Kaspersky Security Center que foi implementado a partir de um SKU com base no uso e faturado mensalmente, o Gerenciamento de patches e vulnerabilidades é automaticamente ativado e o Gerenciamento de Dispositivos Móveis não pode ser ativado.

Sobre o trabalho em o Microsoft Azure

Para uso com a plataforma Microsoft Azure e, em particular, comprar aplicativos no Azure Marketplace e criar máquinas virtuais, você precisará de uma assinatura do Azure. Antes de implementar o Servidor de Administração, crie um ID do aplicativo Azure com as permissões necessárias para a instalação de aplicativos em máquinas virtuais.

Se você comprar uma imagem do Kaspersky Security Center no Azure Marketplace, poderá implementar uma máquina virtual com o seu Servidor de Administração do Kaspersky Security Center pronto para uso. Selecione as configurações da máquina virtual, mas você mesmo não precisa instalar o aplicativo. Após a instalação, você pode iniciar o Console de Administração e conectar-se ao Servidor de Administração para começar a trabalhar com o Kaspersky Security Center.

Você também pode usar uma máquina virtual do Azure que tenha um Servidor de Administração do Kaspersky Security Center nela implementado para proteger os dispositivos locais (por exemplo, se você descobrir ser mais fácil fornecer serviços e manutenção em um servidor na nuvem do que em um servidor físico). Se este for o caso, você trabalha com o Servidor de Administração da mesma forma como faria se o Servidor de Administração estivesse instalado em um dispositivo local. Se você não planeja usar ferramentas API Azure, não precisará de um ID do aplicativo Azure. Nesse caso, uma assinatura do Azure é o suficiente.

Criar uma assinatura, ID do aplicativo e senha

Para uso com o Kaspersky Security Center no ambiente do Microsoft Azure, você precisa de uma assinatura do Azure, um ID do aplicativo Azure e a senha do aplicativo Azure. É possível usar uma assinatura existente, se você já tiver uma.

Uma assinatura do Azure concede ao proprietário acesso ao Portal de Gerenciamento da Plataforma Microsoft Azure e aos serviços do Microsoft Azure. O proprietário pode usar a Plataforma Microsoft Azure para gerenciar serviços como o Azure SQL e o Azure Storage.

Para criar uma assinatura do Microsoft Azure,

Vá para https://learn.microsoft.com/en-us/azure/cost-management-billing/manage/create-subscription e siga as instruções fornecidas.

Mais informações sobre como criar uma assinatura estão disponíveis no site da Microsoft. Você obterá um ID de assinatura que, mais tarde, fornecerá ao Kaspersky Security Center em conjunto com o ID do aplicativo e a senha.

Para criar e salvar o ID do aplicativo Azure e a senha:

1. Acesse https://portal.azure.com e assegure-se de fazer login.
2. Seguindo as instruções na página de referência, crie seu ID do aplicativo.
3. Acesse a seção **Chaves** das configurações do aplicativo.

4. Na seção **Chaves**, preencha os campos **Descrição** e **Expira** e deixe o campo **Valor** em branco.

5. Clique em **Salvar**.

   Quando você clica **em Salvar**, o sistema preenche automaticamente o campo **Valor** com uma sequência de caracteres longa. Essa sequência é a sua senha do Aplicativo Azure (por exemplo, yXyPOy6Tre9PYgP/j4XVyJCvepPHk2M/UYJ+QlfFvdU=). A descrição é exibida da forma como você a digitar.

6. Copie a senha e salve-a para, mais tarde, fornecer o ID do aplicativo e a senha ao Kaspersky Security Center.

   Você pode copiar a senha somente quando ela tiver sido criada. Mais tarde, a senha não será exibida e você não conseguirá restaurá-la.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Atribuir uma função ao ID do aplicativo Azure

Se você quiser detectar máquinas virtuais usando descoberta de dispositivos, o ID do aplicativo Azure deverá ter a função Leitor. Se você quer não só detectar, mas também implementar a proteção nas máquinas virtuais, o ID do aplicativo Azure deve ter a função Virtual Machine Contributor.

Siga as instruções no site da Microsoft para atribuir uma função ao ID do aplicativo Azure.

Implementar o Servidor de Administração no Microsoft Azure e selecionar banco de dados

Para implementar o Servidor de Administração no ambiente do Microsoft Azure:

1. Efetue login no Microsoft Azure usando a sua conta.

2. Acesse o portal do Azure.

3. No painel esquerdo, clique no sinal de mais verde.

4. Digite "Kaspersky Hybrid Cloud Security" no campo de pesquisa no menu.

   O Kaspersky Hybrid Cloud Security é uma combinação do Kaspersky Security Center e de dois aplicativos de segurança para a proteção de instâncias: o Kaspersky Endpoint Security for Linux e o Kaspersky Security for Windows Server.

5. Na lista de resultados, selecione o Kaspersky Hybrid Cloud Security ou o Kaspersky Hybrid Cloud Security (BYOL).

   Na parte direita da tela, uma janela de informações é exibida.

6. Leia as informações e clique no botão Criar ao final da janela de informações.

7. Preencha todos os campos necessários. Use as dicas de ferramentas para obter informações e assistência.

8. Ao selecionar o tamanho, selecione uma das opções com três estreladas.

   Na maioria dos casos, 8 gigabytes (GB) de RAM são suficientes. Entretanto, no Azure, você pode aumentar o tamanho da RAM e de outros recursos da máquina virtual a qualquer momento.

9. Ao selecionar um banco de dados, escolha uma da seguintes opções, segundo o seu plano:

   - Local – Se você quiser ter um banco de dados na mesma máquina virtual onde o Servidor de Administração será implementado. O Kaspersky Security Center vem com um banco de dados SQL Server Express. Escolha esta opção se o SQL Server Express for suficiente para as suas necessidades.

   - Novo – Se você quiser ter um novo Banco de dados RDS no ambiente do Azure. Selecione esta opção se você quiser ter um DBMS diferente do SQL Server Express. Seus dados serão transferidos para o ambiente de nuvem, onde permanecerão, e você não terá nenhuma despesa extra.

   - Existente – Se você quiser usar um servidor de banco de dados existente. Neste caso, você precisará especificar a localização. Se esse servidor estiver fora do ambiente do Azure, os dados serão transferidos pela Internet, o que pode resultar em despesas extras.

10. Ao inserir o ID de assinatura, use a assinatura que você criou anteriormente.

    Após a implementação, você pode conectar-se ao Servidor de Administração usando RDP. Você pode usar o Console de Administração para uso com o Servidor de Administração.

Trabalhar com Azure SQL

Esta seção descreve quais ações devem ser tomadas para preparar um banco de dados do Microsoft Azure para o Kaspersky Security Center, preparar uma conta de armazenamento Azure, e migrar um banco de dados existente para o Azure SQL.

SQL Database é um serviço gerenciado de um banco de dados relacional de uso geral no Microsoft Azure.

> Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Criar uma conta de armazenamento Azure

Você precisa criar uma conta de armazenamento no Microsoft Azure para uso com o banco de dados Azure SQL e para scripts de implementação.

Para criar uma conta de armazenamento:

1. Faça login no portal do Azure.

2. No painel esquerdo, selecione **Contas de armazenamento** para prosseguir até a janela **Contas de armazenamento**.

3. Na janela **Contas de armazenamento**, clique no botão **Adicionar** para prosseguir até a janela **Criar conta de armazenamento**.

4. Preencha todos os campos necessários para criar uma conta de armazenamento:

   - Localização: deve ser a mesma que a do Servidor de Administração.
   - Outros campos: você pode deixar os valores padrão.

   Use as dicas de ferramentas para obter informações sobre cada campo.

   Depois que a conta de armazenamento é criada, a lista com suas contas de armazenamento é exibida.

5. Na lista de contas de armazenamento, clique no nome da conta recém-criada para ver as informações sobre essa conta.

6. Assegurar-se de que sabe o nome da conta, o grupo de recursos e as chaves de acesso para essa conta de armazenamento. Você precisará dessas informações para uso com o Kaspersky Security Center.

Você pode consultar o site do Azure para obter ajuda.

Se já tem uma conta de armazenamento, você pode usá-la com o Kaspersky Security Center.

Criar um banco de dados Azure SQL e um servidor SQL

Você precisa de um banco de dados SQL e de um SQL Server no ambiente do Azure.

Para criar um banco de dados Azure SQL e um servidor SQL:

1. Siga as instruções no site do Azure.

   Você poderá criar um novo servidor quando Microsoft Azure solicitar isso; se já tiver um Azure SQL Server, você poderá usá-lo para o Kaspersky Security Center em vez de criar um novo.

2. Depois de criar o banco de dados SQL e o SQL Server, assegure-se de que você sabe os respectivos nomes e grupos de recursos:

   a. Acesse https://portal.azure.com e assegure-se de fazer login.

   b. No painel esquerdo, selecione **SQL databases**.

   c. Clique no nome de um banco de dados na lista de seus bancos de dados.

      A janela de propriedades é exibida.

   d. O nome do banco de dados é o nome do recurso. O nome do grupo de recursos é exibido na seção **Visão geral** da janela de propriedades.

Você precisa do nome do recurso e do grupo de recursos do banco de dados para migrar o banco de dados para o Azure SQL.

Migrar o banco de dados para Azure SQL

Depois de implementar o Servidor de Administração no ambiente do Azure, você poderá migrar o banco de dados do Kaspersky Security Center de um dispositivo local para o Azure SQL. Você precisa de uma conta de armazenamento do Azure para ter um banco de dados Azure SQL. Você também precisa ter o Microsoft SQL Server Data-Tier Application Framework (DacFx) e o SQLSysCLRTypes no Servidor de Administração.

Para executar a migração do banco de dados:

1. Assegure-se ter criado uma conta de armazenamento do Azure.
2. Certifique-se de ter SQLSysCLRTypes e DacFx no Servidor de Administração.

   Você pode baixar o Microsoft SQL Server Data-Tier Application Framework (17.0.1 DacFx) e SQLSysCLRTypes (escolha a versão correspondente à versão do seu SQL Server) no site oficial da Microsoft.
3. Em seu Servidor de Administração físico (local), execute o utilitário de Backup da Kaspersky para fazer backup dos dados do Servidor de Administração com a opção **Migrar para o formato do Azure** ativada.
4. Copie o arquivo de backup para o Servidor de Administração do Azure.

   > Assegure-se de que você tem espaço em disco suficiente na máquina virtual Azure onde o Servidor de Administração está instalado. No ambiente Azure, você pode adicionar espaço em disco às suas máquinas virtuais para acomodar o processo de migração do banco de dados.
5. No Servidor de Administração localizado no ambiente do Microsoft Azure, inicie novamente o utilitário de Backup da Kaspersky no modo interativo.

   O Assistente de backup e restauração é iniciado.
6. Na etapa **Selecionar ação**, selecione **Restaurar dados do Servidor de Administração** e clique em **Avançar**.
7. Na etapa **Restaurar configurações**, clique no botão **Procurar**, ao lado da **Pasta para armazenamento das cópias de backup**.

8. Na janela **Entrar no Armazenamento Online** exibida, preencha os seguintes campos e clique em **OK**:

   - **Nome da conta de armazenamento do Azure**

     Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center.

   - **Pasta de backup**

     Especifique o local da pasta de armazenamento destinada ao backup.

   - **ID de assinatura do Azure**

     Você criou a assinatura no portal do Azure.

   - **Senha do aplicativo Azure**

     Você recebeu a senha quando criou o ID do aplicativo.

     Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

   - **Chave de acesso ao armazenamento do Azure**

     Disponível nas propriedades da conta de armazenamento, na seção Chaves de Acesso. Você pode usar qualquer uma das chaves (key1 ou key2).

   - **Nome do servidor Azure SQL**

     Disponível nas propriedades do Azure SQL Server.

   - **Grupo de recursos do servidor Azure SQL**

     Disponível nas propriedades do Azure SQL Server.

   - **ID do aplicativo Azure**

     Você criou este ID do aplicativo no portal do Azure.

     É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

9. Selecione a opção **Migrar do backup local**.

   O botão **Procurar** fica disponível.

10. Clique no botão **Procurar** para escolher a pasta no Servidor de Administração do Azure na qual você copiou o arquivo de backup.

11. Clique em **Avançar** e conclua o procedimento.

Os seus dados serão restaurados ao banco de dados Azure SQL usando o armazenamento do Azure. Você pode usar este banco de dados para trabalho adicional com o Kaspersky Security Center no ambiente Azure.

Os endereços das páginas da web citados neste documento estão corretos para a data de lançamento do Kaspersky Security Center.

Trabalhando no Google Cloud

Esta seção fornece informações sobre como trabalhar com o Kaspersky Security Center em um ambiente de nuvem fornecido pelo Google.

Criar o e-mail do cliente, ID do projeto e chave privada

É possível usar o Google API com o Kaspersky Security Center na plataforma Google Cloud. É necessária uma conta do Google. Consulte a documentação do Google em https://cloud.google.com para obter mais informações.

Será necessário criar e fornecer ao Kaspersky Security Center as seguintes credenciais:

- **E-mail do cliente**

  O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

- **ID do projeto**

  O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

Trabalhar com o Google Cloud SQL para instância do MySQL

É possível criar um banco de dados no Google Cloud e usar esse banco de dados para o Kaspersky Security Center.

O Kaspersky Security Center funciona com MySQL 5.7 e 5.6. Outras versões do MySQL não foram testadas.

Para criar e configurar um banco de dados MySQL:

Em seu navegador, abra a página https://cloud.google.com/sql/docs/mysql/create-instance#create-2nd-gen e siga as instruções fornecidas.

Ao configurar um banco de dados MySQL, use os seguintes sinalizadores:

- **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

Prerrequisitos para os dispositivos cliente no um ambiente de nuvem necessários para trabalhar com o Kaspersky Security Center

Para os dispositivos nos quais você pretende instalar o Servidor de Administração, o Agente de Rede e aplicativos de segurança da Kaspersky, as seguintes condições devem ser atendidas:

- A configuração de grupos de segurança torna disponíveis as seguinte portas no Servidor de Administração (conjunto mínimo de portas necessárias para a implementação):

  - 8060 HTTP – Para a transferência de pacotes de instalação de Agente de Rede e de pacotes de instalação do aplicativo de segurança do Servidor de Administração para instâncias protegidas
  - 8061 HTTPS – Para a transferência de pacotes de instalação de Agente de Rede e de pacotes de instalação do aplicativo de segurança do Servidor de Administração para instâncias protegidas
  - 13000 TCP – Para transferências de instâncias protegidas e de Servidores de Administração secundários ao Servidor de Administração principal usando SSL
  - 13000 UDP – Para a transferência de informações sobre paralisação de instâncias para o Servidor de Administração
  - 14000 TCP – Para transferências de instâncias protegidas e de Servidores de Administração secundários ao Servidor de Administração principal sem usar SSL
  - 13291 – Para conexão do Console de Administração ao Servidor de Administração
  - 40080 – Para a operação de scripts de implementação

  Você pode configurar grupos de segurança no Console de Gerenciamento AWS ou no portal do Azure. Se você pretende usar o Kaspersky Security Center em uma configuração diferente do padrão, consulte a Base de Conhecimento. Os exemplos de configurações diferentes do padrão incluem não instalar o Console de Administração que no dispositivo do Servidor de Administração, mas instalá-lo em sua estação de trabalho ou utilizar um servidor proxy da KSN.

- A Porta 15000 UDP está disponível em os dispositivos cliente (para o recebimento de solicitações de comunicação com o Servidor de Administração).

- No ambiente de nuvem AWS:
  - Se você planeja usar AWS API, a função do IAM é definida segundo quais aplicativos serão instalados nas instâncias.
  - Em cada instância do Amazon EC2, o Systems Manager Agent (Agente SSM) é instalado e executado.
  - O Agente SSM permite que o Kaspersky Security Center instale automaticamente aplicativos nos dispositivos e grupos de dispositivos sem a cada vez solicitar a confirmação do administrador.
  - Nas instâncias que estejam sendo executadas em um sistema operacional Windows e que foram implementadas a partir de AMIs posteriores a novembro de 2016, o Agente SSM está instalado e em execução. Você terá de instalar manualmente o SSM Agent em todos outros dispositivos. Para obter detalhes sobre a instalação do Agente SSM em dispositivos executando nos sistemas operacionais Windows e Linux, consulte a página de Ajuda do AWS.
- No ambiente de nuvem do Microsoft Azure:
  - Em cada máquina virtual do Azure, o Azure VM Agent é instalado e executado.

    Por padrão, uma nova máquina virtual é criada com o Azure VM Agent e você não precisa instalá-la ou ativá-la manualmente. Consulte as páginas de Ajuda da Microsoft para obter detalhes sobre o Azure VM Agent em dispositivos Windows e em dispositivos Linux.
  - O ID do aplicativo Azure tem as seguintes funções:
    - Leitor (para descobrir máquinas virtuais usando sondagem)
    - Virtual Machine Contributor (para implementar proteção nas máquinas virtuais)
    - SQL Server Contributor (para usar um banco de dados SQL no ambiente do Microsoft Azure)

    Se deseja executar todas estas operações, atribua as três funções à ID do aplicativo Azure.

Criação de pacotes de instalação necessários para configurar o ambiente em nuvem

O assistente Configurar o ambiente em nuvem no Kaspersky Security Center está disponível caso o usuário tenha os pacotes de instalação e plug-ins de gerenciamento para os seguintes programas:

- Kaspersky Endpoint Security for Linux
- Kaspersky Endpoint Security for Windows

  A implementação do Kaspersky Endpoint Security for Windows em um ambiente em nuvem estará disponível após o lançamento da próxima versão do Kaspersky Endpoint Security 12.0 for Windows.
- Kaspersky Security for Windows Server

Esses pacotes de instalação são necessários para instalar os aplicativos nas instâncias ou máquinas virtuais que deseja proteger. Se não tiver esses pacotes de instalação, deverá criá-los. Caso contrário, o assistente de configuração de ambiente em nuvem talvez não funcione.

Para criar pacotes de instalação:

1. Baixe as versões mais recentes dos aplicativos e plugins no site da Kaspersky:
   - O instalador e o plugin de gerenciamento do Kaspersky Security for Windows Server.
   - O instalador, os arquivos para instalação remota por meio do Kaspersky Security Center e o plugin de gerenciamento do Kaspersky Endpoint Security for Linux.
2. Salve todos os arquivos na instância (ou máquina virtual) na qual o Servidor de Administração está instalado.
3. Extraia os arquivos de todos os pacotes.
4. Inicie o Kaspersky Security Center.
5. Na árvore do console, vá para **Avançado** → **Instalação remota** → **Pacotes de instalação** e clique em **Criar pacote de instalação**.
6. Selecione **Criar pacote de instalação do Kaspersky**.
7. Especifique o nome do pacote e o caminho para o instalador do aplicativo: <pasta> \<nome do arquivo>.kud e clique em **Avançar**.
8. Leia o Contrato de Licença do Usuário Final, selecione a opção para confirmar que aceita os termos e clique em **Avançar**.

O pacote de instalação será carregado no Servidor de Administração e estará disponível na lista de pacotes de instalação.

A configuração do ambiente em nuvem ficará disponível assim que os pacotes de instalação forem criados e os plug-ins de gerenciamento forem instalados no Servidor de Administração.

Configuração do ambiente em nuvem

Para configurar o Kaspersky Security Center com o uso deste ambiente, é necessário ter o seguinte:

- Credenciais específicas para um ambiente em nuvem:
  - Uma função do IAM a qual foi concedida o direito de criar uma sondagem do segmento da nuvem ou uma conta de usuário IAM a qual foi concedida o direito de criar uma sondagem do segmento da nuvem (para uso com Amazon Web Services)
  - ID do Aplicativo Azure, senha e assinatura (para uso com Microsoft Azure)
  - E-mail do cliente do Google, ID do projeto e chave privada (para uso com o Google Cloud)
- Pacotes de instalação:
  - Agente de Rede para Windows
  - Agente de Rede para Linux
  - Kaspersky Endpoint Security for Linux

- Plug-in da Web para o Kaspersky Endpoint Security for Linux
- Pelo menos um dos seguintes itens:
  - Pacote de instalação e plug-in da Web para o Kaspersky Endpoint Security for Windows (recomendado)
  - O pacote de instalação e o plugin da Web para o Kaspersky Security for Windows Server

Caso não queira usar os recursos do ambiente em nuvem (se, por exemplo, o usuário quiser gerenciar somente a proteção de dispositivos cliente físicos), é possível fechar Configurar o ambiente em nuvem e executar manualmente o padrão Assistente de início rápido do Servidor de Administração manualmente.

A operação Configurar o ambiente em nuvem inicia automaticamente na primeira conexão com o Servidor de Administração pelo Console de Administração caso o Kaspersky Security Center esteja sendo implementado a partir da imagem pronta para usar. Também é possível iniciar, a qualquer momento e manualmente, o assistente Configurar o ambiente em nuvem.

Para iniciar manualmente o assistente Configurar o ambiente em nuvem:

1. Na árvore do console, selecione o nó do **Servidor de Administração**.
2. No menu de contexto do nó, selecione **Todas as tarefas → Assistente de configuração de ambiente em nuvem**.

A média da sessão de trabalho é de aproximadamente 15 minutos.

Sobre o assistente Configurar o ambiente em nuvem

O assistente Configurar o ambiente em nuvem permite configurar o Kaspersky Security Center enquanto as especificações do trabalho em um ambiente em nuvem são consideradas.

O assistente cria os seguintes objetos:

- Política do Agente de Rede com configurações padrão
- Política para o Kaspersky Endpoint Security for Linux
- Política para o Kaspersky Security for Windows Server
- Grupo de administração para instâncias e uma regra para mover instâncias automaticamente para este grupo de administração
- Para criar uma tarefa de backup dos dados do Servidor de Administração
- Tarefas para instalar a proteção nos dispositivos sendo executados no Linux e Windows
- Tarefas para cada dispositivo gerenciado:
  - Verificação rápida de malware
  - Download de atualização

Caso a opção de licenciamento BYOL tenha sido selecionada, Configurar o ambiente em nuvem também ativa o Kaspersky Security Center com um arquivo de chave ou com um código de ativação e coloca o arquivo de chave ou o código de ativação no armazenamento da licença.

Etapa 1. Selecionando o método de ativação do aplicativo

Este passo não é exibido se você se inscreveu para uma das AMIs prontas para usar (no AWS Marketplace) ou para um SKU cobrado mensalmente com base no uso (no Azure Marketplace). Nesse caso, o assistente passa imediatamente para a próxima etapa. No entanto, você não pode comprar uma AMI pronta para usar para o Google Cloud.

Se você selecionou a opção de licenciamento BYOL para o Kaspersky Security Center, o assistente solicitará que você selecione o método de ativação do aplicativo.

Ative o aplicativo com um código de ativação (ou com um arquivo de chave) para o Kaspersky Security for Virtualization ou para o Kaspersky Hybrid Cloud Security.

Você pode adicionar o aplicativo em uma das seguintes formas:

- Inserindo um código de ativação.

  A ativação on-line será iniciada. Esse processo envolve a verificação do código de ativação especificado, assim como a emissão e ativação de um arquivo de chave.

- Especificando um arquivo de chave.

  O aplicativo verificará o arquivo de chave e o ativará se ele contiver as informações corretas, ou solicitará que você especifique outro arquivo de chave.

O Kaspersky Security Center coloca a chave de licença no armazenamento da licença e marca-a como uma chave automaticamente distribuída em dispositivos gerenciados.

Se você se conectar a uma instância usando o Remote Desktop Connection no Microsoft Windows ou um aplicativo similar, nas propriedades da conexão remota deverá especificar a unidade do dispositivo físico que está usando para se conectar. Isto assegura o acesso da instância aos arquivos no seu dispositivo físico e lhe permite selecionar e especificar o arquivo de chave.

Ao trabalhar com o Kaspersky Security Center implementado por uma AMI paga ou um SKU com base no uso e faturado mensalmente, você não pode adicionar os arquivos de chave nem códigos de ativação ao armazenamento da licença.

Etapa 2. Selecionar o ambiente de nuvem

Selecione o ambiente em nuvem no qual você está implementando o Kaspersky Security Center: AWS, Azure ou Google Cloud.

Etapa 3. Autorização no ambiente de nuvem

AWS

Se você selecionou AWS, especifique que você tem uma função do IAM com os direitos necessários ou forneça ao Kaspersky Security Center uma chave de acesso AWS IAM. A sondagem do segmento da nuvem não é possível sem uma função do IAM ou uma chave de acesso AWS IAM.

Especifique as seguintes configurações para a conexão que será usada para a sondagem adicional do segmento da nuvem:

- **Nome da conexão**

  Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

  Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

  Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

- **Use AWS IAM role**

  Selecione esta opção se você já tiver criado uma função do IAM para o Servidor de Administração para usar os serviços AWS.

- **Use AWS IAM user account**

  Selecione esta opção se você tiver uma conta de Usuário do IAM com as permissões necessárias e será possível inserir uma ID da chave e uma chave secreta.

  - **ID da chave de acesso**

    A ID da chave de acesso IAM é uma sequência de caracteres alfanuméricos. Você recebeu a ID da chave quando você criou a conta de usuário IAM.

    O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

  - **Chave secreta**

    A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

    Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

    O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

Esta conexão é salva nas configurações do aplicativo. É possível criar apenas uma única chave de acesso AWS IAM com Configurar o ambiente em nuvem. Posteriormente, você poderá especificar mais conexões para gerenciar outros segmentos da nuvem.

Se você quiser instalar aplicativos nas instâncias através do Kaspersky Security Center, deverá assegurar-se que sua função do IAM (ou o Usuário do IAM cuja conta está associada com a chave que você estiver inserindo) tenha todas as permissões necessárias.

Azure

Se você selecionou Azure, especifique as seguintes configurações para a conexão que será usada para a sondagem adicional do segmento da nuvem:

- **Nome da conexão**

  Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

  Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

  Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

- **ID do aplicativo Azure**

  Você criou este ID do aplicativo no portal do Azure.

  É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **ID de assinatura do Azure**

  Você criou a assinatura no portal do Azure.

- **Senha do aplicativo Azure**

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

- **Nome da conta de armazenamento do Azure**

  Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center.

- **Chave de acesso ao armazenamento do Azure**

  Você recebeu uma senha (chave) quando criou a conta de armazenamento Azure para uso com o Kaspersky Security Center.

  A chave está disponível na seção "Visão geral da conta de armazenamento Azure", na subseção "Chaves."

Esta conexão é salva nas configurações do aplicativo.

Google Cloud

Se você selecionou Google Cloud, especifique as seguintes configurações para a conexão que será usada para a sondagem adicional do segmento da nuvem:

- **Nome da conexão**

  Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

  Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

  Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

- **E-mail do cliente**

  O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

- **ID do projeto**

  O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

Esta conexão é salva nas configurações do aplicativo.

Etapa 4. Configurar a sincronização com a nuvem e selecionar ações adicionais

Nesta etapa, a sondagem dos segmentos da nuvem inicia e um grupo de administração especial é criado para as instâncias. As instâncias encontradas durante a sondagem são colocados neste grupo. O agendamento da sondagem do segmento da nuvem é configurado (cada 5 minutos por padrão).

Uma regra automática para mover **Sincronizar com a Nuvem** também é criada. Para cada verificação subsequente da rede na nuvem, os dispositivos virtuais detectados serão movidos ao subgrupo correspondente dentro do grupo **Dispositivos gerenciados\Cloud**.

Na página **Sincronização com o segmento da nuvem**, é possível definir as seguintes configurações:

- **Sincronizar a estrutura de grupos de administração com o segmento da nuvem**

  Se essa opção é ativada, o grupo **Nuvem** é automaticamente criado dentro do grupo **Dispositivos gerenciados** e uma descoberta de dispositivos na nuvem é iniciada. As instâncias e máquinas virtuais detectadas durante cada verificação da rede na nuvem são colocadas no grupo Nuvem. A estrutura dos subgrupos de administração dentro deste grupo corresponde à estrutura do seu segmento da nuvem (no AWS, as zonas de disponibilidade e os grupos de posicionamento não são representados na estrutura; no Azure, as sub-redes não são representadas na estrutura). Os dispositivos que não foram identificados como instância no ambiente nuvem estão no grupo **Dispositivos não atribuídos**. Esta estrutura de grupo permite usar tarefas de instalação de grupo para instalar aplicativos antivírus nas instâncias, assim como definir políticas diferentes para grupos diferentes.

  Se esta opção estiver desativada, o grupo **Nuvem** também será criado, e a descoberta de dispositivos de nuvem também será iniciada; contudo, os subgrupos que correspondem à estrutura do segmento da nuvem não serão criados no grupo. Todas as instâncias detectadas estão no grupo de administração **Nuvem**, portanto elas são exibidos em uma lista única. Se o seu trabalho com o Kaspersky Security Center necessitar da sincronização, você pode modificar as propriedades da regra **Sincronizar com a nuvem** e forçá-la. Forçar esta regra alterará a estrutura dos subgrupos no grupo Nuvem para que ele coincida com a estrutura do seu segmento da nuvem.

  Por padrão, esta opção está desativada.

- **Implementar a proteção**

  Se esta opção estiver selecionada, o assistente cria uma tarefa para instalar aplicativos de segurança nas instâncias. Após a conclusão do assistente, o Assistente de implementação da proteção automaticamente inicia nos dispositivos em seus segmentos da nuvem, e você será capaz de instalar o Agente de Rede e aplicativos de segurança neles.

  O Kaspersky Security Center pode executar a implementação com suas ferramentas nativas. Se você não tiver permissões para instalar os aplicativos nas instâncias do EC2 ou nas máquinas virtuais do Azure, você pode configurar a tarefa de **Instalação remota** manualmente e especificar uma conta com as permissões necessárias. Neste caso, a tarefa de Instalação remota não funcionará para os dispositivos descobertos usando API AWS ou Azure. Essa tarefa só funcionará para os dispositivos descobertos usando a sondagem do Active Directory, de domínios do Windows ou de conjuntos de IPs.

  Se esta opção não está selecionada, o Assistente de Implementação da Proteção não é iniciado e as tarefas para instalar aplicativos de segurança nas instâncias não são criadas. Você pode executar manualmente ambas estas ações em outro momento.

Para o Google Cloud, você só pode executar a implementação com as ferramentas nativas do Kaspersky Security Center. Se você selecionou o Google Cloud, a opção **Implementar a proteção** não está disponível.

Etapa 5. Configurando o Kaspersky Security Network para o ambiente de nuvem

Especifique as configurações para encaminhar informações sobre as operações do Kaspersky Security Center à Base de conhecimento da Kaspersky Security Network. Selecione uma das seguintes opções:

- **Concordo em participar da Kaspersky Security Network**

  O Kaspersky Security Center e os aplicativos gerenciados instalados nos dispositivos cliente transferem automaticamente seus detalhes de operação para o Kaspersky Security Network. A participação na Kaspersky Security Network assegura atualizações mais rápidas dos bancos de dados que contêm informações sobre vírus e outras ameaças, que assegura uma resposta mais rápida a ameaças de segurança emergentes.

- **Não concordo em participar da Kaspersky Security Network**

  O Kaspersky Security Center e os aplicativos gerenciados não fornecerão informações ao Kaspersky Security Network.

  Se você selecionar esta opção, o uso da Kaspersky Security Network será desativado.

A Kaspersky recomenda a participação na Kaspersky Security Network.

Etapa 6. Configurando notificações de e-mail no ambiente de nuvem

Configure a entrega de notificações sobre os eventos registrados durante a operação dos aplicativos Kaspersky em virtual dispositivos cliente. Essas configurações serão usadas como as configurações padrão para as políticas de aplicativo.

Para configurar a entrega de notificações sobre os eventos que ocorrem nos aplicativos Kaspersky, use as seguintes configurações:

- **Destinatários (endereços de e-mail)**

  Os endereços de e-mail de usuários aos quais o aplicativo enviará notificações. Você pode inserir um ou vários endereços; se inserir mais de um endereço, separe-os com um ponto-e-vírgula.

- **Servidores SMTP**

  O endereço ou os endereços dos servidores de e-mail da sua organização.

  Se você inserir mais de um endereço, separe-os com um ponto-e-vírgula. Você pode usar os seguintes parâmetros:

  - Endereço IPv4 ou IPv6
  - Nome da rede Windows (nome NetBIOS) do dispositivo
  - Nome de DNS do servidor SMTP

- **Porta do servidor SMTP**

  Número da porta de comunicação do servidor SMTP. Se você usar vários servidores SMTP, a conexão com eles será estabelecida por meio da porta de comunicação especificada. O número da porta padrão é 25.

- **Usar autenticação ESMTP**

  Ativa o suporte da autenticação ESMTP. Após selecionar a caixa de seleção, nos campos **Nome do usuário** e **Senha**, você poderá especificar as configurações de autenticação ESMTP. Por padrão, esta caixa de seleção está desmarcada.

Você pode testar as novas configurações de notificação por e-mail clicando no botão **Enviar mensagem de teste**. Se a mensagem de teste foi recebida com êxito nos endereços especificados no campo **Destinatários (endereços de e-mail)**, as configurações foram corretamente definidas.

Etapa 7. Criando uma configuração inicial de proteção do ambiente de nuvem

Nesta etapa, o Kaspersky Security Center automaticamente cria políticas e tarefas. A janela **Configurar a proteção inicial**, exibe uma lista de políticas e tarefas criadas pelo aplicativo.

Se você usar um banco de dados RDS no ambiente de nuvem do AWS, precisará fornecer ao Kaspersky Security Center o par de chaves de acesso IAM quando a tarefa de backup do Servidor de Administração estiver sendo criada. Neste caso, preencha os seguintes campos:

- **Nome do bucket S3**

  O nome do S3 bucket que você criou para o Backup.

- **ID da chave de acesso**

  Você recebeu o ID da chave (sequência de caracteres alfanuméricos) quando criou a Conta de Usuário do IAM para uso com a instância de armazenamento do S3 bucket.

  O campo está disponível se você selecionou o banco de dados RDS em um S3 bucket.

- **Chave secreta**

  A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

  Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

  O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

Se você usar um banco de dados SQL no ambiente de nuvem do Azure, precisará fornecer ao Kaspersky Security Center as informações sobre o seu Azure SQL Server quando a tarefa de backup do Servidor de Administração estiver sendo criada. Neste caso, preencha os seguintes campos:

- **Nome da conta de armazenamento do Azure**

  Você criou o nome da conta de armazenamento do Azure para uso com o Kaspersky Security Center.

- **ID de assinatura do Azure**

  Você criou a assinatura no portal do Azure.

- **Senha do aplicativo Azure**

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

- **ID do aplicativo Azure**

  Você criou este ID do aplicativo no portal do Azure.

  É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **Nome do servidor Azure SQL**

  O nome e o grupo do recurso estão disponíveis nas propriedades do Azure SQL Server.

- **Grupo de recursos do servidor Azure SQL**

  O nome e o grupo do recurso estão disponíveis nas propriedades do Azure SQL Server.

- **Chave de acesso ao armazenamento do Azure**

  Disponível nas propriedades da conta de armazenamento, na seção Chaves de Acesso. Você pode usar qualquer uma das chaves (key1 ou key2).

Se você estava implementando o Servidor de Administração no Google Cloud, você precisa selecionar a pasta aonde as copias de backup serão armazenadas. Selecione a pasta no seu dispositivo local ou pasta da instância da maquina virtual.

O botão **Avançar** se torna disponível após a criação de todas as políticas e tarefas que são necessárias para a configuração mínima da proteção.

Se um dispositivo no qual as tarefas supostamente sejam executadas não estiver visível ao Servidor de Administração, as tarefas serão iniciadas somente quando o dispositivo ficar visível. Se você criar uma nova instância do EC2 ou uma nova máquina virtual do Azure, pode demorar algum tempo até que ela fique visível para o Servidor de Administração. Se você quiser que o Agente de Rede e os aplicativos de segurança sejam instalados em todos os dispositivos recentemente criados o mais breve possível, assegure-se de que a opção **Executar tarefas ignoradas** seja ativada para as tarefas **Instalar o aplicativo remotamente**. Caso contrário, uma instância/máquina virtual recentemente criada não obterá o Agente de Rede e os aplicativos de segurança até que a tarefa seja iniciada segundo o agendamento.

Etapa 8. Selecione a ação quando o sistema operacional deve ser reiniciado durante a instalação (para o ambiente de nuvem)

Se você tiver anteriormente selecionado **Implementar a proteção**, deverá escolher o que fazer quando o sistema operacional de um dispositivo de destino precisar ser reiniciado. Se não tiver selecionado a opção **Implementar a proteção**, esta etapa será ignorada.

Selecione se as instâncias deverão ser reiniciadas caso o sistema operacional precise ser reiniciado durante a instalação de aplicativos:

- **Não reiniciar o dispositivo**

  Se esta opção for selecionada, o dispositivo não será reiniciado após a instalação do aplicativo de segurança.

- **Reiniciar o dispositivo**

  Se esta opção for selecionada, o dispositivo será reiniciado após a instalação do aplicativo de segurança.

Se você quiser forçar o fechamento de todos os aplicativos em sessões bloqueadas nas instâncias antes do reinício, selecione a caixa de seleção **Forçar fechamento de aplicativos nas sessões bloqueadas**. Se esta caixa de seleção estiver desmarcada, você terá de fechar manualmente todos os aplicativos que em execução nas instâncias bloqueadas.

Etapa 9. Receber atualizações por o Servidor de Administração

Nesta etapa, você pode ver o andamento do download das atualizações necessárias para a operação correta do Servidor de Administração. Você pode clicar no botão **Avançar** sem esperar pela conclusão do download para prosseguir à página final do assistente.

O assistente é concluído.

Configurar a verificação

Para verificar se o Kaspersky Security Center 14.2 está apropriadamente configurado para funcionar no ambiente de nuvem:

1. Inicie o Kaspersky Security Center e assegure-se de que você consegue conectar-se ao Servidor de Administração através do Console de Administração.

2. Na árvore do console, selecione **Dispositivos gerenciados\Cloud**.

3. Ao exibir algum dos subgrupos no grupo **Dispositivos gerenciados\Cloud**, assegure-se de que a guia **Dispositivos** exibe todos os dispositivos daquele subgrupo.

   Se os dispositivos não forem exibidos, você pode manualmente criar armazenamento dos segmentos da nuvem correspondentes para encontrá-los.

4. Assegure-se de que a guia **Políticas** tenha políticas ativas para os seguintes aplicativos:

   - Agente de Rede do Kaspersky Security Center
   - Kaspersky Security for Windows Server
   - Kaspersky Endpoint Security for Linux

   Se eles não estiverem listados, você pode criá-los manualmente.

5. Assegure-se de que a guia **Tarefas** lista as seguintes tarefas:

   - **Backup de dados do Servidor de Administração**
   - **Tarefa de atualização para Windows Server**
   - **Manutenção do Servidor de Administração**
   - **Baixar atualizações no repositório do Servidor de Administração**
   - **Encontrar vulnerabilidades e atualizações necessárias**
   - **Instalar a proteção para o Windows**
   - **Instalar a proteção para o Linux**
   - **Tarefa de Verificação Rápida para o Windows Server**
   - **Verificação Rápida**
   - **Instalar as atualizações para o Linux**

   Se eles não estiverem listados, você pode criá-los manualmente.

O Kaspersky Security Center 14.2 está apropriadamente configurado para funcionar no ambiente de nuvem.

Grupo de dispositivos Nuvem

Você pode gerenciar instâncias ao combiná-las em grupos. Na etapa de configuração inicial do Kaspersky Security Center, o grupo de administração **Dispositivos gerenciados\Cloud** é criado por padrão e os dispositivos na nuvem detectados durante a sondagem são colocados nesse grupo.

Se você selecionou a opção **Sincronizar a estrutura de grupos de administração com o segmento da nuvem** ao configurar a sincronização, a estrutura de subgrupos neste grupo de administração é idêntica à estrutura de seus segmentos de nuvem. (No entanto, na AWS, as zonas de disponibilidade e os grupos de posicionamento não são representados na estrutura; no Microsoft Azure, as sub-redes não são representadas na estrutura.) Os subgrupos vazios dentro do grupo que são detectados durante a pesquisa são excluídos automaticamente.

Também é possível criar manualmente grupos de administração ao combinar todos os dispositivos ou dispositivos específicos.

Por padrão, o grupo Dispositivos gerenciadosDispositivos gerenciados**Nuvem** herda as políticas e tarefas do grupo Dispositivos gerenciadosDispositivos gerenciados. Você pode modificar as configurações se as caixas de seleção **Edição permitida** forem selecionadas nas propriedades das configurações das políticas e tarefas correspondentes.

Sondagem do segmento de rede

As informações sobre a estrutura da rede e dos dispositivos nesta rede são recebidas pelo Servidor de Administração através da sondagem regular de segmentos da nuvem usando as ferramentas AWS API, Azure API ou Google API. O Kaspersky Security Center usa essas informações para atualizar o conteúdo das pastas **Dispositivos não atribuídos** e **Dispositivos gerenciados**. Se você tiver configurado dispositivos a ser movidos automaticamente para grupo de administração, os dispositivos detectados são incluídos nos grupos de administração.

Para permitir que o Servidor de Administração faça a sondagem dos segmentos da nuvem, é necessário ter os direitos fornecidos com uma função do IAM, uma conta de usuário IAM (no AWS), um ID do Aplicativo e senha (no Azure) ou um cliente de e-mail do Google, ID do projeto do Google e chave privada.

Você pode adicionar e excluir conexões, assim como definir o agendamento da sondagem para cada segmento da nuvem.

Adicionar conexões para a sondagem do segmento da nuvem

Para adicionar uma conexão para a sondagem do segmento da nuvem para a lista de conexões disponíveis:

1. Na árvore do console, selecione o nó **Descoberta de dispositivos** → **Cloud**.
2. No espaço de trabalho da janela clique em **Configurar a sondagem**.

   Uma janela Propriedades é aberta contendo uma lista de conexões disponíveis para a sondagem do segmento da nuvem.
3. Clique no botão **Adicionar**.

   A janela **Conexão** se abre.

4. Especifique o nome do ambiente em nuvem para a conexão que será usada para a sondagem adicional do segmento da nuvem:

Ambiente nuvem

O ambiente no qual as instâncias do EC2 (ou máquinas virtuais) estão localizadas pode ser o Amazon Web Services (AWS), Microsoft Azure ou Google Cloud.

Se você selecionou AWS, especifique as seguintes configurações:

- **Nome da conexão**

  Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

  Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

  Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

- **Use AWS IAM role**

  Selecione esta opção se você já tiver criado uma função do IAM para o Servidor de Administração para usar os serviços AWS.

- **Use AWS IAM user account**

  Selecione esta opção se você tiver uma conta de Usuário do IAM com as permissões necessárias e será possível inserir uma ID da chave e uma chave secreta.

  - **ID da chave de acesso**

    A ID da chave de acesso IAM é uma sequência de caracteres alfanuméricos. Você recebeu a ID da chave quando você criou a conta de usuário IAM.

    O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

  - **Chave secreta**

    A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

    Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

    O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

O assistente Configurar o ambiente em nuvem permite especificar somente uma única a chave de acesso AWS IAM. Posteriormente, você poderá especificar mais conexões para gerenciar outros segmentos da nuvem.

Se você selecionou o Azure, especifique as seguintes configurações:

- **Nome da conexão**

  Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

  Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

  Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

- **ID do aplicativo Azure**

  Você criou este ID do aplicativo no portal do Azure.

  É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **ID de assinatura do Azure**

  Você criou a assinatura no portal do Azure.

- **Senha do aplicativo Azure**

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

- **Nome da conta de armazenamento do Azure**

  Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center.

- **Chave de acesso ao armazenamento do Azure**

  Você recebeu uma senha (chave) quando criou a conta de armazenamento Azure para uso com o Kaspersky Security Center.

  A chave está disponível na seção "Visão geral da conta de armazenamento Azure", na subseção "Chaves."

Se você selecionou o Google Cloud, especifique as seguintes configurações:

- **Nome da conexão**

  Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

  Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

  Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

- **E-mail do cliente**

  O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

- **ID do projeto**

  O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

5. Se você quiser, selecione **Definir agendamento da sondagem** e altere as configurações padrão.

   A conexão é salva nas configurações do aplicativo.

Após o novo segmento na nuvem ter sido amostrado pela primeira vez, um subgrupo que corresponde àquele segmento aparece no grupo de administração **Dispositivos gerenciados\Cloud**.

Se você especificar as credenciais incorretas, nenhuma instância será encontrada durante a amostragem do segmento na nuvem e um novo subgrupo não aparecerá no grupo de administração **Dispositivos gerenciados\Cloud**.

Excluir conexões da sondagem do segmento da nuvem

Se você não tem de amostrar um segmento da nuvem específico, poderá excluir a conexão correspondente àquele segmento da lista de conexões disponíveis. Você também pode excluir uma conexão se, por exemplo, as permissões para amostrar um segmento da nuvem tenham sido transferidas para o outro usuário AWS IAM com uma chave diferente.

Para excluir uma conexão:

1. Na árvore do console, selecione o nó **Descoberta de dispositivos → Cloud**.
2. No espaço de trabalho da janela, selecione **Configurar a sondagem**.

   Uma janela é aberta contendo uma lista de conexões disponíveis para a sondagem do segmento da nuvem.
3. Selecione o conexão que você quer excluir e clique no botão **Excluir** na parte direita da janela.
4. Na janela que se abre, clique no botão **OK** para confirmar a sua seleção.

Se você estiver excluindo componentes da lista de conexões disponíveis, os dispositivos que estão dentro dos segmentos correspondentes são automaticamente excluídos dos grupos de administração correspondentes.

Configurar o agendamento da sondagem

A amostragem do segmento da nuvem é executada segundo um agendamento. Você pode definir a frequência de sondagem.

A frequência de sondagem é automaticamente definida em 5 minutos nas definições Configurar o ambiente em nuvem. É possível alterar esse valor a qualquer momento e definir outro agendamento. Contudo, não é recomendado configurar a execução da sondagem mais frequentemente do que a cada 5 minutos porque isso pode levar a erros na operação da API.

Para configurar um agendamento da sondagem do segmento da nuvem:

1. Na árvore do console, selecione o nó **Descoberta de dispositivos → Cloud**.
2. No espaço de trabalho, clique em **Configurar a sondagem**.

   A janela Propriedades da nuvem é exibida.
3. Na lista, selecione a conexão desejada e clique no botão **Propriedades**.

   A janela de propriedades da conexão é aberta.
4. Na janela de propriedades, clique no link **Definir agendamento da sondagem**.

   A janela **Agendamento** será aberta.

5. Defina as seguintes configurações:

- **Início agendado**

  Opções de agendamento da sondagem:

  - A cada N dias

    A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

    Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

  - A cada N minutos

    A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

    Por padrão, a sondagem é executada a cada cinco minutos, iniciando na hora atual do sistema.

  - Por dias da semana

    A sondagem é executada regularmente, nos dias da semana e na hora especificados.

    Por padrão, a sondagem é executada todas as sextas-feiras às 18h.

  - Todos os meses em dias especificados das semanas selecionadas

    A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

    Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- Executar tarefas ignoradas

  Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

  Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

  Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

  Por padrão, esta opção está ativada.

6. Clique em **OK** para salvar as alterações.

O agendamento da sondagem é configurado e salvo.

Instalar aplicativos em dispositivos no ambiente de nuvem

Você pode instalar os seguintes aplicativos Kaspersky em dispositivos no ambiente de nuvem: Kaspersky Security for Windows Server (para dispositivos Windows) e Kaspersky Endpoint Security for Linux (para dispositivos Linux).

Os dispositivos cliente nos quais você pretende instalar a proteção devem atender os requisitos para a operação do Kaspersky Security Center em um ambiente de nuvem. Você deve ter uma licença válida para instalar aplicativos em instâncias do AWS, máquinas virtuais do Microsoft Azure ou instâncias de máquinas virtuais Google.

O Kaspersky Security Center 14.2 suporta as seguintes cenários:

- Um dispositivo cliente é descoberto através de uma API. A instalação é executada através de uma API. Para ambientes em nuvem da AWS e do Azure, esse cenário é compatível.
- Um dispositivo cliente é descoberto através de sondagem do Active Directory, de domínios do Windows ou de conjuntos de IPs; a instalação é executada através do Kaspersky Security Center.
- Um dispositivo cliente é descoberto através da API Google. A instalação é executada através d o Kaspersky Security Center. Para o Google Cloud, apenas esse cenário é compatível.

Outras formas de instalação dos aplicativos não têm suporte.

Para instalar aplicativos em dispositivos virtuais, use pacotes de instalação.

Para criar uma tarefa para a instalação remota do aplicativo em instâncias usando AWS API ou Azure API:

1. Na árvore do console, selecione a pasta **Tarefas**.
2. Clique no botão **Nova tarefa**.

   O Assistente para novas tarefas inicia. Siga as instruções do Assistente.
3. Na página **Selecionar o tipo de tarefa**, selecione **Instalar o aplicativo remotamente** como o tipo de tarefa.

4. Na página **Selecionar dispositivos**, selecione os dispositivos relevantes no grupo **Dispositivos gerenciados\Cloud**.

5. Se o Agente de Rede ainda não tiver sido instalado nos dispositivos nos quais você está pretendendo instalar o aplicativo, na página **Selecionar uma conta para executar a tarefa** selecione **Conta necessária (Agente de Rede não é usado)** e clique no botão **Adicionar** na parte direita da janela. No menu que aparece, o selecionado do seguinte:

   - **Conta na nuvem**

     Selecione esta opção se você quiser instalar aplicativos em instâncias no AWS e tiver uma Chave de acesso AWS IAM com as permissões necessárias, mas não tiver uma função do IAM. Selecione também esta opção se você deseja instalar aplicativos em dispositivos no ambiente do Azure.

     Na janela que se abre, forneça ao Kaspersky Security Center as credenciais que lhe concedem direitos de instalar aplicativos nos dispositivos relevantes.

     Selecione o ambiente de nuvem: AWS ou Azure.

     No campo **Nome da conta**, digite um nome para essas credenciais. Este nome será exibido na lista das contas a executarem a tarefa.

     Se você selecionou AWS, nos campos **ID da chave de acesso** e **Chave secreta**, insira as credenciais para a Conta de Usuário do IAM que tem os direitos para instalar aplicativos nos dispositivos especificados.

     Se você selecionou Azure, nos campos **ID de assinatura do Azure** e **Senha do Aplicativo Azure**, insira as credenciais da conta do Azure que tem os direitos para instalar aplicativos nos dispositivos especificados.

     Se você especificar as credenciais incorretas, a tarefa de instalação remota será encerrada com um erro nos dispositivos para os quais foi agendada.

   - **Conta**

     Para instâncias executando o Windows, selecione esta opção caso você não pretenda instalar o aplicativo usando as ferramentas da API do AWS ou do Azure. Neste caso, assegure-se de que os dispositivos no segmento da nuvem atendem às condições necessárias. O Kaspersky Security Center instala aplicativos por si só, sem usar o AWS API ou Azure API.

     Se você especificar os dados incorretos, a tarefa de instalação remota será encerrada com um erro nos dispositivos para os quais foi agendada.

   - **Função do IAM**

     Selecione esta opção se você deseja instalar aplicativos nas instâncias no ambiente AWS e tiver uma função do IAM com os direitos necessários.

     Se você selecionar esta opção, mas não tiver uma função do IAM com os direitos necessários, a tarefa de instalação remota será encerrada com um erro nos dispositivos para os quais foi agendada.

   - **Certificado SSH**

Para instâncias executando o Linux, selecione esta opção se você não pretende instalar o aplicativo usando as ferramentas da AWS API ou da Azure API. Neste caso, assegure-se de que os dispositivos no segmento da nuvem atendem às condições necessárias. O Kaspersky Security Center instala aplicativos por si só, sem usar o AWS API ou Azure API.

Para especificar a chave privada do certificado SSH, você pode gerá-la usando o utilitário ssh-keygen. Observe que o Kaspersky Security Center é compatível com o formato PEM de chaves privadas, mas o utilitário ssh-keygen gera chaves SSH no formato OPENSSH por padrão. O formato OPENSSH não é compatível com o Kaspersky Security Center. Para criar uma chave privada no formato PEM compatível, adicione a opção `-m PEM` no comando ssh-keygen. Por exemplo:

```
ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail do usuário>"
```

Você pode fornecer múltiplos credenciais clicando no botão **Adicionar** para cada uma nova. Se segmentos da nuvem diferentes exigirem credenciais diferentes, forneça as credenciais para todos os segmentos.

Após a conclusão do assistente, a tarefa para a instalação remota do aplicativo aparece na lista de tarefas no espaço de trabalho da pasta **Tarefas**.

No Microsoft Azure, a instalação remota de aplicativos de segurança em uma máquina virtual pode resultar na exclusão da Extensão de Script Personalizada instalada nesta máquina virtual.

Exibir as propriedades de dispositivos de nuvem

Para visualizar as propriedades de um dispositivo na nuvem:

1. Na árvore do console, no nó **Descoberta de dispositivos** → **Nuvem**, selecione o subnó que corresponde ao grupo no qual a instância relevante está localizada.

   Se você não estiver ciente do grupo no qual o dispositivo virtual relevante está localizado, use a função de pesquisa:

   a. Clique com o botão direito no nome do nó **Dispositivos gerenciados** → **Nuvem** e, em seguida, selecione **Pesquisar** no menu de contexto.

   b. Na janela que se abre, execute uma pesquisa.

      Se um dispositivo existir que atenda os critérios que você define, o seu nome e os detalhes serão exibidos na parte inferior da janela.

2. Clique com o botão direito do mouse no nome do nó relevante. No menu de contexto, selecione **Propriedades**.

   Na janela que se abre, as propriedades do objeto são exibidas.

   A seção **Informações do sistema** → **Informações gerais do sistema** contém as propriedades específicas para os dispositivos no ambiente de nuvem:

   - **Dispositivo descoberto usando API** (**AWS**, **Azure** ou **Google Cloud**; se o dispositivo não puder ser detectado usando ferramentas de API, o valor **Não** é exibido).
   - **Região da nuvem**.
   - **VPC na nuvem** (apenas para dispositivos AWS e Google Cloud).
   - **Zona de disponibilidade da nuvem** (apenas para dispositivos AWS e Google Cloud).
   - **Sub-rede da nuvem**.
   - **Cloud Placement Group** (essa unidade será exibida apenas se a instância pertencer a um grupo de posicionamento; caso contrário, não será exibida).

Você pode clicar no botão **Exportar para arquivo** para exportar estas informações para um arquivo .csv ou .txt.

Sincronização com o nuvem

Durante a operação de Configurar o ambiente em nuvem, a regra sincronizar com a nuvem é criada automaticamente. Esta regra lhe permite mover automaticamente as instâncias detectadas em cada sondagem, do grupo **Dispositivos não atribuídos** para o grupo **Dispositivos gerenciados\Cloud**, para tornar estas instâncias disponíveis para o gerenciamento centralizado. Por padrão, a regra está ativa após ter sido criada. Você pode desativar, modificar ou forçar a regra a qualquer momento.

Para editar as propriedades da regra de Sincronizar com a nuvem e/ou forçar a regra:

1. No árvore do console, clique com o botão direito do mouse no nome do nó **Descoberta de dispositivos**.
2. No menu de contexto, selecione **Propriedades**.
3. Na janela de **Propriedades** que se abre, no painel **Seções**, selecione **Mover dispositivos**.
4. Na lista de regras para migrar dispositivos no espaço de trabalho, selecione a regra **Sincronizar com o Nuvem** e clique no botão **Propriedades** na parte inferior da janela.

   A janela Propriedades da regra é aberta.

5. Se necessário, especifique as seguintes configurações no grupo de configurações **Segmentos da nuvem**:

- Device is in cloud segment

  A regra só é aplicada aos dispositivos que estão no segmento da nuvem selecionado. Caso contrário, a regar se aplica a todos os dispositivos que tenham sido descobertos.

  Por padrão, esta opção está selecionada.

  - Incluir objetos filhos

    A regra se aplica a todos os dispositivos no segmento selecionado e em todas as subsecções da nuvem aninhadas. Caso contrário, a regra só é aplicada aos dispositivos que estão no segmento raiz.

    Por padrão, esta opção está selecionada.

  - Mover dispositivos de objetos aninhados para subgrupos correspondentes

    Se essa opção é ativada, os dispositivos de objetos aninhados são automaticamente movidos aos subgrupos que correspondem à sua estrutura.

    Se essa opção é desativada, os dispositivos de objetos aninhados são automaticamente movidos para a raiz do subgrupo Nuvem sem nenhuma ramificação adicional.

    Por padrão, esta opção está ativada.

    - Criar subgrupos correspondentes a contêineres de dispositivos recém-detectados

      Se esta opção estiver ativada, quando a estrutura do grupo **Dispositivos gerenciados\Nuvem** não tiver nenhum subgrupo que corresponda à seção que contém o dispositivo, o Kaspersky Security Center criará os subgrupos. Por exemplo, se uma nova sub-rede for descoberta durante a descoberta de dispositivos, um novo grupo com o mesmo nome será criado abaixo do grupo **Dispositivos gerenciados\Nuvem**.

      Se esta opção estiver desativada, o Kaspersky Security Center não criará nenhum novo subgrupo. Por exemplo, se uma nova sub-rede for descoberta durante a sondagem da rede, um novo grupo com o mesmo nome não será criado sob o grupo **Dispositivos gerenciados\Nuvem**, e os dispositivos naquela sub-rede serão movidos para o grupo **Dispositivos gerenciados\Nuvem**.

      Por padrão, esta opção está ativada.

    - Excluir subgrupos para os quais nenhuma correspondência foi encontrada nos segmentos da nuvem

      Se esta opção estiver ativada, o aplicativo excluirá do grupo Nuvem todos os subgrupos que não correspondem a nenhum dos objetos da nuvem existentes.

      Se esta opção estiver desativada, os subgrupos que não correspondem a nenhum dos objetos da nuvem existentes serão mantidos.

      Por padrão, esta opção está ativada.

  Caso a opção **Sincronizar com a Nuvem** tenha sido ativada ao executar Configurar o ambiente em nuvem, a regra sincronizar com a nuvem será criada com as caixas de seleção **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente** e **Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem** marcadas.

Se você não ativou a opção **Sincronizar com Nuvem**, a regra Sincronizar com a Nuvem será criada com essas opções desativadas (desmarcadas). Se o seu trabalho com o Kaspersky Security Center precisar que a estrutura de subgrupos no subgrupo **Dispositivos gerenciados\Nuvem** coincida com a estrutura dos segmentos da nuvem, ative as opções **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente** e **Excluir subgrupos aos quais correspondência alguma foi achada nos segmentos da nuvem** nas propriedades da regra e, a seguir, force a regra.

6. Na lista suspensa **Dispositivo encontrado usando a API**, selecione um dos seguintes valores:
   - **AWS**. O dispositivo é detectado usando a AWS API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do AWS.
   - **Azure**. O dispositivo é detectado usando a Azure API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do Azure.
   - **Google Cloud.** O dispositivo é descoberto usando a Google API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do Google.
   - **Não**. O dispositivo não pode ser detectado usando API do AWS, Azure ou Google, ou seja, está fora do ambiente em nuvem ou está no ambiente em nuvem, mas não pode ser detectado usando uma API.
7. **Nenhum valor**. Esta condição não se aplica. Se necessário, defina outras propriedades da regra em outras seções.
8. Se necessário, force a regra ao clicar no botão **Forçar** na parte inferior da janela.

   O Assistente de execução de regras é iniciado. Siga as instruções do Assistente. Após a conclusão do assistente, a regra será executada e a estrutura de subgrupos no subgrupo **Dispositivos gerenciados\Cloud** vai coincidir com a estrutura dos segmentos da nuvem.
9. Clique no botão **OK**.

As propriedades são configuradas e salvas.

Para desativar a regra Sincronizar com o Nuvem:

1. No árvore do console, clique com o botão direito do mouse no nome do nó **Descoberta de dispositivos**.
2. No menu de contexto, selecione **Propriedades**.
3. Na janela de **Propriedades** que se abre, no painel **Seções**, selecione **Mover dispositivos**.
4. Na lista de regras para mover o dispositivo, no espaço de trabalho, desative (desmarque) a opção **Sincronizar com a Nuvem** e clique em **OK**.

A regra é desativada e não será mais aplicada.

Implementação do Kaspersky Security Center no Yandex.Cloud

É possível implementar o Kaspersky Security Center no Yandex.Cloud. Apenas o modo pay-per-use está disponível; não há suporte para bancos de dados na nuvem.

No Yandex.Cloud, os seguintes métodos de implementação de aplicativos de segurança estão disponíveis:

- Por meio nativo do Kaspersky Security Center, ou seja, utilizando a tarefa de *Instalação remota* (a implementação dos programas de segurança só é possível se o Servidor de Administração e as máquinas virtuais a serem protegidas estiverem no mesmo segmento de rede)

- Por meio de scripts de implementação

Para a implementação do Kaspersky Security Center no Yandex.Cloud, você deve ter uma conta de serviço no Yandex.Cloud. É necessário conceder a essa conta a permissão marketplace.meteringAgent e associá-la à máquina virtual (consulte https://cloud.yandex.com/en para obter detalhes).

Apêndices

Esta seção fornece informações de referência e fatos adicionais relativas ao uso do Kaspersky Security Center.

Recursos avançados

Esta seção descreve uma faixa de opções adicionais do Kaspersky Security Center, elaboradas para expandir a funcionalidade do gerenciamento centralizado de aplicativos nos dispositivos.

Automação de operação do Kaspersky Security Center. Utilitário klakaut

Você pode automatizar a operação do Kaspersky Security Center usando o utilitário klakaut. O utilitário klakaut e um sistema de Ajuda para o mesmo estão localizados na pasta de instalação do Kaspersky Security Center.

Ferramentas personalizadas

O Kaspersky Security Center permite criar uma lista de *ferramentas personalizadas* (aqui referido como *ferramentas*), ou seja, os aplicativos ativados para um dispositivo cliente a partir no Console de Administração através do grupo **Ferramentas personalizadas** no menu de contexto. Cada ferramenta na lista será associada com um comando de menu separado, o qual o Console de Administração utiliza para iniciar o aplicativo correspondente àquela ferramenta.

O aplicativo é iniciado na estação de trabalho do administrador. O aplicativo pode aceitar os atributos de um dispositivo cliente remoto como opções da linha de comando (nome NetBIOS, nome DNS, endereço IP). A conexão ao dispositivo remoto pode ser estabelecida usando uma conexão de túnel.

Por padrão, a lista de ferramentas personalizadas contém os seguintes programas de serviço para cada dispositivo cliente:

- **Diagnóstico remoto** é um utilitário para o diagnóstico remoto do Kaspersky Security Center.
- **Área de trabalho remota** é um componente padrão do Microsoft Windows denominado Conexão com a área de trabalho remota.
- **Gerenciamento de Computadores** é um componente padrão do Microsoft Windows.

Para adicionar ou remover ferramentas personalizadas, ou para editar suas configurações,

No menu de contexto do dispositivo cliente, selecione **Ferramentas personalizadas → Configurar ferramentas personalizadas**.

A janela **Ferramentas personalizadas** se abre. Nesta janela, é possível adicionar ferramentas personalizadas ou editar suas configurações usando os botões **Adicionar** e **Modificar**. Para remover uma ferramenta personalizada, clique no botão de remoção com o ícone de cruz vermelha ( ).

Modo de clonagem do disco do Agente de Rede

Clonar o disco rígido de um dispositivo de referência é um método popular de instalação de software em novos dispositivo. Se o Agente de Rede estiver sendo executado no modo padrão no disco rígido do dispositivo de referência, o seguinte problema surge:

Após a imagem do disco de referência com o Agente de Rede tiver sido implementada em novos dispositivos, eles são exibidos no Console de Administração com um ícone único. Este problema surge porque o procedimento de clonagem causa que os novos dispositivos mantenham dados internos idênticos, que permitem ao Servidor de Administração associar um dispositivo com um ícone no Console de Administração.

O *Modo de clonagem do disco do Agente de Rede* especial permite evitar os problemas com uma exibição incorreta de novos dispositivos no Console de Administração após a clonagem. Use este modo ao implementar o software (com o Agente de Rede) em novos dispositivos clonando o disco.

No modo de clonagem do disco, o Agente de Rede continua a ser executado, mas ele não se conecta ao Servidor de Administração. Ao sair do modo de clonagem, o Agente de Rede exclui os dados internos, que fazem com que o Servidor de Administração associe múltiplos dispositivos com um ícone único no Console de Administração. Para concluir a clonagem da imagem do dispositivo de referência, os novos dispositivos são exibidos no Console de Administração corretamente (sob ícones individuais).

Cenário de uso do modo de clonagem do disco do Agente de Rede

1. O administrador instala o Agente de Rede no dispositivo de referência.
2. O administrador verifica a conexão do Agente de Rede com o Servidor de Administração usando o utilitário klnagchk.
3. O administrador ativa o modo de clonagem do disco do Agente de rede.
4. O administrador instala software e os patches no dispositivo, e reinicia-o quantas vezes for necessário.

5. O administrador clona o disco rígido do dispositivo de referência em qualquer número de dispositivos.

6. Cada cópia clonada deve atender as seguintes condições:

   a. O nome do dispositivo precisa ser alterado.

   b. O dispositivo deve ser reiniciado.

   c. O modo de clonagem de disco deve ser desativado.

Ativar e desativar o modo de clonagem do disco usando o utilitário klmover

Para ativar ou desativar o modo de clonagem do disco do Agente de rede:

1. Execute o utilitário klmover no dispositivo com o Agente de Rede instalado que você precisar clonar.

   O utilitário klmover está localizado na pasta Instalação do Agente de Rede.

2. Para ativar o modo de clonagem do disco, insira o seguinte comando no prompt de comando do Windows:

   `klmover -cloningmode 1`

   O Agente de Rede alterna para o modo de clonagem do disco.

3. Para solicitar o status atual do modo de clonagem do disco, insira o seguinte comando no prompt de comando:

   `klmover -cloningmode`

   A janela do utilitário mostra se o modo de clonagem do disco está ou não ativado.

4. Para desativar o modo de clonagem do disco, insira o seguinte comando na linha de comando do utilitário:

   `klmover -cloningmode 0`

Preparando um dispositivo de referência com o Agente de Rede instalado para criar uma imagem do sistema operacional

Você pode criar uma imagem do sistema operacional de um dispositivo de referência com o Agente de Rede instalado e depois implementar a imagem nos dispositivos em rede. Nesse caso, você cria uma imagem do sistema operacional de um dispositivo de referência no qual o Agente de Rede ainda não foi iniciado. Se você iniciar o Agente de Rede em um dispositivo de referência antes de criar uma imagem do sistema operacional, a identificação do Servidor de Administração dos dispositivos implementados a partir de uma imagem do sistema operacional do dispositivo de referência será problemática.

Para preparar o dispositivo de referência para criar uma imagem do sistema operacional:

1. Assegure-se de que o sistema operacional Windows esteja instalado no dispositivo de referência e instale o outro software necessário nesse dispositivo.

2. No dispositivo de referência, nas configurações do Windows Network Connections, desconecte o dispositivo de referência da rede em que o Kaspersky Security Center está instalado.

3. No dispositivo de referência, inicie a instalação local do Agente de Rede usando o arquivo setup.exe.

   O Assistente de instalação do Agente de Rede do Kaspersky Security Center é iniciado. Siga as instruções do Assistente.

4. Na página **Servidor de Administração** do assistente, especifique o endereço IP do Servidor de Administração.

   Se você não souber o endereço exato do Servidor de Administração, insira localhost. Você pode alterar o endereço IP mais tarde usando o utilitário klmover com a chave `-address`.

5. Na página **Iniciar aplicativo** do assistente, desative a opção **Iniciar o aplicativo durante a instalação**.

6. Quando a instalação do Agente de Rede estiver concluída, não reinicie o dispositivo antes de criar uma imagem do sistema operacional.

   Se você reiniciar o dispositivo, precisará repetir todo o processo de preparação de um dispositivo de referência para criar uma imagem do sistema operacional.

7. No dispositivo de referência, na linha de comando, inicie o utilitário sysprep e execute o seguinte comando: `sysprep.exe /generalize /oobe /shutdown`.

O dispositivo de referência está pronto para criar uma imagem do sistema operacional.

Para configurar o recebimento de mensagens do Monitor de integridade do arquivo

Aplicativos gerenciados, tal como o Kaspersky Security for Windows Server ou Kaspersky Security for Virtualization Light Agent enviam mensagens do Monitor de integridade para o Kaspersky Security Center. O Kaspersky Security Center também lhe permite monitorar qualquer modificação de componentes de sistemas críticos e importantes (tal como Servidores da Web e Caixas Eletrônicos) e prontamente responder a violações da integridade de tais sistemas. Para estes propósitos, você pode receber mensagens do componente Monitor de integridade do arquivo. O componente Monitor de integridade do arquivo lhe permite monitorar não somente o sistema de arquivos de um dispositivo, mas também suas entradas do registro, status do Firewall e o status do hardware conectado.

Você tem de configurar o Kaspersky Security Center para receber as mensagens do Monitor de integridade do arquivo sem usar o Kaspersky Security for Windows Server ou o Kaspersky Security for Virtualization Light Agent.

Para configurar o recebimento de mensagens do Monitor de integridade do arquivo:

1. Abra o registro do sistema do dispositivo cliente no qual o Servidor de Administração está instalado (por exemplo, usando o comando regedit no menu **Iniciar** → **Executar**).

2. Vá ao seguinte hive:

   - Para sistemas de 32 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags

   - Para sistemas de 64 bits:

     HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerF

3. Criar chaves:

   - Crie a chave KLSRV_EVP_FIM_PERIOD_SEC para especificar o período do tempo para contar o número de eventos processados. Especificar as seguintes configurações:

     a. Especificar KLSRV_EVP_FIM_PERIOD_SEC como o nome de chave.

     b. Especifique DWORD como o tipo de chave.

     c. Especifique uma faixa de valores para o intervalo de tempo de 43 200 a 172 800 segundos. Por padrão, o intervalo de tempo é de 86 400 segundos.

   - Crie a chave KLSRV_EVP_FIM_LIMIT para limitar o número de eventos recebidos no intervalo de tempo especificado. Especificar as seguintes configurações:

     a. Especificar KLSRV_EVP_FIM_LIMIT como o nome de chave.

     b. Especifique DWORD como o tipo de chave.

     c. Especifique uma faixa de valores de eventos recebidos de 2 000 a 50 000. O número predefinido de eventos é 20 000.

   - Crie a chave KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC para contar os eventos com precisão até um intervalo de tempo específico. Especificar as seguintes configurações:

     a. Especificar KLSRV_EVP_FIM_PERIOD_ACCURACY_SEC como o nome de chave.

     b. Especifique DWORD como o tipo de chave.

     c. Especifique uma faixa de valores de 120 a 600 segundos. O intervalo de tempo predefinido é de 300 segundos.

   - Crie a chave KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC para que, depois do período de tempo especificado, o aplicativo possa verificar se o número de eventos processados ao longo do intervalo de tempo resulta ser menos do que o limite especificado. Esta verificação é executada para ao alcançar o limite para receber eventos. Se esta condição for atendida, o aplicativo retoma a ação de salvar os eventos no banco de dados. Especificar as seguintes configurações:

     a. Especificar KLSRV_EVP_FIM_OVERFLOW_LATENCY_SEC como o nome de chave.

     b. Especifique DWORD como o tipo de chave.

     c. Especifique uma faixa de valores de 600 a 3 600 segundos. O intervalo de tempo predefinido é de 1 800 segundos.

   Se as chaves não forem criadas, os valores padrões serão usados.

4. Reinicie o serviço do Servidor de Administração.

Os limites na recepção de eventos do componente Monitor de integridade do arquivo serão configurados. Você pode visualizar os resultados do componente File Integrity Monitor nos relatórios denominados **10 regras do Monitor de integridade de arquivos/Monitor de integridade de arquivos acionadas com maior frequência nos dispositivos** e **10 dispositivos com acionamento mais frequente das regras do Monitor de integridade de arquivos/Monitor de integridade de arquivos**.

Manutenção do Servidor de Administração

A manutenção do Servidor de Administração permite liberar espaço na pasta do Servidor de Administração e reduzir o volume do banco de dados excluindo objetos que não são mais necessários. Isso ajuda a melhorar o desempenho e a confiabilidade operacional do aplicativo. Recomendamos que você execute a manutenção no Servidor de Administração pelo menos uma vez por semana.

A manutenção do Servidor de Administração é executada usando uma tarefa dedicada. O aplicativo executa as seguintes ações ao efetuar a manutenção do Servidor de Administração:

- Exclui pastas e arquivos desnecessários da pasta de armazenamento.
- Exclui registros desnecessários das tabelas (também conhecidos como "ponteiros pendentes").
- Limpa o cache.
- Mantém o banco de dados (se você usar o SQL Server ou PostgreSQL como um DBMS):
  - Verifica se há erros no banco de dados (disponível somente para o SQL Server).
  - Reorganiza os índices do banco de dados.
  - Atualiza as estatísticas do banco de dados.
  - Diminui o banco de dados (se necessário).

A tarefa *Manutenção do Servidor de Administração* oferece suporte às versões 10.3 e posteriores do MariaDB. Caso as versões 10.2 ou anteriores do MariaDB sejam usadas, os administradores terão que manter esse DBMS por conta própria.

Para criar uma tarefa Manutenção do Servidor de Administração:

1. Na árvore do console, selecione o nó do Servidor de Administração para o qual deseja criar uma tarefa *Manutenção do Servidor de Administração*.
2. Selecione a pasta **Tarefas**.
3. No espaço de trabalho da pasta **Tarefas**, clique no botão **Nova tarefa**.

   O Assistente para novas tarefas inicia.
4. Na janela **Selecionar o tipo de tarefa** do assistente, selecione **Manutenção do Servidor de Administração** como o tipo de tarefa e clique em **Avançar**.
5. Se você precisar compactar o banco de dados do Servidor de Administração durante a manutenção, na janela **Configurações** do assistente, selecione a caixa de seleção **Compactar o banco de dados**.
6. Siga o restante das instruções do assistente.

A tarefa recém criada é exibida na lista de tarefas no espaço de trabalho da pasta **Tarefas**. Somente uma tarefa *Manutenção do Servidor de Administração* pode ser executada para um único Servidor de Administração. Se uma tarefa de *Manutenção do Servidor de Administração* já tiver sido criada para um Servidor de Administração, nenhuma nova tarefa de *Manutenção do Servidor de Administração* poderá ser criada.

Acesso aos servidores DNS públicos

Caso o acesso aos servidores da Kaspersky que estão usando o DNS do sistema não seja possível, o Kaspersky Security Center poderá usar esses servidores DNS públicos na seguinte ordem:

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)

As solicitações para esses servidores DNS podem conter endereços de domínio e o endereço IP público do Servidor de Administração, porque o aplicativo estabelece uma conexão TCP/UDP com o servidor DNS. Caso o Kaspersky Security Center Linux esteja usando um servidor DNS público, o processamento de dados será regido pela Política de Privacidade do serviço pertinente.

Para configurar o uso de DNS público usando o utilitário klscflag:

1. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.
2. Para desativar o uso do DNS público, execute o seguinte comando:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 1
   ```

3. Para ativar o uso do DNS público, execute o seguinte comando:

   ```
   klscflag -fset -pv ".core/.independent" -s Transport -n ForceUseSystemDNS -t d -v 0
   ```

Janela Método de notificação ao usuário

Na janela **Método de notificação ao usuário**, você pode especificar a notificação ao usuário sobre a instalação do certificado no dispositivo móvel:

- **Mostrar link no assistente**. Se você selecionar esta opção, um link ao pacote de instalação será mostrado na etapa final do Assistente de conexão de novos dispositivos móveis.
- **Enviar link para o usuário**. Se você selecionar esta opção, poderá especificar as configurações para notificar o usuário sobre a conexão de um dispositivo.

No grupo **Por e-mail** de configurações, você pode configurar a notificação ao usuário sobre a instalação de um novo certificado em seu dispositivo móvel usando mensagens de e-mail. Este método de notificação somente está disponível se o Servidor de SMTP estiver ativado.

No grupo **Por SMS** de configurações, você pode configurar a notificação ao usuário sobre a instalação de um certificado em seu dispositivo móvel usando o SMS. Este método de notificação somente está disponível se notificação por SMS estiver ativada.

Clique no link **Editar mensagem** nos grupos **Por e-mail** e **Por SMS** de configurações para exibir e editar a mensagem de notificação, se necessário.

Seção Geral

Nesta seção, você pode ajustar as configurações gerais de perfil para dispositivos móveis Exchange ActiveSync:

- **Nome**

  Nome do perfil.

- **Permitir dispositivos não provisionáveis**

  Caso esta opção esteja ativada, os dispositivos que não podem acessar todas as configurações da política do Exchange ActiveSync são autorizados a se conectar com o servidor de dispositivos móveis. Usando a conexão, é possível gerenciar dispositivos móveis Exchange ActiveSync. Por exemplo, é possível definir senhas, configurar o envio de e-mails ou visualizar informações sobre os dispositivos, como o ID do dispositivo ou o status da política.

  Caso a opção esteja desabilitada, não será possível se conectar ao servidor de dispositivos móveis e gerenciar os dispositivos móveis do Exchange ActiveSync.

  Por padrão, esta opção está ativada. É possível desabilitar a opção caso os dispositivos móveis do Exchange ActiveSync não sejam gerenciados e as informações sobre eles não serão recebidas.

- **Frequência de atualização (horas)**

  Se esta opção estiver ativada, o aplicativo atualiza as informações sobre a política Exchange ActiveSync com a frequência especificada no campo de entrada.

  Se esta opção estiver desativada, as informações sobre a política Exchange ActiveSync não são atualizadas.

  Por padrão, esta opção é ativada e o intervalo de atualização é de uma hora.

Janela Seleção de dispositivos

Escolha uma seleção na lista **Seleção de dispositivos**. A lista contém as seleções predefinidas e as seleções criadas pelo usuário.

Você pode visualizar os detalhes das seleções de dispositivos no espaço de trabalho do nó **Seleções de dispositivos**.

Definir o nome da janela de novo objeto

Na janela, especifique o nome do objeto recentemente criado. O nome não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

Seção Categorias de aplicativos

Nesta seção, você poderá configurar a distribuição de informações sobre categorias de aplicativo em dispositivos cliente.

Transmissão completa de dados (para Agentes de Rede Service Pack 2 e anterior)

Se esta opção estiver selecionada, todos os dados de uma categoria de aplicativo serão transmitidos aos dispositivos cliente após a modificação daquela categoria. Esta opção de transmissão de dados é usada com o Service Pack 2 do Agente de Rede e para versões anteriores.

Somente a transmissão de dados modificados (para Agentes de Rede Service Pack 2 e posterior)

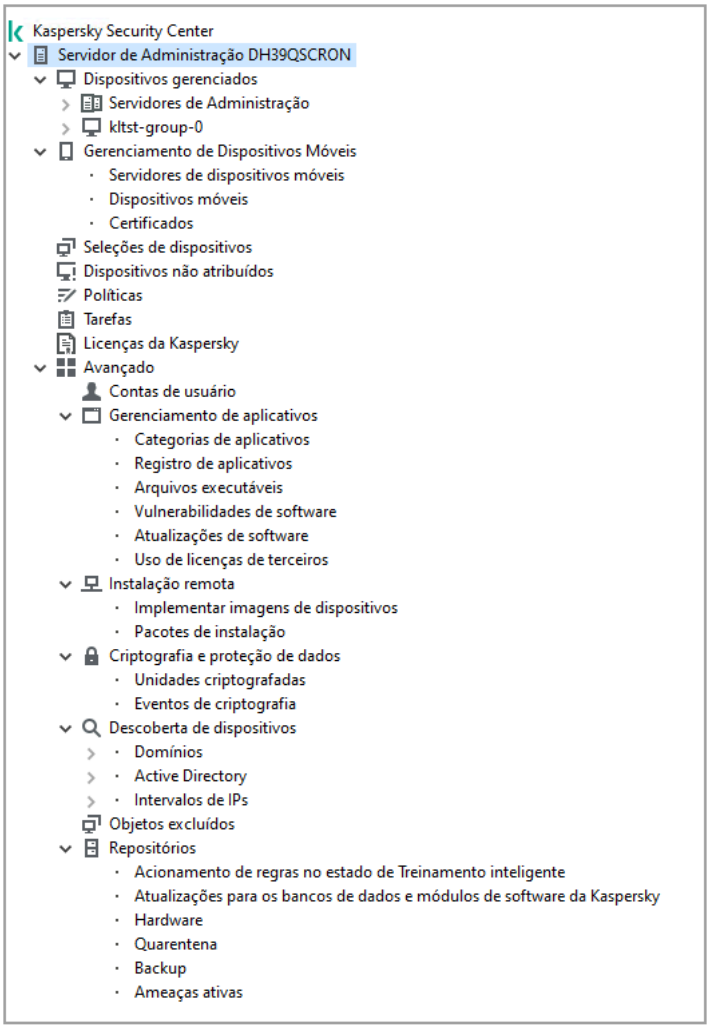
Se esta opção estiver selecionada, quando uma categoria de aplicativo for modificada, somente os dados modificados serão transmitidos aos dispositivos cliente, não todos os dados daquela categoria. Esta opção de transmissão de dados é usada com o Service Pack 2 do Agente de Rede e para versões posteriores.

Recursos de uso da interface de gerenciamento

Esta seção descreve ações que você pode executar na janela principal do Kaspersky Security Center.

Árvore do console

A árvore do console (veja a figura abaixo) é concebida para exibir a hierarquia dos Servidores de Administração na rede corporativa, a estrutura de seus grupos de administração e outros objetos do aplicativo, como as pastas **Repositórios** ou **Gerenciamento de aplicativos**. O espaço de nome do Kaspersky Security Center pode conter vários nós incluindo os nomes de servidores correspondentes aos Servidores de Administração instalados e incluídos na hierarquia.



Árvore do console

Nó do Servidor de Administração

O nó **Servidor de Administração – <Nome do dispositivo>** é um contêiner que mostra a organização estrutural do Servidor de Administração selecionado.

O espaço de trabalho do nó **Servidor de Administração** contém informações resumidas sobre o status atual do aplicativo e dos dispositivos gerenciados através do Servidor de Administração. As informações no espaço de trabalho são distribuídas entre diversas guias:

- **Monitorar**. Exibe as informações sobre a operação do aplicativo e o status atual dos dispositivos cliente no modo de tempo real. As mensagens importantes para o administrador (como as mensagens sobre vulnerabilidades, erros ou vírus detectado) são realçadas com uma cor específica. Você pode usar links na guia **Monitorar** para executar tarefas padrão de administrador (por exemplo, instalar e configurar o aplicativo de segurança nos dispositivos cliente), assim como ir para outras pastas na árvore do console.

- **Estatísticas**. Contém um conjunto de gráficos agrupados por tópicos (status da proteção, estatística de antivírus, atualizações e etc.). Estes gráficos exibem as informações atuais sobre a operação do aplicativo e o status dos dispositivos cliente.

- **Relatórios**. Contém modelos para relatórios gerados pelo aplicativo. Nesta guia, você pode criar relatórios usando modelos predefinidos, assim como criar modelos de relatórios personalizados.

- Janela **Eventos**. Contém registros sobre eventos que foram registrados durante a operação do aplicativo. Estes registros são distribuídos entre os tópicos para facilitar a leitura e filtragem. Nesta guia, você pode visualizar seleções de eventos que foram geradas automaticamente, assim como criar seleções personalizadas.

Pastas no nó Servidor de Administração

O nó **Servidor de Administração – <Nome do dispositivo>** inclui as seguintes pastas:

- **Dispositivos gerenciados**. A pasta é destinada ao armazenamento, exibição, configuração e modificação da estrutura de grupos de administração, políticas de grupo e tarefas de grupo.

- **Gerenciamento de Dispositivos Móveis**. Esta pasta é projetada para gerenciar os dispositivos móveis. **Gerenciamento de dispositivos móveis** e eventos contém as seguintes subpastas:

  - **Servidor de dispositivos móveis**. Destinado para gerenciar Servidores MDM do iOS e Microsoft Exchange Mobile Devices Server.

  - **Dispositivos Móveis**. É projetado para gerenciar dispositivos móveis, KES, Exchange ActiveSync e MDM do iOS.

  - **Certificados**. É projetado para gerenciar os certificados de dispositivos móveis.

- **Seleções de dispositivos**. Esta pasta é projetada para a seleção rápida de dispositivos que atendem ao critério especificado (uma seleção de dispositivos), entre todos os dispositivos gerenciados. Por exemplo, você pode selecionar rapidamente os dispositivos nos quais o aplicativo de segurança foi instalado, e seguir para estes dispositivos (exibir a lista). Você pode executar algumas ações nestes dispositivos selecionados, por exemplo, atribui-los algumas tarefas. Você pode usar seleções predefinidas ou criar suas próprias seleções personalizadas.

- **Dispositivos não atribuídos**. Esta pasta contém uma lista de dispositivos que não foram incluídos em nenhum grupo de administração. Você pode executar algumas ações em dispositivos não atribuídos, por exemplo, movê-los para seus grupos de administração ou instalar aplicativos neles.

- **Políticas**. Esta pasta é projetada para visualizar e criar políticas.

- **Tarefas**. Esta pasta é projetada para visualizar e criar tarefas.

- **Licenças da Kaspersky**. Contém uma lista das chaves de licença disponíveis para os aplicativos Kaspersky. No espaço de trabalho desta pasta, você pode adicionar novas chaves de licença ao repositório de chaves de licença, implementar chaves de licença nos dispositivos gerenciados e visualizar relatórios sobre o uso de chaves de licença.

- **Avançado**. Esta pasta contém um conjunto de subpastas que correspondem a diversos grupos de recursos do aplicativo.

Pasta Avançado. Mover pastas na árvore do console

A pasta **Avançado** inclui as seguintes subpastas:

- **Contas de usuário**. Contém uma lista de contas de usuário da rede.

- **Gerenciamento de aplicativos**. Concebida para gerenciar aplicativos instalados nos dispositivos na rede. A pasta **Gerenciamento de aplicativos** contém as seguintes subpastas:

  - **Categorias de aplicativos**. Destinado para gerenciar categorias de aplicativos personalizados.

  - **Registro de aplicativos**. Contém uma lista de aplicativos em dispositivos nos quais o Agente de Rede está instalado.

  - **Arquivos executáveis**. Contém uma lista de arquivos executáveis armazenados em dispositivos cliente com o Agente de Rede instalado.

  - **Vulnerabilidades de software**. Contém uma lista de aplicativos em dispositivos cliente nos quais o Agente de Rede está instalado.

  - **Atualizações de software**. Contém uma lista de atualizações de aplicativo recebidas pelo Servidor de Administração que podem ser distribuídas aos dispositivos.

  - **Uso de licenças de terceiros**. Contém uma lista de grupos de aplicativos licenciados. É possível usar grupos de aplicativos licenciados para monitorar o uso das licenças de software de terceiros (aplicativos que não sejam da Kaspersky) e as possíveis violações de restrições de licenciamento.

- **Instalação remota**. A pasta é concebida para o gerenciamento de instalação remota de sistemas operacionais e aplicativos. A pasta **Instalação remota** contém as seguintes subpastas:

  - **Implementar imagens do dispositivo**. Concebido para implementar imagens de sistemas operacionais nos dispositivos.

  - **Pacotes de instalação**. Contém uma lista de pacotes de instalação que pode ser usada para a instalação remota de aplicativos em dispositivos.

- **Criptografia e proteção de dados**. Esta pasta é concebida para gerenciar o processo de criptografia dos dados em discos rígidos e unidades removíveis.

- **Sondagem da rede**. Esta pasta exibe a rede na qual o Servidor de Administração está instalado. O Servidor de Administração recebe informações sobre a estrutura da rede e seus dispositivos por meio de sondagens regulares da rede Windows, sub-redes IP e do Active Directory® na rede corporativa. Os resultados da sondagem são exibidos nos espaços de trabalho das pastas correspondentes: **Domínios**, **Conjuntos de IPs** e **Active Directory**.

- **Repositórios**. A pasta é destinada a operações com objetos usados para monitorar o status dos dispositivos e executar suas manutenções. A pasta **Repositórios** contém os seguintes subpastas:

  - **Detecção de anomalia adaptativa**. Contém uma lista de detecções realizadas pelas regras do Kaspersky Endpoint Security que funcionam no modo de Treinamento inteligente em dispositivos clientes.

  - **Atualizações e patches de software da Kaspersky**. Contém uma lista de atualizações recebidas pelo Servidor de Administração que pode ser distribuída aos dispositivos.

  - **Hardware**. Contém uma lista de hardware conectado à rede corporativa.

  - **Quarentena**. Contém uma lista de objetos movidos para Quarentena pelo software antivírus em dispositivos.

  - **Backup**. Contém uma lista das cópias de backup dos arquivos que foram excluídos ou modificados durante o processo de desinfecção nos dispositivos.

  - **Arquivos não processados**. Contém uma lista de arquivos atribuídos para verificação posterior pelos aplicativos antivírus.

Você poderá alterar o conjunto de subpastas incluído na pasta **Avançado**. As subpastas frequentemente usadas podem ser movidas um nível acima da pasta **Avançado**. As subpastas que sejam raramente usadas podem ser movidas para a pasta **Avançado**.

*Para mover uma subpasta para fora da pasta **Avançado**:*

1. Na árvore do console, selecione a subpasta que você precisa mover para fora da pasta **Avançado**.
2. No menu de contexto da subpasta, selecione **Exibir → Mover da pasta Avançado**.

> Você também pode mover uma subpasta para fora da pasta **Avançado** no espaço de trabalho da pasta **Avançado** ao clicar no link **Mover da pasta Avançado** na seção com o nome daquela subpasta.

*Para mover uma subpasta para a pasta **Avançado**:*

1. Na árvore do console, selecione a subpasta que você precisa mover para a pasta **Avançado**.
2. No menu de contexto da subpasta, selecione **Exibir → Mover para a pasta Avançado**.

Como atualizar dados no espaço de trabalho

> No Kaspersky Security Center, os dados do espaço de trabalho (tal como status do dispositivo, estatísticas e relatórios) nunca são atualizados automaticamente.

Para atualizar dados no espaço de trabalho:

- Pressione a tecla **F5**.
- No menu de contexto do objeto na árvore do console, selecione **Atualizar**.
- Clique no ícone de atualização () no espaço de trabalho.

Como navegar na árvore do console

Para navegar na árvore do console, você pode usar os seguintes botões na barra de ferramentas:

-  – Voltar uma etapa.
-  – Uma etapa adiante.
-  – Um nível acima.

Você também pode usar uma cadeia de navegação localizada no canto superior direito do espaço de trabalho. A cadeia de navegação contém o caminho completo para a pasta da árvore do console na qual você está atualmente localizado. Todos os elementos da cadeia, exceto o último, são links para os objetos na árvore do console.

Como abrir a janela de propriedades do objeto no espaço de trabalho

Você pode alterar as propriedades da maioria dos objetos do Console de Administração na janela de propriedades do objeto.

Para abrir a janela de propriedades de um objeto localizado no espaço de trabalho:

- No menu de contexto do objeto, selecione **Propriedades**.
- Selecione um objeto e pressione **ALT**+**ENTER**.

Como selecionar um grupo de objetos no espaço de trabalho

Você pode selecionar um grupo de objetos no espaço de trabalho. Você pode selecionar um grupo de objetos, por exemplo, para criar o grupo de dispositivos para os quais é possível criar tarefas posteriormente.

Para selecionar uma faixa de objetos:

1. Selecione o primeiro objeto na faixa e pressione **Shift**.
2. Mantenha a tecla **Shift** pressionada e selecione o último objeto na faixa.

A faixa será selecionada.

Para agrupar objetos separados:

1. Selecione o primeiro objeto no grupo e pressione **Ctrl**.
2. Mantenha a tecla **Ctrl** pressionada e selecione outros objetos para serem incluídos no grupo.

Os objetos serão agrupados.

Como alterar o conjunto de colunas no espaço de trabalho

O Console de Administração lhe permite alterar um conjunto de colunas exibidas no espaço de trabalho.

Para alterar um conjunto de colunas exibidas no espaço de trabalho:

1. Na árvore do console, clique no objeto para o qual você pretende alterar o conjunto de colunas.
2. No espaço de trabalho da pasta, abra a janela destinada para a configuração do conjunto de colunas clicando no link **Adicionar/Remover colunas**.
3. Na janela **Adicionar/Remover colunas**, especifique o conjunto de colunas a ser exibido.

Informações de referência

As tabelas desta seção fornecem informações sumarizadas sobre o menu de contexto dos objetos do Console de Administração, assim como sobre os status dos objetos da árvore do console e dos objetos do espaço de trabalho.

Comandos no menu de contexto

Esta seção lista os objetos do Console de Administração e respectivos itens do menu de contexto (consulte a tabela abaixo).

Itens do menu de contexto dos objetos do Console de Administração

Objeto	Item de menu	Propósito do item de menu
Itens gerais do menu de contexto	**Pesquisar**	Abre a janela Pesquisa por dispositivos.
	Atualizar	Atualize a exibição do objeto selecionado.
	Exportar a lista	Exporta a lista atual para um arquivo.
	Propriedades	Abre a janela Propriedades para o objeto selecionado.
	Exibir → Adicionar/Remover colunas	Adiciona ou remove colunas para/da tabela de objetos no espaço de trabalho.
	Exibir → Ícones grandes	Exibe os objetos no espaço de trabalho como ícones grandes.
	Exibir → Ícones pequenos	Exibe os objetos no espaço de trabalho como ícones pequenos.
	Exibir → Lista	Exibe objetos no espaço de trabalho como uma lista.
	Exibir → Tabela	Exibe os objetos no espaço de trabalho como uma tabela.
	Exibir → Configurar	Configura a exibição dos elementos do Console de Administração.
Kaspersky Security Center	**Novo → Servidor de Administração**	Adiciona um Servidor de Administração à árvore do console.
<Nome do Servidor de Administração>	**Conectar-se ao Servidor de Administração**	Conecta-se ao Servidor de Administração.
	Desconectar do Servidor de Administração	Desconecta do Servidor de Administração.
Dispositivos gerenciados	**Instalar o aplicativo**	Inicia o Assistente de instalação remota.
	Visualizar → Configurar interface	Configurar a exibição dos elementos da interface.
	Remover	Remove o Servidor de Administração da árvore do console.
	Instalar o aplicativo	Inicia o Assistente de instalação remota para o grupo de administração.
	Redefinir o contador de vírus	Redefine os contadores de vírus para os dispositivos incluídos no grupo de administração.
	Visualizar o relatório de ameaças	Cria um relatório sobre ameaças e atividade de vírus nos dispositivos incluídos no grupo de administração.
	Novo → Grupo	Cria um grupo de administração.
	Todas as tarefas → Nova estrutura de grupos	Crie uma estrutura de grupos de administração com base na estrutura de domínios ou do Active Directory.
	Todas as tarefas → Mostrar a mensagem	Inicia o Assistente de nova mensagem para usuário, concebido para usuários de dispositivos cliente incluídos no grupo de administração.
Dispositivos gerenciados → Servidores de Administração	**Novo → Servidor de Administração secundário**	Inicia o Assistente para adicionar Servidor de Administração secundário.
	Novo → Servidor de Administração virtual	Inicia o Assistente de novo Servidor de Administração virtual.
Gerenciamento de Dispositivos Móveis → Dispositivos móveis	**Novo → Dispositivo móvel**	Conecta um novo dispositivo móvel do usuário.
Gerenciamento de Dispositivos Móveis → Certificados	**Novo → Certificado**	Cria um certificado.
	Criar → Dispositivo móvel	Conecta um novo dispositivo móvel do usuário.
Seleções de dispositivos	**Novo → Nova seleção**	Cria uma seleção de dispositivos.
	Todas as tarefas → Importar	Importar a seleção de um arquivo.

Objeto	Item de menu	Propósito do item de menu
Licenças da Kaspersky	**Adicionar código de ativação ou arquivo de chave**	Adição de uma chave de licença ao repositório do Servidor de Administração.
	Ativar aplicativo	Inicia o Assistente de criação de tarefa de ativação do aplicativo.
	Relatório de uso das chaves de licença	Cria e exibe um relatório sobre as chaves de licença nos dispositivos cliente.
Gerenciamento de aplicativos → Categorias de aplicativos	**Novo → Categoria**	Cria uma categoria de aplicativo.
Gerenciamento de aplicativos → Registro de aplicativos	**Filtro**	Configure um filtro para a lista de aplicativos.
	Aplicativos monitorados	Configura a publicação de eventos relativos a instalação de aplicativos.
	Remover aplicativos que não estão instalados	Limpa a lista de todos os detalhes de aplicativos que não mais estão instalados em dispositivos na rede.
Gerenciamento de aplicativos → Atualizações de software	**Aceitar os Contratos de Licença para atualizações**	Aceita os Contratos de Licença de atualizações do software.
Gerenciamento de aplicativos → Uso de licenças de terceiros	**Novo → Grupo de aplicativos licenciados**	Cria um grupo de aplicativos licenciados.
Instalação remota → Pacotes de instalação	**Mostrar as versões atuais dos aplicativos**	Mostra a lista de versões atualizadas dos aplicativos Kaspersky disponíveis nos servidores da Web.
	Novo → Pacote de instalação	Cria um pacote de instalação.
	Todas as tarefas → Atualizar bancos de dados	Bancos de dados de atualização do aplicativo nos pacotes de instalação.
	Todas as tarefas → Mostrar a lista geral de pacotes independentes	Mostra a lista de pacotes independentes criados para os pacotes de instalação.
Descoberta de dispositivos → Domínios	**Todas as tarefas → Atividade de dispositivos**	Define a resposta do Servidor de Administração sobre a inatividade de dispositivos na rede.
Descoberta de dispositivos → Intervalos de IPs	**Novo → Intervalo de IP**	Cria um conjunto de IPs.
Repositórios → Atualizações para os bancos de dados e módulos de software da Kaspersky	**Baixar atualizações**	Abre a janela de propriedades da tarefa Baixar atualizações para o repositório do Servidor de Administração.
	Configurações de Download de Atualizações	Configura a tarefa Baixar atualizações para o repositório do Servidor de Administração.
	Relatório de uso de bancos de dados de antivírus	Cria e exibe um relatório sobre as versões dos bancos de dados.
	Todas as tarefas → Limpar repositório de atualizações	Limpa o repositório de atualizações do Servidor de Administração.
Repositórios → Hardware	**Novo → Dispositivo**	Cria um novo dispositivo.

Lista de dispositivos gerenciados. Descrição das colunas

A tabela a seguir exibe os nomes e respectivas descrições das colunas na lista de dispositivos gerenciados.

Descrições das colunas na lista de dispositivos gerenciados

Nome da coluna	Valor
Nome	Nome NetBIOS do dispositivo cliente. As descrições dos ícones dos nomes de dispositivos são fornecidas no apêndice.
Tipo de sistema operacional	Tipo de sistema operacional instalado no dispositivo cliente.
Domínio do Windows	Nome do domínio do Windows no qual o dispositivo está localizado.

Nome da coluna	Valor
Agente de Rede instalado	Resultado da instalação do Agente de Rede no dispositivo cliente *Sim*, *Não*, *Desconhecido*.
Agente de Rede em execução	Resultado da operação do Agente de Rede *Sim*, *Não*, *Desconhecido*.
Proteção em tempo real	O aplicativo de segurança está instalado *Sim*, *Não*, *Desconhecido*.
Última conexão com o Servidor de Administração	O período de tempo que decorreu desde que o de dispositivo cliente se conectou ao Servidor de Administração.
Última atualização da proteção	O período de tempo decorrido desde a última atualização dos dispositivos gerenciados.
Status	O status atual do dispositivo cliente *OK, Crítico ou Advertência*.
Descrição de status	Condições para alteração do status do dispositivo cliente para *Crítico* ou *Advertência*. O status do dispositivo muda para *Advertência* ou *Crítico* por conta das seguintes condições: • O aplicativo de segurança não está instalado. • Excesso de vírus detectados. • O nível da proteção em tempo real é diferente do nível definido pelo administrador. • A verificação de malwares não é executada há muito tempo. • Os bancos de dados estão desatualizados. • Não conectado há muito tempo. • Foram detectadas ameaças ativas. • A reinicialização é necessária. O motivo para reiniciar o dispositivo pode ser um dos seguintes: ◦ Reiniciado por motivo desconhecido. ◦ O aplicativo não funcionará até a reinicialização. ◦ É necessário reiniciar para concluir a atualização; o aplicativo está em execução. ◦ É necessário reiniciar para iniciar a atualização. ◦ É necessário reiniciar para concluir a verificação ou a desinfecção. ◦ A reinicialização é necessária para concluir a instalação/desinstalação remota. ◦ Concluindo a criptografia de dados no disco. Você pode definir os motivos ao configurar a mudança de status do dispositivo. • Aplicativos incompatíveis estão instalados. • Foram detectadas vulnerabilidades de software. • A verificação de atualizações do Windows Update não é executada há muito tempo. • Status de criptografia inválido. • As configurações do dispositivo móvel não estão em conformidade com a política. • Incidentes não processados detectados. • Status do dispositivo definido pelo aplicativo. • O dispositivo está com espaço em disco insuficiente. • A licença expira em breve. O status do dispositivo só é alterado para *Crítico* pelos seguintes motivos: • A licença expirou. • O dispositivo está sem gerenciamento. • A proteção está desativada. • O aplicativo de segurança não está em execução. Os aplicativos Kaspersky gerenciados nos dispositivos cliente podem adicionar descrições de status à lista. O Kaspersky Security Center pode receber a descrição de um status do dispositivo cliente de aplicativos Kaspersky gerenciados e instalados naquele dispositivo. Se o status que foi atribuído ao dispositivo pelo aplicativo gerenciado for diferente do que o atribuído pelo Kaspersky Security Center, o Console de Administração exibe o status, que é o mais crítico para a segurança do dispositivo. Por exemplo, se um aplicativo gerenciado tiver atribuído o status *Crítico* ao dispositivo enquanto o Kaspersky Security Center atribuiu o status *Advertência*, o Console de Administração exibirá o status *Crítico* para o dispositivo, com a descrição correspondente fornecida pelo aplicativo gerenciado.
Última atualização das informações	O período de tempo que decorreu desde que o de dispositivo cliente foi sincronizado com êxito pela última vez com o Servidor de Administração (ou seja, desde a última verificação da rede).

Nome da coluna	Valor
Nome DNS	O nome do domínio DNS do dispositivo cliente.
Domínio DNS	O sufixo principal DNS.
Endereço IP	Endereço IP do dispositivo cliente. Recomenda-se o uso do endereço IPv4.
Última visualização	O período de tempo durante o qual o de dispositivo cliente permaneceu visível na rede.
Última verificação completa	A data e hora da última verificação do dispositivo cliente executada pelo aplicativo de antivírus a pedido do usuário.
Número total de ameaças detectadas	Número de ameaças encontradas.
Status da proteção em tempo real	Status da proteção em tempo real *Iniciando*, *Executando*, *Executando (proteção máxima)*, *Executando (velocidade máxima)*, *Executando (configurações recomendadas)*, *Executando (configurações personalizadas)*, *Parado*, *Pausado*, *Falhou*.
Endereço IP da conexão	O endereço IP usado para conexão com o Servidor de Administração do Kaspersky Security Center.
Versão do Agente de Rede	Versão do Agente de Rede.
Versão do aplicativo	Versão do aplicativo de segurança instalada no dispositivo cliente.
Última atualização dos bancos de dados de antivírus	A versão dos bancos de dados de antivírus.
Última inicialização do sistema	A data e hora em que o dispositivo cliente foi ligado pela última vez.
A reinicialização é necessária	O reinício do dispositivo cliente é necessário.
Ponto de distribuição	O nome do dispositivo que atua como ponto de distribuição para este dispositivo cliente.
Descrição	Descrição do dispositivo cliente recebido após uma verificação da rede.
Status da criptografia	O status da criptografia dos dados do dispositivo cliente.
Status WUA	Status do Windows Update Agent no dispositivo cliente. O valor *Sim* corresponde aos dispositivos cliente que recebem atualizações através do Windows Update a partir do Servidor de Administração. O valor *Não* corresponde aos dispositivos cliente que recebem atualizações através do Windows Update a partir de outras fontes.
Tipo de bit do sistema operacional	O tipo de bit do sistema operacional instalado no dispositivo cliente.
Status da proteção contra spam	Status do componente Proteção contra spam *Executando*, *Iniciando*, *Parado*, *Pausado*, *Falhou*, *Sem dados do dispositivo*
Status da prevenção de vazamento de dados	Status do componente Prevenção de vazamento de dados *Executando*, *Iniciando*, *Parado*, *Pausado*, *Falhou*, *Sem dados do dispositivo*
Status da proteção dos servidores de colaboração	Status do componente Filtragem de Conteúdo *Executando*, *Iniciando*, *Parado*, *Pausado*, *Falhou*, *Sem dados do dispositivo*
Status da proteção antivírus dos servidores de correio	Status do componente Proteção antivírus do Servidor de Correio *Executando*, *Iniciando*, *Parado*, *Pausado*, *Falhou*, *Sem dados do dispositivo*
Status do Endpoints Sensor	Status do componente Endpoint Detection and Response (KATA) *Executando*, *Iniciando*, *Parado*, *Pausado*, *Falhou*, *Sem dados do dispositivo*

Nome da coluna	Valor
Criação	Tempo desde que o ícone <Nome do dispositivo> foi criado. Este atributo é usado para comparar vários eventos entre si.
Nome do Servidor de Administração virtual ou secundário	Nome do Servidor de Administração virtual ou secundário. Esta coluna está disponível apenas em listas que contêm dispositivos de diferentes Servidores de Administração.
Grupo principal	Nome do grupo de administração onde o ícone <Nome do dispositivo> está localizado. Esta coluna está disponível apenas em listas que contêm dispositivos de diferentes Servidores de Administração.
Gerenciado por outro Servidor de Administração	O parâmetro pode assumir um destes valores: • Verdadeiro, se durante a instalação remota de aplicativos de segurança no dispositivo, for descoberto que o dispositivo é gerenciado por um Servidor de Administração diferente. • Falso, caso contrário.
Compilação do sistema operacional	O número da compilação do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um número de compilação igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de compilação, exceto o especificado.
ID da versão do sistema operacional	O identificador (ID) da versão do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um ID da versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de ID da versão, exceto o especificado.

Status de dispositivos, tarefas e políticas

A tabela abaixo contém uma lista de ícones exibidos na árvore do console e no espaço de trabalho do Console de Administração, próximos aos nomes dos dispositivos cliente, tarefas e políticas. Esses ícones definem os status de objetos.

Status de dispositivos, tarefas e políticas

Ícone	Status
	O dispositivo com um sistema operacional para estações de trabalho detectado no sistema e não incluído em nenhum dos grupos de administração.
	O dispositivo com um sistema operacional para estações de trabalho incluído em um grupo de administração, com o status *OK*.
	O dispositivo com um sistema operacional para estações de trabalho incluído em um grupo de administração, com o status *Advertência*.
	O dispositivo com um sistema operacional para estações de trabalho incluído em um grupo de administração, com o status *Crítico*.
	O dispositivo com um sistema operacional para estações de trabalho incluído em um grupo de administração, que perdeu sua conexão ao Servidor de Administração.
	O dispositivo com um sistema operacional para servidores detectados no sistema mas ainda não incluído em nenhum dos grupos de administração.
	O dispositivo com um sistema operacional para servidores incluído em um grupo de administração, com o status *OK*.
	O dispositivo com um sistema operacional para servidores incluído em um grupo de administração, com o status *Advertência*.
	O dispositivo com um sistema operacional para servidores incluído em um grupo de administração, com o status *Crítico*.
	O dispositivo com um sistema operacional para servidores incluído em um grupo de administração, que perdeu sua conexão ao Servidor de Administração.

	O dispositivo móvel detectado na rede e não incluído em nenhum dos grupos de administração.
	Dispositivo móvel incluído em um grupo de administração, com o status *OK*.
	Dispositivo móvel incluído em um grupo de administração, com o status *Advertência*.
	Dispositivo móvel incluído em um grupo de administração, com o status *Crítico*.
	O dispositivo móvel incluído em um grupo de administração, tendo perdido sua conexão com o Servidor de Administração.
	Dispositivo de proteção UEFI detectado na rede mas não incluído em nenhum grupo de administração. O dispositivo de proteção UEFI está na rede.
	Dispositivo de proteção UEFI detectado na rede mas não incluído em nenhum grupo de administração. O dispositivo de proteção UEFI não está na rede.
	Dispositivo de proteção UEFI incluído em um grupo de administração, com o status *OK*. O dispositivo de proteção UEFI está na rede.
	Dispositivo de proteção UEFI incluído em um grupo de administração, com o status *OK*. O dispositivo de proteção UEFI não está na rede.
	Dispositivo de proteção UEFI incluído em um grupo de administração, com o status *Advertência*. O dispositivo de proteção UEFI está na rede.
	Dispositivo de proteção UEFI incluído em um grupo de administração, com o status *Advertência*. O dispositivo de proteção UEFI não está na rede.
	Dispositivo de proteção UEFI incluído em um grupo de administração, com o status *Crítico*. O dispositivo de proteção UEFI está na rede.
	Dispositivo de proteção UEFI incluído em um grupo de administração, com o status *Crítico*. O dispositivo de proteção UEFI não está na rede.
	Política ativa.
	Política inativa.
	A política ativa herdada de um grupo que foi criado no Servidor de administração principal.
	Política ativa herdada de um grupo de nível superior.
	Tarefa (tarefa de grupo, tarefa do Servidor de Administração ou tarefa para dispositivos específicos) com o status *Agendado* ou *Conclusão com êxito*.
	Tarefa (tarefa de grupo, tarefa do Servidor de Administração ou tarefa para dispositivos específicos) com o status *Executando*.
	Tarefa (tarefa de grupo, tarefa do Servidor de Administração ou tarefa para dispositivos específicos) com o status *Falhou*.
	Tarefa herdada de um grupo que foi criado no Servidor de Administração principal.
	Tarefa herdada de um grupo de nível superior.

Ícones de status do arquivo no Console de Administração

Para a facilidade de gerenciamento de arquivos no Console de Administração do Kaspersky Security Center, os ícones são exibidos ao lado dos nomes dos arquivos (consulte a tabela abaixo). Os ícones indicam o status atribuído aos arquivos por aplicativos Kaspersky gerenciados nos dispositivos cliente. Os ícones são mostrados nos espaços de trabalho das pastas **Quarentena**, **Backup** e **Ameaças ativas**.

Os status são atribuídos aos objetos pelo Kaspersky Endpoint Security instalado no dispositivo cliente no qual o objeto está localizado.

Correspondência entre ícones e status de arquivo

Ícone	Status
	Arquivo com o status de *Infectado*.
	Arquivo com o status de *Advertência* ou *Provavelmente infectado*.
	Arquivo com o status de *Adicionado pelo usuário*.
	Arquivo com o status de *Falso positivo*.
	Arquivo com o status de *Desinfectado*.
	Arquivo com o status de *Excluído*.
	Arquivo na pasta **Quarentena** com o status *Não infectado, Protegido por senha* ou *Deve ser enviado para a Kaspersky*. Se não houver descrição do status junto a um ícone, isto significa que o aplicativo da Kaspersky gerenciado no dispositivo cliente reportou um status desconhecido ao Kaspersky Security Center.
	Arquivo na pasta **Backup** com o status *Não infectado, Protegido por senha* ou *Deve ser enviado para a Kaspersky*. Se não houver descrição do status junto a um ícone, isto significa que o aplicativo da Kaspersky gerenciado no dispositivo cliente reportou um status desconhecido ao Kaspersky Security Center.
	Arquivo na pasta **Ameaças ativas** com o status *Não infectado, Protegido por senha* ou *Deve ser enviado para a Kaspersky*. Se não houver descrição do status junto a um ícone, isto significa que o aplicativo da Kaspersky gerenciado no dispositivo cliente reportou um status desconhecido ao Kaspersky Security Center.

Pesquisar e exportar dados

Esta seção contém informações sobre métodos de busca de dados e sobre a exportação de dados.

Dispositivos encontrados

O Kaspersky Security Center permite encontrar dispositivos com base em critérios especificados. Os resultados da busca podem ser salvos em um arquivo de texto.

O recurso de pesquisa lhe permite localizar os seguintes dispositivos:

- Os dispositivos cliente nos grupos de administração de um Servidor de Administração e seus servidores secundários.
- Dispositivos não atribuídos gerenciados por um Servidor de Administração e seus Servidores secundários.

Para localizar dispositivos cliente incluídos em um grupo de administração:

1. Na árvore do console, selecione uma pasta do grupo de administração.
2. Selecione **Pesquisar** no menu de contexto da pasta do grupo de administração.
3. Nas guias da janela **Pesquisar**, especifique o critério para a busca de dispositivos e clique no botão **Localizar agora**.

Os dispositivos que atendem aos critérios de pesquisa especificados serão exibidos em uma tabela na parte inferior da janela **Pesquisar**.

Para localizar dispositivos não atribuídos:

1. Na árvore do console, selecione a pasta **Dispositivos não atribuídos**.
2. Selecione **Pesquisar** no menu de contexto da pasta **Dispositivos não atribuídos**.
3. Nas guias da janela **Pesquisar**, especifique o critério para a busca de dispositivos e clique no botão **Localizar agora**.

Os dispositivos que atendem aos critérios de pesquisa especificados serão exibidos em uma tabela na parte inferior da janela **Pesquisar**.

Para localizar dispositivos a despeito se eles estão incluídos em um grupo de administração:

1. Na árvore do console, selecione o nó **Servidor de Administração**.
2. No menu de contexto do nó selecione **Pesquisar**.
3. Nas guias da janela **Pesquisar**, especifique o critério para a busca de dispositivos e clique no botão **Localizar agora**.

Os dispositivos que atendem aos critérios de pesquisa especificados serão exibidos em uma tabela na parte inferior da janela **Pesquisar**.

Na janela **Pesquisar**, você pode também pesquisar por grupos de administração e Servidores Administrativos secundários usando uma lista suspensa no canto superior direito da janela. A funcionalidade de pesquisa por grupos de administração e Servidores de Administração secundários não está disponível se você tiver aberto a janela **Pesquisar** na pasta **Dispositivos não atribuídos**.

Para localizar dispositivos, você poderá usar expressões regulares nos campos na janela **Pesquisar**.

A pesquisa de texto completo na janela **Pesquisar** está disponível:

- Na guia **Rede**, no campo **Descrição**
- Na guia **Hardware**, nos campos **Dispositivo**, **Fornecedor** e **Descrição**

Configurações de pesquisa de dispositivo

Abaixo estão as descrições das configurações usadas para pesquisar por dispositivos gerenciados. Os resultados da pesquisa são exibidos na parte inferior da janela.

Rede

Na guia **Rede**, você poderá especificar os critérios que serão usados para pesquisar por dispositivos de acordo com dados na rede:

- **Nome do dispositivo ou endereço IP**

  Nome da rede Windows (nome NetBIOS) do dispositivo ou o endereço IPv4 ou IPv6.

- **Domínio do Windows**

  Exibe todos os dispositivos incluídos no domínio do Windows especificado.

- **Grupo de administração**

  Exibe os dispositivos incluídos no grupo de administração especificado.

- Descrição

Texto na janela Propriedades do dispositivo: no campo **Descrição** da seção **Geral**.

Para descrever texto no campo **Descrição**, é possível usar os seguintes caracteres:

- Em uma palavra:
  - *****. Substitui qualquer sequência por qualquer número de caracteres.

    Exemplo:

    Para descrever as palavras **Servidor** ou **Servidores**, é possível inserir **Servidor***.
  - **?.** Substitui qualquer caractere único.

    Exemplo:

    Para descrever palavras como **Janela** ou **Janelas**, você pode inserir **Janel?.**

    O asterisco (*****) ou o ponto de interrogação (**?**) não pode ser usado como o primeiro caractere na consulta.
- Para encontrar várias palavras:
  - Espaço. Exibe todos os dispositivos cujas descrições contêm qualquer uma das palavras listadas.

    Exemplo:

    Para localizar uma frase que contenha as palavras **Secundário** ou **Virtual**, você pode incluir a linha **Secundário Virtual** na consulta.
  - **+**. Quando o sinal de mais antecede uma palavra, todos os resultados de pesquisa contêm essa palavra.

    Exemplo:

    Para encontrar uma frase que contenha as palavras **Secundário** e **Virtual**, insira **+Secundário+Virtual** na consulta.
  - **-**. Quando um sinal de menos antecede uma palavra, nenhum dos resultados de pesquisa contém essa palavra.

    Exemplo:

    Para encontrar uma frase que contenha **Secundário**, mas que não contenha **Virtual**, insira **+Secundário-Virtual** na consulta.
  - **"<algum texto>"**. O texto dentro de aspas deve estar no texto.

    Exemplo:

    Para encontrar uma expressão que contenha a combinação de palavras **Servidor Secundário**, você pode inserir **"Servidor Secundário"** na consulta.

- Intervalo de IPs

  Se esta opção estiver ativada, você poderá inserir os endereços IP inicial e final do conjunto de IPs no qual os dispositivos relevantes devem ser incluídos.

  Por padrão, esta opção está desativada.

- Gerenciado por outro Servidor de Administração

  Selecione um dos seguintes valores:

  - **Sim**. Somente os dispositivos cliente gerenciados por outros Servidores de Administração são levados em consideração.
  - **Não**. Somente os dispositivos cliente gerenciados pelo mesmo Servidor de Administração são levados em consideração.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

Tags

Na guia **Tags**, você pode configurar uma pesquisa por dispositivos com base em palavras-chave (tags) adicionadas anteriormente às descrições dos dispositivos gerenciados:

- Aplicar se pelo menos uma tag especificada corresponder

  Se esta opção estiver ativada, o resultado da pesquisa mostrará os dispositivos com descrições que contêm ao menos uma das tags selecionadas.

  Se esta opção estiver ativada, o resultado da pesquisa irá mostrar os dispositivos com descrições que não contêm todos as tags selecionadas.

  Por padrão, esta opção está desativada.

- A tag deve ser incluída

  Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

  Por padrão, esta opção está selecionada.

- A tag deve ser excluída

  Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições não contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

Active Directory

Na guia **Active Directory**, é possível especificar os dispositivos que devem ser pesquisados na unidade organizacional (OU) do Active Directory ou no grupo. Também é possível incluir os dispositivos de todas as OUs filhas da OU do Active Directory especificado na seleção. Para selecionar dispositivos, defina as seguintes configurações:

- **O dispositivo está em uma unidade organizacional do Active Directory**

  Se esta opção estiver ativada, a seleção inclui os dispositivos da unidade do Active Directory especificada no campo de entrada.

  Por padrão, esta opção está desativada.

- **Incluir unidades organizacionais secundárias**

  Caso esta opção esteja ativada, a seleção incluirá os dispositivos das unidades de organização secundárias da unidade organizacional do Active Directory especificada.

  Por padrão, esta opção está desativada.

- **Este dispositivo é membro de um grupo do Active Directory**

  Se esta opção estiver ativada, a seleção incluirá os dispositivos do grupo do Active Directory especificado no campo de entrada.

  Por padrão, esta opção está desativada.

Atividade de rede

Na guia **Atividade de rede**, você poderá especificar o critério que será usado para pesquisar por dispositivos de acordo com sua atividade na rede:

- Este dispositivo é um ponto de distribuição

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. A seleção inclui dispositivos que agem como pontos de distribuição.
  - **Não**. Dispositivos que atuam como pontos de distribuição não serão incluídos na seleção.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Não desconectar do Servidor de Administração

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Ativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** está selecionada.
  - **Desativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** não está selecionada.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Perfil de conexão trocado

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. A seleção incluirá os dispositivos que se conectaram ao Servidor de Administração após o perfil de conexão ter sido alternado.
  - **Não**. A seleção não incluirá os dispositivos que se conectaram com o Servidor de Administração após o perfil de conexão ter sido alternado.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Última conexão com o Servidor de Administração

  Você pode usar essa caixa de seleção para configurar um critério para pesquisar por dispositivos pela hora da sua última conexão com o Servidor de Administração.

  Se essa caixa de seleção estiver selecionada, é possível, nos campos de entrada especificar o intervalo de tempo (data e hora) durante o qual a última conexão entre o Agente de Rede instalado no dispositivo cliente e o Servidor de Administração foi estabelecida. A seleção inclui dispositivos que estejam no intervalo especificado.

  Se essa caixa de seleção for desmarcada, o critério não é aplicado.

  Por padrão, esta caixa de seleção está desmarcada.

- Novos dispositivos detectados pela sondagem da rede

  Procura por novos dispositivos que tenham sido detectados pela sondagem da rede ao longo dos poucos últimos dias.

  Se esta opção estiver ativada, a seleção somente inclui novos dispositivos que tenham sido detectados pela descoberta de dispositivos durante a quantidade de dias especificada no campo **Período de detecção (dias)**.

  Se esta opção estiver ativada, a seleção inclui todos os dispositivos que tenham sido detectados pela descoberta de dispositivos.

  Por padrão, esta opção está desativada.

- Dispositivo visível

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos atualmente visíveis na rede.
  - **Não**. O aplicativo é incluído na seleção de dispositivos atualmente invisíveis na rede.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

Aplicativo

Na guia **Aplicativo**, você poderá especificar o critério que será usado para pesquisar por dispositivos de acordo com o aplicativo gerenciado selecionado:

- Nome do aplicativo

  Na lista suspensa, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome de um aplicativo da Kaspersky.

  A lista somente fornece os nomes de aplicativos com plugins de gerenciamento instalados na estação de trabalho do administrador.

  Se nenhum aplicativo for selecionado, o critério não será aplicado.

- Versão do aplicativo

  No campo de entrada, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo número da versão de um aplicativo da Kaspersky.

  Se nenhum número de versão for especificado, o critério não será aplicado.

- Nome da atualização crítica

  No campo de entrada de dados, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome do aplicativo ou pelo número do pacote de atualização.

  Se o campo for deixado em branco, o critério não será aplicado.

- Última atualização dos módulos

  Você pode usar esta opção para definir um critério para pesquisar dispositivos pela hora da última atualização dos módulos de aplicativos instalados nesses dispositivos.

  Se essa caixa de seleção estiver selecionada, nos campos de entrada você poderá especificar o intervalo de tempo (data e hora) durante o qual a última atualização de módulos de aplicativos instalados nesses dispositivos foi executada.

  Se essa caixa de seleção for desmarcada, o critério não é aplicado.

  Por padrão, esta caixa de seleção está desmarcada.

- O dispositivo é gerenciado através do Kaspersky Security Center

  Na lista suspensa, você poderá incluir nos dispositivos selecionados gerenciados através do Kaspersky Security Center:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos gerenciados através do Kaspersky Security Center.
  - **Não**. O aplicativo inclui dispositivos na seleção se eles não forem gerenciados pelo Kaspersky Security Center.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Aplicativo de segurança instalado

  Na lista suspensa, você poderá incluir na seleção todos os dispositivos com o aplicativo de segurança instalado:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos com o aplicativo de segurança instalado.
  - **Não**. O aplicativo inclui na seleção todos os dispositivos sem nenhum aplicativo de segurança instalado.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

Sistema operacional

Na guia **Sistema operacional**, você pode definir os seguintes critérios para encontrar dispositivos por seu tipo de sistema operacional (SO):

- Versão do sistema operacional

  Se esta caixa de seleção estiver marcada, você pode selecionar um sistema operacional da lista. Os dispositivos com o sistema operacional especificado instalado são incluídos nos resultados de pesquisa.

- Tipo de bit do sistema operacional

  Na lista suspensa, você poderá selecionar a arquitetura para o sistema operacional, que determinará como a regra para mover será aplicada ao dispositivo (**Desconhecido**, **x86**, **AMD64** ou **IA64**). Por padrão, nenhuma opção é selecionada na lista para que a arquitetura do sistema operacional não fique definida.

- **Versão do Service Pack do sistema operacional**

  Neste campo, você pode especificar a versão do pacote do sistema operacional (no formato *X.Y*), o que determinará como a regra de migração será aplicada ao dispositivo. Por padrão, nenhum valor de versão é especificado.

- **Compilação do sistema operacional**

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  O número da compilação do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um número de compilação igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de compilação, exceto o especificado.

- **ID da versão do sistema operacional**

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  O identificador (ID) da versão do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um ID da versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de ID da versão, exceto o especificado.

Status do dispositivo

Na guia **Status do dispositivo**, você pode especificar o critério para pesquisar dispositivos com base no status do dispositivo do aplicativo gerenciado:

- **Status do dispositivo**

  Lista suspensa na qual você pode selecionar um dos status do dispositivo: *OK*, *Crítico* ou *Advertência*.

- **Status da proteção em tempo real**

  Lista suspensa na qual você pode selecionar o status da proteção em tempo real. Os dispositivos com um status da proteção em tempo real especificado serão incluídos na seleção.

- **Descrição do status do dispositivo**

  Neste campo, você poderá selecionar caixas de seleção próximas das condições que, se atendidas, atribuem um dos seguintes status ao dispositivo: *OK, Crítico* ou *Advertência*.

- **Status do dispositivo definido pelo aplicativo**

  Lista suspensa na qual você pode selecionar o status da proteção em tempo real. Os dispositivos com um status da proteção em tempo real especificado serão incluídos na seleção.

Componentes de proteção

Na guia **Componentes de proteção**, você poderá configurar o critério de pesquisa de dispositivos cliente por status da proteção.

- **Bancos de dados lançados**

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes por data de lançamento de versão do banco de dados antivírus. Nos campos de entrada, você pode definir o intervalo de tempo com base no qual a pesquisa é realizada.

  Por padrão, esta opção está desativada.

- **Última verificação**

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pela hora da última verificação de malwares. No campo de entrada, você poderá especificar o período de tempo no qual a última verificação de malwares foi executada.

  Por padrão, esta opção está desativada.

- **Número total de ameaças detectadas**

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pelo número de vírus detectados. Nos campos de entrada, você pode definir os valores limite inferiores e superiores pelo número de vírus encontrados.

  Por padrão, esta opção está desativada.

Registro de aplicativos

Na guia **Registro de aplicativos**, você poderá configurar a pesquisa por dispositivos com base nos aplicativos neles instalados:

- **Nome do aplicativo**

  Lista suspensa na qual é possível selecionar um aplicativo. Os dispositivo nos quais o aplicativos especificado estiver instalado, serão incluídos na seleção.

- **Versão do aplicativo**

  Campo de entrada onde é possível especificar a versão do aplicativo selecionado.

- **Fornecedor**

  Lista suspensa na qual é possível selecionar o fabricante de um aplicativo instalado no dispositivo.

- **Status do aplicativo**

  Uma lista suspensa na qual é possível selecionar o status de um aplicativo (*Instalado*, *Não instalado*). Os dispositivos nos quais o aplicativo especificado está ou não instalado, dependendo do status selecionado, serão incluídos na seleção.

- **Localizar por atualização**

  Se esta opção estiver ativada, a pesquisa será executada usando os dados das atualizações para os aplicativos instalados nos dispositivos relevantes. Após selecionar a caixa de seleção, os campos **Nome do aplicativo**, **Versão do aplicativo** e **Status do aplicativo** mudam para **Nome da atualização**, **Versão da atualização** e **Status** respectivamente.

  Por padrão, esta opção está desativada.

- **Nome de aplicativo de segurança incompatível**

  Lista suspensa na qual é possível selecionar aplicativos de segurança de terceiros. Durante a pesquisa, os dispositivos nos quais está instalado o aplicativo especificado, serão incluídos na seleção.

- **Tag do aplicativo**

  Na lista suspensa, você pode selecionar a tag do aplicativo. Todos os dispositivos que instalaram aplicativos com a tag selecionada na descrição são incluídos na seleção de dispositivo.

Hierarquia de Servidores de Administração

Na guia **Hierarquia de Servidores de Administração**, marque a caixa **Incluir dados de Servidores de Administração secundários (até o nível)** se desejar que as informações armazenadas nos Servidores de Administração secundários sejam consideradas ao pesquisar por dispositivos. No campo de entrada, é possível especificar o nível de aninhamento do Servidor de Administração secundário do qual as informações são consideradas durante a pesquisa por dispositivos. Por padrão, esta caixa de seleção está desmarcada.

Máquinas virtuais

Na guia **Máquinas virtuais**, você pode configurar a pesquisa por dispositivos com base no fato de que estes sejam máquinas virtuais ou parte da Virtual Desktop Infrastructure (VDI):

- Esta é uma máquina virtual

  Na lista suspensa, você pode selecionar as seguintes opções:

  - **Irrelevante**.
  - **Não**. Localizar dispositivos que não sejam máquinas virtuais.
  - **Sim**. Localizar dispositivos que são máquinas virtuais.

- Tipo de máquina virtual

  Na lista suspensa, você pode selecionar o fabricante da máquina virtual.

  Essa lista suspensa estará disponível se o valor **Sim** ou **Irrelevante** estiver selecionado na lista suspensa **Esta é uma máquina virtual**.

- Parte da Virtual Desktop Infrastructure

  Na lista suspensa, você pode selecionar as seguintes opções:

  - **Irrelevante**.
  - **Não**. Localizar dispositivos que não fazem parte da Virtual Desktop Infrastructure.
  - **Sim**. Localizar dispositivos que fazem parte da Virtual Desktop Infrastructure (VDI).

Hardware

Na guia **Hardware**, você pode configurar a pesquisa por dispositivos cliente de acordo com seu hardware:

- **Dispositivo**

  Na lista suspensa, você pode selecionar um tipo de unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

  O campo suporta a pesquisa de texto completo.

- **Fornecedor**

  Na lista suspensa, você pode selecionar o nome do fabricante da unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

  O campo suporta a pesquisa de texto completo.

- **Descrição**

  Descrição de um dispositivo ou de uma unidade de hardware. Os dispositivos com a descrição especificada neste campo serão incluídos na seleção.

  A descrição de um dispositivo em qualquer formado pode ser inserida na janela de propriedades desse dispositivo. O campo suporta a pesquisa de texto completo.

- **Número de inventário**

  Equipamentos com o número de inventário especificado neste campo serão incluídos na seleção.

- **Frequência da CPU em MHz**

  O intervalo de frequência de uma CPU. Os dispositivos com CPU's que correspondem a faixa de frequência nesses campos (inclusive) serão incluídos na seleção.

- **Núcleos de CPU virtuais**

  Faixa de número de núcleos virtuais em uma CPU. Os dispositivos com CPU's que correspondem a faixa de frequência nesses campos (inclusive) serão incluídos na seleção.

- **Volume do disco rígido, em GB**

  Faixa de valores para o tamanho do disco rígido no dispositivo. Os dispositivos com discos rígidos que correspondem a faixa nesses campos de entrada (inclusive) serão incluídos na seleção.

- **Tamanho da RAM, em MB**

  Intervalo de valores para o tamanho da RAM do dispositivo. Dispositivos com RAMs que correspondam ao intervalo nestes campos de entrada (inclusive) serão incluídos na seleção.

Vulnerabilidades e atualizações

Na guia **Vulnerabilidades e atualizações**, você pode definir o critério para pesquisar por dispositivos de acordo com sua origem do Windows Update:

- **WUA foi mudado para o Servidor de Administração**

  Você pode selecionar uma das seguintes opções de pesquisa da lista suspensa:

  - **Sim**. Se essa opção estiver selecionada, os resultados da pesquisa incluirão os dispositivos que recebem atualizações através do Windows Update do Servidor de Administração.
  - **Não**. Caso essa opção esteja selecionada, os resultados incluirão os dispositivos que recebem atualizações pelo Windows Update de outras fontes.

Usuários

Na guia **Usuários**, você pode definir o critério para pesquisar por dispositivos de acordo com as contas de usuários que efetuaram o login no sistema operacional.

- **Último usuário que fez login no sistema**

  Se esta opção estiver ativada, clique no botão **Procurar** para especificar uma conta de usuário. Os resultados da pesquisa incluem os dispositivos onde o usuário especificado efetuou o último login no sistema.

- **Usuário que fez login no sistema pelo menos uma vez**

  Se esta opção estiver ativada, clique no botão **Procurar** para especificar uma conta de usuário. Os resultados da pesquisa incluem os dispositivos nos quais o usuário especificado efetuou o login no sistema ao menos uma vez.

Problemas que afetam o status em aplicativos gerenciados

Na guia **Problemas que afetam o status em aplicativos gerenciados**, você pode definir o critério para pesquisar por dispositivos de acordo a descrição de seu status fornecido pelo aplicativo gerenciado:

- **Descrição do status do dispositivo**

  Você pode selecionar as caixas de seleção para descrições de status do aplicativo gerenciado; ao receber este status, os dispositivos serão incluídos na seleção. Quando você seleciona um status listado para vários aplicativos, você tem a opção de selecionar esse status em todas das listas automaticamente.

Status dos componentes em aplicativos gerenciados

Na guia **Status dos componentes em aplicativos gerenciados**, você pode definir o critério para pesquisar por dispositivos de acordo com o status de componentes em aplicativos gerenciados:

- **Status da prevenção de vazamento de dados**

  Pesquise dispositivos pelo status da Prevenção de vazamento de dados (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

- **Status da proteção dos servidores de colaboração**

  Procure dispositivos pelo status da proteção de colaboração do servidor (*Sem dados do dispositivo*, *Parado*, *Iniciando, Pausado*, *Executando*, *Falhou*).

- **Status da proteção antivírus dos servidores de correio**

  Procure dispositivos pelo status da proteção do servidor de e-mail (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

- **Status do Endpoints Sensor**

  Procure dispositivos pelo status do componente Endpoint Sensor (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

Criptografia

- **Criptografia**

  Algoritmo de criptografia de bloco simétrico Advanced Encryption Standard (AES). Na lista suspensa, você pode selecionar o tamanho de chave de criptografia (de 56 bits, de 128 bits, de 192 bits ou de 256 bits).

  Valores disponíveis: *AES56*, *AES128*, *AES192* e *AES256*.

Segmentos da nuvem

Na guia **Segmentos da nuvem**, você pode configurar uma pesquisa com base em se um dispositivo pertence aos segmentos na nuvem específicos:

- **O dispositivo está no segmento da nuvem**

  Se esta opção estiver ativada, você pode clicar no botão **Procurar** para especificar o segmento a ser pesquisado.

  Se a opção **Incluir objetos secundários** estiver marcada, a pesquisa é executada em todos os objetos secundários do segmento especificado.

  Os resultados da pesquisa somente incluem dispositivos do segmento selecionado.

- **Dispositivo detectado usando a API**

  Na lista suspensa, você pode selecionar se um dispositivo é detectado pelas ferramentas API:

  - **AWS**. O dispositivo é detectado usando a AWS API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do AWS.
  - **Azure**. O dispositivo é detectado usando a Azure API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do Azure.
  - **Google Cloud.** O dispositivo é descoberto usando a Google API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do Google.
  - **Não**. O dispositivo não pode ser detectado usando API do AWS, Azure ou Google, ou seja, está fora do ambiente em nuvem ou está no ambiente em nuvem, mas não pode ser detectado usando uma API.
  - **Nenhum valor**. Esta condição não se aplica.

Componentes do aplicativo

Esta seção contém a lista de componentes dos aplicativos que têm plugins de gerenciamento correspondentes instalados no Console de Administração.

Na seção **Componentes do aplicativo**, você pode especificar critérios para a inclusão de dispositivos em uma seleção segundo os status e os números da versão dos componentes que fazem referência ao aplicativo que você selecionar:

- **Status**

  Pesquise dispositivos segundo o status do componente enviado por um aplicativo ao Servidor de Administração. Você pode selecionar um dos seguintes status: *Nenhum dado do dispositivo*, *Interrompido*, *Iniciando*, *Pausado*, *Executando*, *Mau funcionamento*, ou *Não instalado*. Se o componente selecionado do aplicativo instalado em um dispositivo gerenciado tiver o status especificado, o dispositivo será incluído na seleção de dispositivos.

  Status enviados pelos aplicativos:

  - *Iniciando* – O componente está atualmente em processo de inicialização.
  - *Executando* – O componente está ativado e funcionando corretamente.
  - *Pausado* – O componente está suspenso, por exemplo, depois que o usuário pausou a proteção no aplicativo gerenciado.
  - *Mau funcionamento* – Um erro ocorreu durante a operação do componente.
  - *Interrompido* – O componente está desativado e não está funcionando no momento atual.
  - *Não instalado* – O usuário não selecionou o componente para instalação ao configurar a instalação personalizada do aplicativo.

  Diferentemente de outros status, o status *Nenhum dado do dispositivo* não é enviado pelos aplicativos. Esta opção mostra que os aplicativos não têm nenhuma informação sobre o status do componente selecionado. Por exemplo, isto pode acontecer quando o componente selecionado não pertence a nenhum dos aplicativos instalados no dispositivo, ou quando o dispositivo está desligado.

- **Versão**

  Pesquise dispositivos segundo o número da versão do componente que você selecionar na lista. Você pode digitar um número de versão, por exemplo `3.4.1.0`, e especificar se o componente selecionado deve ter uma versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todas as versões, exceto a especificada.

Usar máscaras para variáveis de sequência

É permitido o uso de máscaras para variáveis de sequência. Durante a criação de máscaras, você pode usar as seguintes expressões regulares:

- Caractere curinga (*) – Qualquer sequência de 0 ou mais caracteres.
- Ponto de interrogação (?) – Qualquer caractere único.
- [<range>] – Qualquer caractere único a partir de um conjunto ou intervalo especificado.

  Por exemplo: [0–9] – Qualquer dígito. [abcdef] – Qualquer um dos caracteres a, b, c, d, e ou f.

Usar expressões regulares no campo de pesquisa

Você pode usar as seguintes expressões regulares no campo de pesquisa para procurar por palavras e caracteres específicas:

- *. Substitui qualquer combinação de caracteres. Para pesquisar por palavras como Servidor, Servidores ou Sala do servidor, insira a expressão `Servidor*` no campo de pesquisa.

- ?. Substitui qualquer caractere único. Para pesquisar por palavras Branco ou Brinco, insira a expressão `B?anc` no campo de pesquisa.

  > O texto no campo de pesquisa não pode ser iniciado por um ponto de interrogação (?).

- [<range>]. Substitui qualquer caractere único a partir de um conjunto ou intervalo especificado. Para pesquisar por qualquer número, insira a expressão `[0-9]` no campo de pesquisa. Para pesquisar por um dos caracteres – a, b, c, d, e ou f – insira a expressão `[abcdef]` no campo de pesquisa.

Use as seguintes expressões regulares no campo de pesquisa para obter uma pesquisa de texto completo:

- Espaço. O resultado de todos os dispositivos cujas descrições contêm qualquer uma das palavras listadas. Por exemplo, para pesquisar por uma frase que contenha a palavra "Secundário" ou "Virtual" (ou ambas essas palavras), insira a expressão `Secundário Virtual` no campo de pesquisa.

- Sinal de mais (+), AND ou &&. Quando o sinal de mais antecede uma palavra, todos os resultados de pesquisa contêm essa palavra. Por exemplo, para pesquisar por uma frase que contenha a palavra "Secundário" e a palavra "Virtual", você poderá inserir alguma das seguintes expressões no campo de pesquisa: `+Secundário+Virtual`, `Secundário E Virtual`, `Secundário && Virtual`.

- OR ou ||. Quando colocado entre duas palavras, indica que uma das palavras ou a outra pode ser encontrada no texto. Para pesquisar por uma frase que contenha a palavra "Secundário" ou "Virtual", insira uma das seguintes expressões no campo de pesquisa: `Secundário OU Virtual`, `Secundário || Virtual`.

- Sinal de menos (-). Quando um sinal de menos antecede uma palavra, nenhum dos resultados de pesquisa contém essa palavra. Para pesquisar por uma frase que deve conter a palavra Secundário e não deve conter a palavra Virtual, é preciso inserir a expressão `+Secundário+Virtual` no campo de pesquisa.

- `"< algum texto >"`. O texto dentro de aspas deve estar no texto. Para pesquisar por uma frase que contenha a combinação de palavras como Servidor Secundário, é preciso inserir a expressão `" Servidor Secundário "` no campo de pesquisa.

A pesquisa de texto completo está disponível nos seguintes blocos de filtragem:

- No bloco de filtragem da lista de eventos, junto das colunas **Evento** e **Descrição**.

- No bloco de filtragem da conta do usuário, junto da coluna **Nome**.

- No bloco de filtragem de registro de aplicativos, junto da coluna **Nome**, se a seção **Mostrar na lista** tiver **nenhum agrupamento** selecionado como o critério de filtragem.

Exportar listas a partir de caixas de diálogo

Em caixas de diálogo do aplicativo você pode exportar listas de objetos para arquivos de texto.

A exportação de uma lista de objetos é possível para seções de caixas de diálogo que contêm o botão **Exportar para arquivo**.

Configurações de tarefas

Esta seção lista todas as configurações de tarefas no Kaspersky Security Center.

Configurações de tarefa gerais

Esta seção contém as configurações que podem ser definidas e especificadas para a maioria das tarefas. A lista de configurações disponíveis depende da tarefa que se está configurando.

Configurações especificadas durante a criação de tarefa

Você pode especificar as seguintes configurações ao criar uma tarefa. Algumas dessas configurações também podem ser modificadas nas propriedades da tarefa criada.

- Configurações para reiniciar o sistema operacional:
  - **Não reiniciar o dispositivo**

    Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

  - **Reiniciar o dispositivo**

    Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

  - **Perguntar ao usuário o que fazer**

    O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

    Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Reiniciar após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  - **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

- Configurações de agendamento de tarefas:
  - **Configuração Início agendado:**
    - A cada N horas

      A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

      Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

    - A cada N dias

      A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

      Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

    - A cada N semanas

      A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

      Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

    - A cada N minutos

      A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

      Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

    - Diariamente (não é compatível com horário de verão)

A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

Por padrão, a tarefa inicia diariamente na hora atual do sistema.

- **Semanalmente**

  A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todo mês em dias especificados de semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **Quando novas atualizações são baixadas no repositório**

  A tarefa é executada após as atualizações serem baixadas no repositório. Por exemplo, pode ser necessário usar esse agendamento para a tarefa Encontrar as vulnerabilidades e atualizações necessárias.

- **No surto de vírus**

A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

- Antivírus para estações de trabalho e servidores de arquivo
- Antivírus para defesa de perímetro
- Antivírus para sistemas de correio

Por padrão, todos os tipos de aplicativos estão selecionados.

Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

  Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

  Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

  Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

  Por padrão, esta opção está desativada.

- **Usar atraso aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

- Dispositivos aos quais a tarefa será atribuída:
  - **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**

    A tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

    Por exemplo, pode ser necessário usar esta opção em uma tarefa de instalação do Agente de Rede em dispositivos não atribuídos.

  - **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**

    Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

    Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

  - **Atribuir a tarefa a uma seleção de dispositivos**

    A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

    Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

  - **Atribuir tarefa a um grupo de administração**

    A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

    Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

    Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

- Configurações de conta:
  - **Conta padrão**

    A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

    Por padrão, esta opção está selecionada.

  - **Especificar conta**

    Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

  - **Conta**

Conta sob a qual a tarefa é executada.

- **Senha**

  Senha da conta sob a qual a tarefa será executada.

Caso o Agente de Rede não esteja instalado no dispositivo de destino, você precisará indicar a conta que será usada nele para acessar o compartilhamento admin$. A conta que você indicou só tem o propósito de copiar os dados do seu dispositivo. Caso o Agente de Rede esteja instalado no seu dispositivo de destino, os dados serão copiados usando o Agente de Rede, e você não precisará indicar nenhuma conta ao criar uma tarefa.

Configurações especificadas após a criação da tarefa

Você pode especificar as seguintes configurações após criar uma tarefa.

- Configurações de tarefa de grupo:
  - **Distribuir para subgrupos**

    Essa opção só está disponível nas configurações das tarefas de grupo.

    Quando essa opção está habilitada, o escopo da tarefa inclui:

    - O grupo de administração selecionado ao criar a tarefa.
    - Os grupos de administração subordinados ao grupo de administração selecionado em qualquer nível abaixo na hierarquia do grupo.

    Quando essa opção está desabilitada, o escopo da tarefa inclui apenas o grupo de administração selecionado ao criar a tarefa.

    Por padrão, esta opção está ativada.

  - **Distribuir em Servidores de Administração secundários e virtuais**

    Quando essa opção está habilitada, a tarefa efetiva no Servidor de Administração principal também é aplicada nos Servidores de Administração secundários (incluindo os virtuais). Caso já exista uma tarefa do mesmo tipo no Servidor de Administração secundário, ambas as tarefas serão aplicadas no Servidor de Administração secundário (a existente e a herdada do Servidor de Administração principal).

    Essa opção só está disponível quando a opção **Distribuir para subgrupos** está habilitada.

    Por padrão, esta opção está desativada.

- Configurações de agendamento avançado:
  - **Ligar dispositivos usando a função Wake-On-LAN antes de iniciar a tarefa (min.)**

    O sistema operacional do dispositivo selecionado inicia na hora especificada, antes do início da tarefa. O período de tempo padrão é de cinco minutos.

    Ative esta opção se você quiser que a tarefa seja executada em todos os dispositivos clientes do escopo da tarefa, inclusive nos dispositivos que são desligados quando a tarefa está prestes a ser iniciada.

    Se você quiser que o dispositivo seja desativado automaticamente após a conclusão da tarefa, ative a opção **Desligar os dispositivos após concluir a tarefa**. Esta opção pode ser encontrada na mesma janela.

    Por padrão, esta opção está desativada.

  - **Desligar os dispositivos após concluir a tarefa**

Por exemplo, pode ser necessário ativar esta opção para uma tarefa que instala atualizações nos dispositivos clientes todas as sextas-feiras após o horário comercial e, em seguida, desliga esses dispositivos durante o fim de semana.

Por padrão, esta opção está desativada.

- **Parar a tarefa se ela for executada por mais que (min.)**

  Após o final do período especificado, a tarefa é interrompida automaticamente, quer tenha sido concluída ou não.

  Ative esta opção se você quiser interromper (ou parar) tarefas que levam muito tempo para serem executadas.

  Por padrão, esta opção está desativada. O tempo predefinido de execução da tarefa é de 120 minutos.

- Configurações de notificação:
  - Bloco **Armazenar histórico de tarefas**:
    - No Servidor de Administração por (dias)

      Os eventos de aplicativo relacionados à execução da tarefa em todos os dispositivos clientes do escopo da tarefa são armazenados no Servidor de Administração durante o número de dias especificado. Quando esse período termina, as informações são excluídas do Servidor de Administração.

      Por padrão, esta opção está ativada.

    - Armazenar no log de eventos do SO no dispositivo

      Os eventos de aplicativo relacionados à execução da tarefa são armazenados localmente no Log de Eventos do Windows de cada dispositivo cliente.

      Por padrão, esta opção está desativada.

    - Armazenar no log de eventos do SO no Servidor de Administração

      Os eventos de aplicativo relacionados à execução da tarefa em todos os dispositivos cliente do escopo da tarefa são armazenados centralmente no Log de Eventos do Windows do sistema operacional (SO) do Servidor de Administração.

      Por padrão, esta opção está desativada.

    - Salvar todos os eventos

      Se esta opção estiver selecionada, todos os eventos relacionados à tarefa serão salvos nos logs de eventos.

    - Salvar eventos relacionados ao progresso da tarefa

      Se esta opção estiver selecionada, apenas os eventos relacionados à execução da tarefa serão salvos nos logs de eventos.

    - Salvar apenas os resultados da execução da tarefa

      Se esta opção estiver selecionada, apenas os eventos relacionados aos resultados da tarefa serão salvos nos logs de eventos.

  - Notificar administrador sobre os resultados de execução de tarefas

    Você pode selecionar os métodos pelos quais os administradores recebem notificações sobre os resultados de execução da tarefa: por e-mail, por SMS e pela execução de um arquivo executável. Para configurar a notificação, clique em link **Configurações**.

    Por padrão, todos os métodos de notificação estão desativados.

  - Notificar somente erros

Se esta opção estiver ativada, os administradores serão notificados apenas quando uma execução de tarefa for concluída com um erro.

Se esta opção estiver desativada, os administradores serão notificados após cada conclusão de execução de tarefa.

Por padrão, esta opção está ativada.

- Configurações de segurança
- Configurações do escopo da tarefa

  Dependendo de como o escopo da tarefa é determinado, as seguintes configurações estão presentes:

  - Dispositivos

    Se o escopo de uma tarefa for determinado por um grupo de administração, você pode exibir visualizar esse grupo. Nenhuma alteração está disponível nesse ponto. No entanto, você pode definir **Exclusões do escopo da tarefa**.

    Se o escopo de uma tarefa for determinado por uma lista de dispositivos, você pode alterar essa lista adicionando e removendo dispositivos.

  - Seleção de dispositivos

    Você pode alterar a seleção de dispositivos aos quais a tarefa é aplicada.

  - Exclusões do escopo da tarefa

    Você pode especificar grupos de dispositivos aos quais a tarefa não é aplicada. Os grupos a serem excluídos podem somente ser subgrupos do grupo de administração ao qual a tarefa é aplicada.

- **Histórico de revisões**

Baixar atualizações nas configurações da tarefa do repositório do Servidor de Administração

Configurações especificadas durante a criação de tarefa

Você pode especificar as seguintes configurações ao criar uma tarefa. Algumas dessas configurações também podem ser modificadas nas propriedades da tarefa criada.

- Fontes de atualizações

  Os seguintes recursos podem ser utilizados como uma origem das atualizações do Servidor de Administração:

  - Servidores de atualização da Kaspersky

    Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo. Por padrão, o Servidor de Administração comunica-se com os servidores de atualização Kaspersky e baixa as atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração para usar o protocolo HTTP em vez de HTTPS.

    Selecionado por padrão.

  - Servidor de Administração Principal

    Este recurso é aplicado a tarefas criadas para um Servidor de Administração virtual ou secundário.

  - Pasta local ou de rede

    Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Uma pasta de rede pode ser um servidor FTP ou HTTP, ou um compartilhamento SMB. Se uma pasta de rede exigir autenticação, apenas o protocolo SMB será compatível. Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado.

    Um servidor FTP ou HTTP ou pasta de rede utilizados por uma fonte de atualização devem conter uma estrutura de pastas (com atualizações) que corresponda à estrutura criada ao usar servidores de atualização Kaspersky.

- **Outras configurações**

  Forçar a atualização de Servidores de Administração secundários

  Caso esta opção esteja ativada, o Servidor de Administração inicia as tarefas de atualização nos Servidores de Administração secundários assim que as novas atualizações são baixadas. As tarefas de atualização são iniciadas usando a fonte de atualização configurada nas propriedades da tarefa nos Servidores de Administração secundários.

  Caso esta opção esteja desativada, as tarefas de atualização nos Servidores de Administração secundários serão iniciadas de acordo com seus agendamentos.

  Por padrão, esta opção está desativada.

  Copiar as atualizações baixadas em pastas adicionais

Após recepção das atualizações pelo Servidor de Administração, estas são copiadas para as pastas especificadas. Use esta opção se você deseja gerenciar manualmente a distribuição das atualizações na rede.

Por exemplo, você pode desejar usar esta opção na seguinte situação: a rede de sua organização consiste em várias sub-redes independentes e os dispositivos de cada uma das sub redes não têm acesso a outras sub-redes. Entretanto, os dispositivos em todas das sub-redes têm acesso a um compartilhamento de rede comum. Neste caso, você define o Servidor de Administração em uma das sub-redes para baixar atualizações dos Servidores de Atualização Kaspersky, ativar essa opção e especificar esse compartilhamento de rede. Nas atualizações baixadas para as tarefas de repositório de outros Servidores de Administração, especifique o mesmo compartilhamento de rede como a origem da atualização.

Por padrão, esta opção está desativada.

Não forçar a atualização de dispositivos e Servidores de Administração secundários a não ser que a cópia tenha sido concluída

As tarefas de download das atualizações nos dispositivos cliente e no Servidor de Administração secundário somente inicia depois das atualizações serem copiadas da pasta principal das atualizações para as pastas de atualização adicionais.

Essa opção deve ser ativada se os de dispositivos cliente e os Servidores de Administração secundários baixam atualizações de pastas adicionais da rede.

Por padrão, esta opção está desativada.

Configurações especificadas após a criação da tarefa

Você pode especificar as seguintes configurações após criar uma tarefa.

- Seção **Configurações**, bloco **Conteúdo das atualizações**

  Baixar arquivos diff

  Esta opção ativa o recurso de download dos arquivos diff.

  Por padrão, esta opção está desativada.

- Seção **Verificação de atualizações**

  Verificar atualizações antes de distribuir

  O Servidor de Administração baixa as atualizações da fonte, salva-as num repositório temporário e executa a tarefa definida no campo **Tarefa de verificação de atualizações**. Se a tarefa for concluída com êxito, as atualizações serão copiadas do repositório temporário para uma pasta compartilhada no Servidor de Administração e distribuídas a todos os dispositivos para os quais o Servidor de Administração atua como a fonte de atualizações (tarefas com o agendamento de **Quando novas atualizações são baixadas no repositório** forem iniciadas). A tarefa de download de atualizações para o repositório é concluída somente após o término da *Tarefa de verificação de atualizações*.

  Por padrão, esta opção está desativada.

  Tarefa de verificação de atualizações

  Esta tarefa verifica as atualizações baixadas antes que elas sejam distribuídas para todos os dispositivos para os quais o Servidor de Administração atua como a origem das atualizações.

  Nesse campo, é possível especificar a tarefa de *Verificação de atualizações* criada anteriormente. Alternativamente, é possível pode criar uma nova tarefa de *Verificação de atualizações*.

As configurações da tarefa Baixar atualizações para os repositórios de pontos de distribuição

Configurações especificadas durante a criação de tarefa

Você pode especificar as seguintes configurações ao criar uma tarefa. Algumas dessas configurações também podem ser modificadas nas propriedades da tarefa criada.

- **Fontes de atualizações**

  Os seguintes recursos podem ser utilizados como uma origem das atualizações para o ponto de distribuição:

  - Servidores de atualização da Kaspersky

    Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

    Esta opção está marcada por padrão.

  - Servidor de Administração Principal

    Este recurso é aplicado a tarefas criadas para um Servidor de Administração virtual ou secundário.

  - Pasta local ou de rede

    Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Uma pasta de rede pode ser um servidor FTP ou HTTP, ou um compartilhamento SMB. Se uma pasta de rede exigir autenticação, apenas o protocolo SMB será compatível. Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado.

    Um servidor FTP ou HTTP ou pasta de rede utilizados por uma fonte de atualização devem conter uma estrutura de pastas (com atualizações) que corresponda à estrutura criada ao usar servidores de atualização Kaspersky.

- **Outras configurações** → **Pasta para armazenar atualizações**

  O caminho para a pasta especificada para armazenar atualizações salvas. É possível copiar o caminho da pasta especificada para uma área de transferência. Não é possível alterar o caminho para uma pasta especificada para uma tarefa de grupo.

Configurações especificadas após a criação da tarefa

Você poderá especificar a seguinte configuração na seção **Configurações**, no bloco **Conteúdo das atualizações** somente após criar uma tarefa.

Baixar arquivos diff

Esta opção ativa o recurso de download dos arquivos diff.

Por padrão, esta opção está desativada.

As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias

Configurações especificadas durante a criação de tarefa

Você pode especificar as seguintes configurações ao criar uma tarefa. Algumas dessas configurações também podem ser modificadas nas propriedades da tarefa criada.

- **Buscar por vulnerabilidades e atualizações listadas pela Microsoft**

  Ao procurar por vulnerabilidades e atualizações, o Kaspersky Security Center usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft, que estão disponíveis no momento.

  Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

  As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

  - **Conectar com o servidor de atualizações para atualizar dados**

O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

- Servidor de Administração do Kaspersky Security Center Cloud Console (consulte as Configurações da política do Agente de Rede)
- Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
- Servidores de atualizações da Microsoft

Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

Caso esta opção esteja desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows recebidas da fonte de atualizações da Microsoft antes.

A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

Por padrão, esta opção está ativada.

A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

- O Windows Update Agent em um dispositivo gerenciado se conecta com o servidor de atualização para obter atualizações somente se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada nas propriedades da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* e a opção **Modo de pesquisa do Windows Update** estiver definida como **Ativo** nas configurações da política do Agente de Rede.
- Caso não precise do Agente de Rede para iniciar uma conexão com a fonte de atualização do Microsoft Windows e as atualizações sejam baixadas durante a execução da tarefa de *Verificação de vulnerabilidades*, será possível definir a opção **Modo de pesquisa do Windows Update** como **Passivo**, enquanto a opção **Conectar com o servidor de atualizações para atualizar dados** deve permanecer ativada. Isso permite economizar recursos e usar atualizações do Windows recebidas anteriormente para verificar vulnerabilidades. É possível usar o modo passivo se o recebimento de atualizações do Microsoft Windows for configurado de uma forma diferente. Caso o recebimento de atualizações do Microsoft Windows não seja configurado de outra forma, não defina a opção **Modo de pesquisa do Windows Update** como **Passivo**, pois, nesse caso, as informações sobre as atualizações nunca serão recebidas.
- Independentemente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativado ou desativado), caso a opção **Modo de pesquisa do Windows Update** esteja definida como **Desativado**, o Kaspersky Security Center não solicitará nenhuma informação sobre as atualizações.

- Buscar por vulnerabilidades e atualizações de terceiros, listadas pela Kaspersky

Se esta opção estiver ativada, o Kaspersky Security Center pesquisará vulnerabilidades e atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

Se esta opção estiver desativada, o Kaspersky Security Center não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

Por padrão, esta opção está ativada.

- Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos

  As pastas nas quais o Kaspersky Security Center pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

  Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista contém pastas do sistema nas quais a maioria dos aplicativos está instalada.

- Ativar diagnóstico avançado

  Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento mesmo que a gravação de arquivos de rastreamento esteja desativada para o Agente de Rede no Utilitário de Diagnóstico Remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

- Tamanho máximo, em MB, de arquivos de diagnóstico avançado

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

Configurações de tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades

Configurações especificadas durante a criação de tarefa

Você pode especificar as seguintes configurações ao criar uma tarefa. Algumas dessas configurações também podem ser modificadas nas propriedades da tarefa criada.

- **Especificar regras para a instalação de atualizações**

  Estas regras são aplicadas à instalação de atualizações nos dispositivos cliente. Se as regras não forem especificadas, a tarefa não terá nenhuma ação a ser executada. Para informações sobre operações com regras, consulte Regras para instalação da atualização.

- **Iniciar a instalação ao reiniciar ou fechar o dispositivo**

  Se esta opção estiver ativada, as atualizações serão instaladas quando o dispositivo for reiniciado ou desligado. Caso contrário, as atualizações são instaladas segundo o agendamento.

  Use esta opção caso a instalação das atualizações afete o desempenho do dispositivo.

  Por padrão, esta opção está desativada.

- **Instalar os componentes gerais do sistema necessários**

  Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional.

  Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

  Por padrão, esta opção está desativada.

- **Permitir a instalação de novas versões dos aplicativos durante atualizações**

  Se esta opção estiver ativada, as atualizações serão permitidas quando resultarem na instalação de uma nova versão de um aplicativo de software.

  Se esta opção estiver desativada, o software não será atualizado. Você poderá então instalar novas versões do software manualmente ou através de outra tarefa. Por exemplo, você pode usar esta opção se a infraestrutura da sua empresa não tiver como base uma nova versão do software ou se você quiser verificar uma atualização usando uma infraestrutura de teste.

  Por padrão, esta opção está ativada.

  A atualização de um aplicativo pode causar o funcionamento incorreto de aplicativos dependentes instalados em dispositivos cliente.

- **Baixar atualizações para o dispositivo sem instalá-las**

  Se esta opção estiver ativada, o aplicativo baixa as atualizações em um dispositivo cliente, mas não as instala automaticamente. Você então poderá instalar manualmente as atualizações baixadas.

  As atualizações da Microsoft são baixadas no armazenamento de sistema do Windows. Atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky e à Microsoft) são baixados na pasta especificada no campo **Pasta para download de atualizações**.

  Se esta opção estiver desativada, as atualizações serão instaladas no dispositivo automaticamente.

  Por padrão, esta opção está desativada.

  - **Pasta para download de atualizações**

    Esta pasta é usada para baixar atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft).

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento mesmo que a gravação de arquivos de rastreamento esteja desativada para o Agente de Rede no Utilitário de Diagnóstico Remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

  - **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

    O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

Configurações especificadas após a criação da tarefa

Você poderá especificar as configurações das seções listadas abaixo somente após criar uma tarefa. Para obter uma descrição completa das configurações da tarefa, consulte Configurações gerais da tarefa.

- **Geral**. Nesta seção, informações gerais sobre a tarefa são exibidas. Além disso, você pode especificar para quais dispositivos a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* deve se aplicar:

  - **Distribuir para subgrupos**

    Essa opção só está disponível nas configurações das tarefas de grupo.

    Quando essa opção está habilitada, o escopo da tarefa inclui:

    - O grupo de administração selecionado ao criar a tarefa.
    - Os grupos de administração subordinados ao grupo de administração selecionado em qualquer nível abaixo na hierarquia do grupo.

    Quando essa opção está desabilitada, o escopo da tarefa inclui apenas o grupo de administração selecionado ao criar a tarefa.

    Por padrão, esta opção está ativada.

  - **Distribuir em Servidores de Administração secundários e virtuais**

    Quando essa opção está habilitada, a tarefa efetiva no Servidor de Administração principal também é aplicada nos Servidores de Administração secundários (incluindo os virtuais). Caso já exista uma tarefa do mesmo tipo no Servidor de Administração secundário, ambas as tarefas serão aplicadas no Servidor de Administração secundário (a existente e a herdada do Servidor de Administração principal).

    Essa opção só está disponível quando a opção **Distribuir para subgrupos** está habilitada.

    Por padrão, esta opção está desativada.

- Atualizações para instalar

  Na seção **Atualizações para instalar** você pode exibir a lista de atualizações instaladas pela tarefa. Somente as atualizações que correspondem com as configurações da tarefa aplicada são exibidas.

- Instalação de teste de atualizações:

  - **Não verificar**. Selecione esta opção se você não quiser efetuar uma instalação de teste de atualizações.
  - **Executar a verificação nos dispositivos selecionados**. Selecione esta opção se você quiser testar a instalação de atualizações nos dispositivos selecionados. Clique no botão **Adicionar** e selecione os dispositivos nos quais você deseja efetuar uma instalação de teste das atualizações.
  - **Executar verificação nos dispositivos no grupo especificado**. Selecione esta opção se você quiser testar a instalação de atualizações em um grupo de dispositivos. No campo **Especifique um grupo de teste**, especifique um grupo de dispositivos nos quais você deseja executar uma instalação de teste.
  - **Executar verificação no percentual de dispositivos especificados**. Selecione esta opção se você quiser testar a instalação de atualizações em alguma quantidade de dispositivos. No campo **Porcentagem de dispositivos de teste de todos os dispositivos de destino**, especifique a porcentagem de dispositivos nos quais você deseja executar uma instalação de teste de atualizações.

Lista de sub-redes globais

Esta seção fornece informações sobre a lista global de sub-redes que você pode usar nas regras.

Para armazenar as informações sobre sub-redes da sua rede, você pode configurar uma lista global de sub-redes para cada Servidor de Administração que você usar. Esta lista ajuda você a combinar pares {endereço IP, máscara} e unidades físicas, como escritórios de filiais. Você pode usar sub-redes desta lista nas regras e configurações de rede.

Adicionar sub-redes à lista global de sub-redes

Você pode adicionar sub-redes com as descrições à lista global de sub-redes.

Para adicionar sub-redes à lista global de sub-redes:

1. Na árvore do console, selecione o nó do Servidor de Administração que você necessita.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de **propriedades** que se abre, no painel **Seções**, selecione **Lista de sub-redes globais**.
4. Clique no botão **Adicionar**.

   A janela **Nova sub-rede** se abre.

5. Preencha os campos a seguir:

- **Configurações gerais**

  O endereço IP de sub-rede para a sub-rede que está sendo adicionada.

- **Máscara de sub-rede**

  A máscara de sub-rede da sub-rede que você está adicionando.

- **Nome**

  O nome da sub-rede. O nome deve ser exclusivo na lista global de sub-redes. Se você digitar um nome que já existe na lista, um índice será adicionado, por exemplo: ~~1, ~~2.

- **Descrição**

  A descrição pode conter algumas informações adicionais sobre o escritório da filial que tem essa sub-rede. Esse texto será exibido em todas as listas onde esta sub-rede estiver presente como, por exemplo, na lista de regras de limitação de tráfego.

  Este campo não é obrigatório e pode ficar vazio.

6. Clique em **OK**.

A sub-rede aparecerá na lista de sub-redes.

Visualização e modificação das propriedades de sub-redes na lista global de sub-redes

Você pode exibir e modificar as propriedades das sub-redes na lista global de sub-redes.

Para exibir ou modificar propriedades de uma sub-rede na lista global de sub-redes:

1. Na árvore do console, selecione o nó do Servidor de Administração que você necessita.
2. No menu de contexto do Servidor de Administração, selecione **Propriedades**.
3. Na janela de **propriedades** que se abre, no painel esquerdo **Seções**, selecione **Lista de sub-redes globais**.
4. Na lista, selecione o sub-rede que você deseja.
5. Clique no botão **Propriedades**.

   A janela **Nova sub-rede** se abre.
6. Se necessário, altere as configurações da sub-rede.
7. Clique em **OK**.

Se você tiver feito alterações, elas serão armazenadas.

Uso do Agente de Rede para Windows, macOS e Linux: comparativo

O uso do Agente de Rede depende do sistema operacional do dispositivo. A política do Agente de Rede e as configurações do pacote de instalação também diferem, dependendo do sistema operacional. A tabela a seguir compara os recursos do Agente de Rede e os cenários de uso disponíveis para os sistemas operacionais Windows, macOS e Linux.

Comparativo de recursos do Agente de Rede

Recurso do Agente de Rede	Windows	macOS	Linux
Instalação			
Geração automática do pacote de instalação do Agente de Rede após a instalação do Kaspersky Security Center	✓	—	—
Instalar no modo forçado, usando opções especiais na tarefa de instalação remota do Kaspersky Security Center	✓	✓	✓
Instalar enviando aos usuários de dispositivo links para pacotes independentes pelo Kaspersky Security Center	✓	✓	✓
Instalando por clonagem uma imagem do disco rígido do administrador com o sistema operacional e com o Agente de Rede: utilizando ferramentas fornecidas pelo Kaspersky Security Center para tratar imagens do disco	✓	—	—
Instalando por clonagem uma imagem do disco rígido do administrador com o sistema operacional e o Agente de Rede usando ferramentas de terceiros	✓	✓	✓
Instalar com ferramentas de terceiros para a instalação remota de aplicativos	✓	✓	✓
Instalar manualmente, executando os instaladores do aplicativo em dispositivos	✓	✓	✓
Instalar o Agente de Rede em modo silencioso	✓	✓	✓
Conecte manualmente um dispositivo cliente ao Servidor de administração. Utilitário klmover	✓	✓	✓
Instalar as atualizações e patches para componentes do Kaspersky Security Center automaticamente	✓	—	—
Distribuir uma chave automaticamente	✓	✓	✓
Sincronização forçada	✓	✓	✓
Ponto de distribuição			
Usar como ponto de distribuição	✓	✓	✓
Atribuição automática de pontos de distribuição	✓	✓ Sem usar o Reconhecimento de Local de Rede (NLA).	✓ Sem usar o Reconhecimento de Local de Rede (NLA).
Modelo offline de download da atualização	✓	✓	✓

Recurso do Agente de Rede	Windows	macOS	Linux
Sondagem da rede	✓ • Sondagem do conjunto de IPs • Sondagem da rede do Windows • Sondagem do Active Directory	—	✓ Sondagem do conjunto de IPs
Execução do Serviço de Proxy da KSN no lado do ponto de distribuição	✓	—	✓
Baixar atualizações via servidores de atualização Kaspersky para os repositórios de pontos de distribuição que distribuem atualizações para dispositivos gerenciados	✓	— (Se um ou mais dispositivos executando Linux ou macOS estiverem dentro do escopo da tarefa Baixar atualizações para os repositórios de pontos de distribuição, a tarefa será concluída com o status Falha, mesmo se for concluída com êxito em todos os dispositivos Windows.)	✓
Instalação push de aplicativos	✓	Restrito: não é possível realizar a instalação push em dispositivos Windows usando pontos de distribuição do macOS.	Restrito: não é possível realizar instalação push em dispositivos Windows usando pontos de distribuição Linux.
Usar como servidor push	✓	—	✓
Gerenciamento de aplicativos de terceiros			
Instalação remota de aplicativos em dispositivos	✓	—	—
Atualizações de software	✓	—	—
Configurar as atualizações do sistema operacional em uma política de Agente de Rede	✓	—	—
Exibir informações sobre as vulnerabilidades do software	✓	—	—
Verificar os aplicativos quanto a vulnerabilidades	✓	—	—
Inventário de software instalado nos dispositivos	✓	—	—
Máquinas virtuais			
Instalar o Agente de Rede em uma máquina virtual	✓	✓	✓
As configurações de optimização da infraestrutura de desktop virtual (VDI)	✓	✓	✓
Suporte de máquinas virtuais dinâmicas	✓	✓	✓
Outro			
Auditoria de ações em um dispositivo cliente remoto usando o Windows Desktop Sharing	✓	—	—
Monitoramento do status de proteção antivírus	✓	✓	✓
Gerenciar reinícios de dispositivos	✓	—	—
Suporte da reversão do sistema	✓	✓	✓

Recurso do Agente de Rede	Windows	macOS	Linux
Usar um Agente de Rede como um gateway de conexão	✓	✓	✓
Gerenciador de conexões	✓	✓	✓
Agente de Rede alternando de um Servidor de Administração para outro (automaticamente pelo local da rede)	✓	✓	—
Verificar a conexão entre um dispositivo cliente e o Servidor de Administração. Utilitário klnagchk	✓	✓	✓
Conexão remota à Área de trabalho de um dispositivo cliente	✓	✓ Usando o sistema de computação de rede virtual (VNC).	—
Baixar um pacote de instalação independente por meio do Assistente de migração	✓	✓	✓
Sondagem Zeroconf	—	—	✓

Comparativo entre configurações de Agente de Rede por sistemas operacionais

A tabela abaixo mostra quais são as configurações do Agente de Rede disponíveis e dependendo do sistema operacional do dispositivo gerenciado no qual o Agente de Rede foi instalado.

Configurações do Agente de Rede: comparativo entre sistemas operacionais

Seção Settings	Windows	macOS	Linux
Geral	✓	✓	✓
Configuração de eventos	✓	✓	✓
Configurações	✓	✓	✓ As seguintes opções estão disponíveis: • **Distribuir os arquivos somente através dos pontos de distribuição** • **Tamanho máximo da fila de eventos, em MB** • **O aplicativo tem permissão para recuperar os dados estendidos da política no dispositivo**
Repositórios	✓	—	✓ As seguintes opções estão disponíveis: • **Detalhes dos aplicativos instalados** • **Detalhes do registro de hardware**
Atualizações e vulnerabilidades de software	✓	—	—
Gerenciamento de reinício	✓	—	—
Windows Desktop Sharing	✓	—	—
Gerenciar patches e atualizações	✓	—	—
Conectividade → Rede	✓	✓	✓ Exceto a opção **Abrir portas do Agente de Rede no firewall do Microsoft Windows**.
Conectividade → Perfis de conexão	✓	✓	—

Seção Settings	Windows	macOS	Linux
Conectividade → Agendador de conexão	✓	✓	✓
Sondagem da rede por pontos de distribuição	✓ Apenas as opções **Rede Windows**, **Intervalos de IPs** e **Active Directory** estão disponíveis.	—	✓ As seguintes opções estão disponíveis: • **Zeroconf** • **Intervalos de IPs**
Configurações de rede para pontos de distribuição	✓	✓	✓
KSN Proxy (pontos de distribuição)	✓	—	✓
Atualizações (pontos de distribuição)	✓	—	✓
Histórico de revisões	✓	✓	✓

Kaspersky Security Center Web Console

Esta seção descreve as operações que você pode executar usando o Kaspersky Security Center Web Console.

Sobre o Kaspersky Security Center Web Console

O Kaspersky Security Center Web Console (adiante também denominado Kaspersky Security Center Web Console) é um aplicativo Web concebido para gerenciar o status do sistema de segurança da rede protegida por aplicativos Kaspersky.

Usando o aplicativo, você pode:

- Gerenciar o status do sistema de segurança da organização.
- Instalar aplicativos Kaspersky em dispositivos em sua rede e gerenciar aplicativos instalados.
- Gerencie as políticas criadas para sue dispositivos na sua rede.
- Gerenciar contas de usuário.
- Gerenciar tarefas para aplicativos instalados em dispositivos na sua rede.
- Exibir relatórios sobre o status do sistema de segurança.
- Gerenciar a entrega de relatórios aos administradores do sistema e outros especialistas de TI.

Kaspersky Security Center Web Console fornece uma interface da Web que assegura a interação entre o seu dispositivo e o Servidor de Administração através de um navegador. O Servidor de Administração é um aplicativo projetado para gerenciar aplicativos da Kaspersky instalados nos dispositivos na sua rede. O Servidor de Administração se conecta com os dispositivos em sua rede através de canais protegidos pelo protocolo Secure Socket Layer (SSL). Quando você se conecta ao Kaspersky Security Center Web Console usando seu navegador, o navegador estabelece uma conexão com o servidor do Kaspersky Security Center Web Console.

Você opera o Kaspersky Security Center Web Console da seguinte maneira:

1. Use um navegador para se conectar ao Kaspersky Security Center Web Console, onde a interface do portal da Web é exibida.
2. Use controles do portal da Web para escolher o comando que você deseja executar. O Kaspersky Security Center Web Console executa as seguintes operações:
    - Se você tiver escolhido um comando usado para a recepção de informações (por exemplo, para visualizar uma lista de dispositivos), o Kaspersky Security Center Web Console gera uma solicitação de informação ao Servidor de Administração, recebe os dados necessários e os envia para o navegador em um formato de fácil visualização.
    - Se você tiver escolhido um comando usado para o gerenciamento (por exemplo, instalação remota de um aplicativo), o Kaspersky Security Center Web Console recebe o comando do navegador e o envia para o Servidor de Administração. A seguir, o aplicativo recebe o resultado do Servidor de Administração e o envia para o navegador da em um formato de fácil visualização.

O Kaspersky Security Center Web Console é um aplicativo disponível em vários idiomas. Você pode alterar o idioma da interface a qualquer momento, sem necessidade de reabrir o aplicativo. Ao instalar o Kaspersky Security Center Web Console com o Kaspersky Security Center Web Console, a solução usa o mesmo idioma de interface que o arquivo de instalação. Quando você instala apenas o Kaspersky Security Center Web Console, o aplicativo usa o mesmo idioma da interface do seu sistema operacional. Se o Kaspersky Security Center Web Console não for compatível com o idioma do arquivo de instalação ou do sistema operacional, o inglês será definido por padrão.

O Gerenciamento de Dispositivos Móveis não é suportado no Kaspersky Security Center Web Console. Contudo, se você tiver adicionado dispositivos móveis a um grupo de administração usando o Console de Gerenciamento Microsoft, esses dispositivos também serão exibidos no Kaspersky Security Center Web Console.

Requisitos de hardware e software para o Kaspersky Security Center Web Console

Kaspersky Security Center Web Console Server

Requisitos mínimos de hardware:

- CPU: 4 núcleos, frequência operacional de 2,5 GHz
- RAM: 8 GB
- Espaço disponível em disco: 40 GB

Sistemas operacionais compatíveis com o Kaspersky Security Center Web Console Server

Sistemas operacionais. Microsoft Windows (somente as versões 64 bits):	Windows Server 2012 Server Core Windows Server 2012 Datacenter Windows Server 2012 Essentials Windows Server 2012 Foundation Windows Server 2012 Standard Windows Server 2012 R2 Server Core Windows Server 2012 R2 Datacenter Windows Server 2012 R2 Essentials Windows Server 2012 R2 Foundation Windows Server 2012 R2 Standard Windows Server 2016 Datacenter (LTSB) Windows Server 2016 Standard (LTSB) Windows Server 2016 Server Core (opção de Instalação) (LTSB) Windows Server 2019 Standard Windows Server 2019 Datacenter Windows Server 2019 Core Windows Server 2022 Standard Windows Server 2022 Datacenter Windows Server 2022 Core Windows Storage Server 2012 Windows Storage Server 2012 R2 Windows Storage Server 2016 Windows Storage Server 2019
Sistemas operacionais. Linux (apenas versões de 64 bits)	Debian GNU/Linux 9.x (Stretch) Debian GNU/Linux 10.x (Buster) Debian GNU/Linux 11.x (Bullseye) Ubuntu Server 18.04 LTS (Bionic Beaver) Ubuntu Server 20.04 LTS (Focal Fossa) Ubuntu Server 22.04 LTS (Jammy Jellyfish) CentOS 7.x Red Hat Enterprise Linux Server 7.x Red Hat Enterprise Linux Server 8.x Red Hat Enterprise Linux Server 9.x SUSE Linux Enterprise Server 12 (todos os Service Packs) SUSE Linux Enterprise Server 15 (todos os Service Packs)

	Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.6) Astra Linux Special Edition RUSB.10015-01 (atualização operacional 1.7) Astra Linux Common Edition (atualização operacional 2.12) ALT Server 9.2 ALT Server 10 ALT 8 SP Server (LKNV.11100-01) ALT 8 SP Server (LKNV.11100-02) ALT 8 SP Server (LKNV.11100-03) Oracle Linux 7 Oracle Linux 8 Oracle Linux 9 RED OS 7.3 Server RED OS 7.3 Certified Edition Máquina virtual baseada em kernel (todos os sistemas operacionais Linux compatíveis com o Kaspersky Security Center Web Console Server)

Dispositivos cliente

Em um dispositivo cliente, o uso do Kaspersky Security Center Web Console requer apenas um navegador.

A resolução mínima da tela é de 1366x768 pixels.

Os requisitos de hardware e software para o dispositivo são idênticos aos requisitos do navegador utilizado com o Kaspersky Security Center Web Console.

Navegadores:

- Mozilla Firefox Extended Support Versão 91.8.0 ou posterior (91.8.0 lançada em 5 de abril de 2022)
- Google Chrome 100.0.4896.88 ou posterior (compilação oficial)
- Microsoft Edge 100 ou posterior
- Safari 15 no macOS

Diagrama de implementação do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center Web Console

A figura abaixo mostra o diagrama de implementação do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center Web Console.

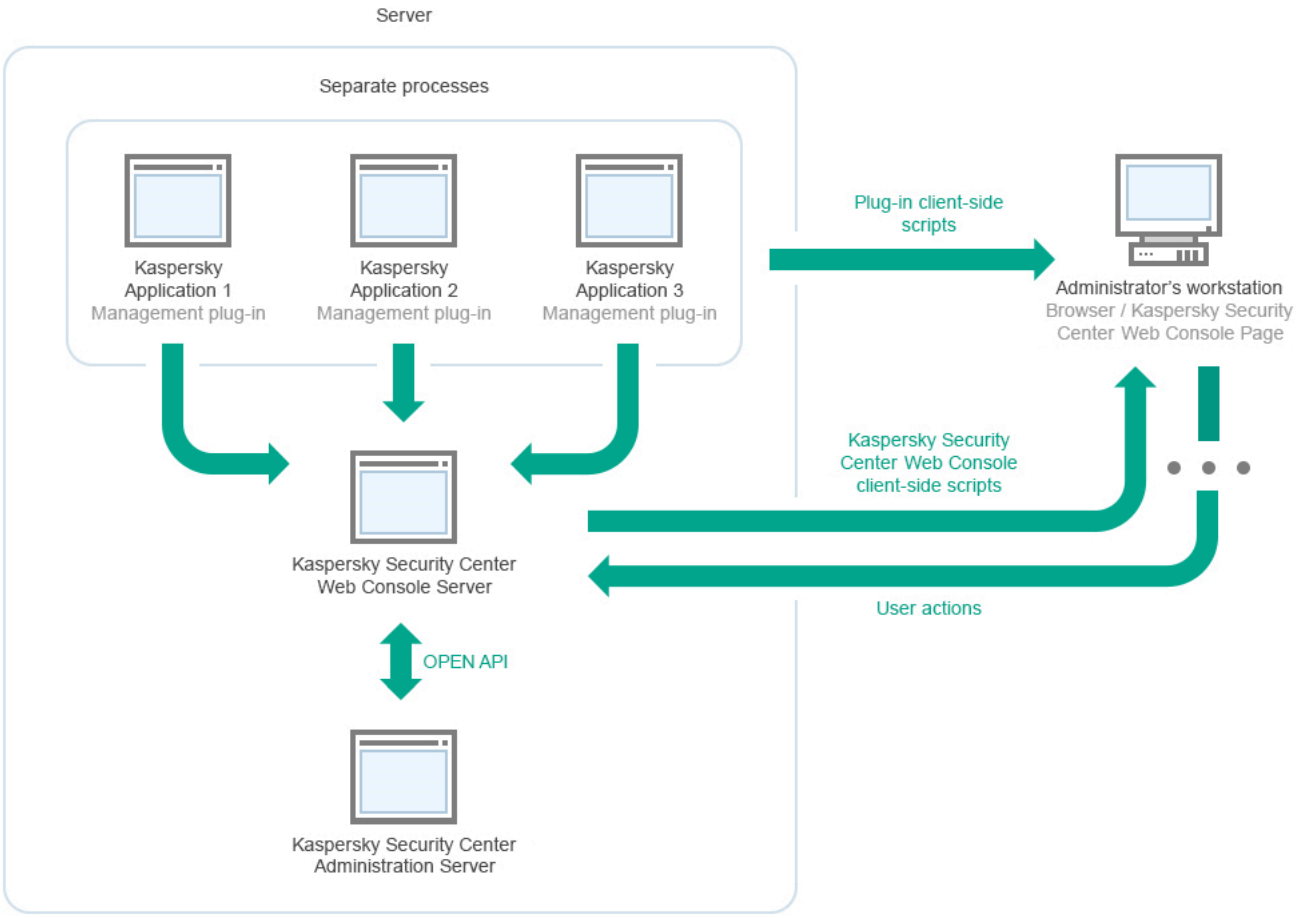


Diagrama de implementação do Servidor de Administração do Kaspersky Security Center e do Kaspersky Security Center Web Console

Os plugins para gerenciamento de aplicativos Kaspersky instalados em dispositivos protegidos (um plugin para cada aplicativo) são implementados juntamente com o Kaspersky Security Center Web Console Server.

Como administrador, você acessa o Kaspersky Security Center Web Console usando um navegador na sua estação de trabalho.

Quando você executa ações específicas no Kaspersky Security Center Web Console, o Kaspersky Security Center Web Console Server se comunica com o Servidor de Administração do Kaspersky Security Center por meio do OpenAPI. O Kaspersky Security Center Web Console Server solicita as informações necessárias do Servidor de Administração do Kaspersky Security Center e exibe os resultados das operações no Kaspersky Security Center Web Console.

Portas usadas pelo Kaspersky Security Center Web Console

A tabela abaixo lista as portas que devem estar abertas no dispositivo em que o Servidor do Kaspersky Security Center Web Console (também chamado de Kaspersky Security Center Web Console) está instalado.

Portas usadas pelo Kaspersky Security Center Web Console

Número da porta	Nome do serviço	Protocolo	Propósito da porta	Escopo
2001	Servidor de plugins de produto do Kaspersky Security Center	HTTPS	Porta de API usada pelos processos do plug-in de gerenciamento para receber solicitações do "Serviço de gerenciamento do Kaspersky Security Center Web Console"	Execução de processos node.exe de plug-ins de gerenciamento
1329, 2003	Serviço de gerenciamento do Kaspersky Security Center Web Console	HTTPS	Portas de API usadas para receber solicitações do "Serviço de gerenciamento do Kaspersky Security Center Web Console" em execução no mesmo dispositivo	Atualização de componentes do Kaspersky Security Center Web Console
2005	Kaspersky Security Center Web Console	HTTPS	Porta de API usada para receber solicitações do "Serviço de gerenciamento do Kaspersky Security Center Web Console" em execução no mesmo dispositivo	Execução dos processos node.exe do Kaspersky Security Center Web Console
3333	Serviço Kaspersky OSMP KAS	HTTPS	Porta do endpoint de autorização do OAuth2.0	Gerenciador de identidade e Acesso (IAM)
4004	Kaspersky OSMP Facade Service	HTTPS	Porta do provedor de identidade OAuth2.0	Gerenciador de identidade e Acesso (IAM)
4444	Serviço Kaspersky OSMP KAS	HTTPS	Porta do endpoint de introspecção de token do OAuth2.0	Gerenciador de identidade e Acesso (IAM)
8200	—	HTTP	Porta API usada para gerar certificados por meio do HashiCorp Vault (para mais detalhes, consulte o site do HashiCorp Vault)	Instalação do Kaspersky Security Center Web Console e atualização dos componentes do Kaspersky Security Center Web Console
4150, 4151, 4152	Fila de mensagens do Kaspersky Security Center Web Console	HTTPS	Portas API do processador de mensagens usadas para comunicação entre processos do Kaspersky Security Center Web Console e plugins de gerenciamento	Interação de processos entre o Kaspersky Security Center Web Console e os plugins de gerenciamento

A tabela a seguir lista as portas que não precisam ser abertas no dispositivo onde o Kaspersky Security Center Web Console Server está instalado. No entanto, o Kaspersky Security Center Web Console usa essas portas para o Gerenciador de Identidade e Acesso.

Portas usadas pelo Kaspersky Security Center Console da Web para o Gerenciador de Identidade e Acesso

Número da porta	Nome do serviço	Protocolo	Propósito da porta	Escopo
4445	Serviço Kaspersky OSMP KAS	HTTPS	Porta principal do Identity and Access Manager que recebe a configuração do Kaspersky Security Center Web Console para a porta do terminal de autorização do OAuth2.0 (para obter mais informações sobre o OAuth 2.0, consulte o site do OAuth)	Gerenciador de identidade e Acesso (IAM)
2444	Kaspersky OSMP Facade Service	HTTPS	Porta para a configuração do Gerenciador de Identidade e Acesso	Gerenciador de identidade e Acesso (IAM)
2445	Kaspersky OSMP Facade Service	HTTPS	Porta para conexão do "Kaspersky OSMP KAS Service" ao "Kaspersky OSMP Facade Service"	Gerenciador de identidade e Acesso (IAM)

Cenário: instalação e configuração inicial do Kaspersky Security Center Web Console

Este cenário descreve como instalar o Servidor de Administração do Kaspersky Security Center e o Kaspersky Security Center Web Console, como executar a configuração inicial do Servidor de Administração usando o Assistente de início rápido e como instalar aplicativos da Kaspersky nos dispositivos gerenciados usando o Assistente de implementação de proteção.

A instalação e configuração inicial do Kaspersky Security Center Web Console prossegue em etapas:

1. **Instalação de um sistema de gerenciamento de banco de dados (DBMS)**

   Instale o DBMS que será usado pelo Kaspersky Security Center ou use um existente.

   Para obter informações sobre como instalar o DBMS selecionado, consulte a sua documentação.

2. **Instalação do Servidor de Administração, Console de Administração, Agente de Rede**

   O Console de Administração e a versão do servidor do Agente de Rede são instaladas em conjunto com o Servidor de Administração.

   Durante a instalação do Servidor de Administração do Kaspersky Security Center, especifique se deseja instalar o Kaspersky Security Center Web Console no mesmo dispositivo. Se decidir instalar ambos os componentes no mesmo dispositivo, você não precisará instalar o Kaspersky Security Center Web Console separadamente, porque ele é instalado automaticamente. Caso queira instalar o Kaspersky Security Center Web Console em um dispositivo diferente, depois de instalar o Servidor de Administração do Kaspersky Security Center, prossiga com a instalação do Kaspersky Security Center Web Console.

3. **Instalar o Kaspersky Security Center Web Console**

   Se tiver decidido não instalar o Kaspersky Security Center Web Console em conjunto com o Servidor de Administração do Kaspersky Security Center na etapa anterior, instale o Kaspersky Security Center Web Console separadamente. Você pode instalar o Kaspersky Security Center Web Console em um dispositivo diferente ou no mesmo dispositivo em que o Servidor de Administração está instalado.

4. **Execução da configuração inicial**

   Quando a instalação de Servidor de Administração estiver concluída, na primeira conexão ao Servidor de Administração o Assistente de início rápido inicia automaticamente. Execute a configuração inicial do Servidor de Administração de acordo com os requisitos existentes. Durante a etapa de configuração inicial, o assistente usa as configurações padrão para criar as políticas e tarefas necessárias para a implementação de proteção. No entanto, as configurações padrão podem ser menos ótimas para as necessidades da sua organização. Se necessário, você pode editar as configurações das políticas e tarefas.

5. **Licenciamento do Kaspersky Security Center (opcional)**

   O Kaspersky Security Center com o suporte da funcionalidade básica do Console de Administração não necessita de uma licença. Você precisará de uma licença comercial se quiser usar um ou vários dos recursos adicionais, inclusive Gerenciamento de patches e vulnerabilidades, Gerenciamento de Dispositivos Móveis e Integração com os sistemas SIEM. Você pode adicionar um arquivo de chave ou um código de ativação para esses recursos na etapa correspondente do Assistente de início rápido ou manualmente.

6. **Localização de dispositivos na rede**

Esta etapa faz parte do Assistente de início rápido. Você também pode descobrir os dispositivos manualmente. O Kaspersky Security Center recebe os endereços e os nomes de todos os dispositivos detectados na rede. Você então pode usar o Kaspersky Security Center para instalar aplicativos Kaspersky e software de outros fornecedores nas dispositivos detectados. O Kaspersky Security Center regularmente inicia uma descoberta de dispositivos, o que significa que se alguma nova instância aparecer na rede, ela será detectada automaticamente.

7. **Organização de dispositivos em grupos de administração**

   Esta etapa faz parte do Assistente de início rápido, mas você também pode mover manualmente os dispositivos detectados para os grupos.

8. **Instalar o Agente de Rede e aplicativos de segurança em dispositivos na rede**

   A implementação da proteção em uma rede corporativa engloba a instalação do Agente de Rede e de aplicativos de segurança (por exemplo, Kaspersky Endpoint Security for WIndows) nos dispositivos que foram detectados pelo Servidor de Administração durante a descoberta de dispositivos.

   Para instalar os aplicativos remotamente, execute o Assistente de implementação da proteção.

   Os aplicativos de segurança protegem os dispositivos contra vírus e outros programas que apresentem uma ameaça. O Agente de Rede assegura a comunicação entre o dispositivo e o Servidor de Administração. As configurações do Agente de Rede são definidas automaticamente por padrão.

   Antes que você inicie a instalação do Agente de Rede e dos aplicativos de segurança nos dispositivos na rede, assegure-se de que estes dispositivos estejam acessíveis (ligados).

9. **Implementação de chaves de licença para dispositivos clientes**

   Implemente chaves de licença em dispositivos clientes para ativar aplicativos de segurança gerenciados naqueles dispositivos.

10. **Instalando o Kaspersky Security for Mobile (opcional)**

    Se você planeja gerenciar dispositivos móveis corporativos, siga as instruções fornecidas no Ajuda do Kaspersky Security for Mobile para obter informações sobre a implementação do Kaspersky Endpoint Security for Android.

11. **Configuração de políticas de aplicativo da Kaspersky**

    Para aplicar configurações de aplicativo diferentes a dispositivos diferentes, você pode usar gerenciamento de segurança centrado no dispositivo e/ou gerenciamento de segurança centrado no usuário. O gerenciamento de segurança centrado no dispositivo pode ser implementado usando políticas e tarefas. Você pode aplicar tarefas somente aos dispositivos que atendem a condições específicas. Para definir as condições para filtrar dispositivos, use seleções de dispositivos e identificadores.

12. **Monitorar o status da proteção da rede**

    Você pode monitorar sua rede usando widgets no relatório, gerar relatórios a partir de aplicativos da Kaspersky, configurar e visualizar seleções de eventos recebidos dos aplicativos nos dispositivos gerenciados e visualizar listas de notificações.

Instalação

Esta seção descreve a instalação do Kaspersky Security Center e do Kaspersky Security Center Web Console.

Instalar o Kaspersky Security Center Web Console

Esta seção descreve como instalar o Kaspersky Security Center Web Console Server (também mencionado como Kaspersky Security Center Web Console) separadamente. Antes da instalação, é necessário instalar um DBMS e o Servidor de Administração do Kaspersky Security Center. Você pode instalar o Kaspersky Security Center Web Console no mesmo dispositivo onde o Kaspersky Security Center está instalado ou em outro.

Para instalar o Kaspersky Security Center Web Console:

1. Em uma conta com privilégios de administrador, execute o arquivo de instalação ksc-web-console-<número da versão>.<número da compilação>.exe.

   Isso inicia o Assistente de instalação.

2. Selecione um idioma para o Assistente de instalação.

3. Na janela de boas-vindas, clique em **Avançar**.

4. Na janela **Contrato de Licença**, leia e aceite os termos do Contrato de Licença do Usuário Final. A instalação continua depois que você aceita o EULA, caso contrário, o botão **Avançar** ficará indisponível.

5. Na janela **Pasta de destino**, selecione a pasta na qual o Kaspersky Security Center Web Console será instalado (por padrão, %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center Web Console). Se essa pasta não existir, ela é criada automaticamente durante a instalação.

   Você pode alterar a pasta de destino usando o botão **Procurar**.

6. Na janela **Configurações de conexão do Kaspersky Security Center Web Console**, especifique as seguintes informações:

   - O endereço do Kaspersky Security Center Web Console (por padrão, 127.0.0.1);
   - A porta que o Kaspersky Security Center Web Console usará para conexões de entrada, ou seja, a porta que dá acesso ao Kaspersky Security Center Web Console a partir de um navegador (por padrão, 8080).

   Recomendamos que você deixe o endereço e o número de porta como estão.

   Se quiser, pode clicar em **Teste** para se assegurar de que a porta selecionada esteja disponível.

   Se quiser ativar o registro em log das atividades do Kaspersky Security Center Web Console, selecione a opção apropriada. Se não marcar esta caixa de seleção, os arquivos de registro do Kaspersky Security Center Web Console não serão criados.

7. Na janela **Configurações da conta**, especifique os nomes e as senhas da conta.

   Recomendamos o uso de contas padrão.

8. Na janela **Certificado de cliente**, selecione um dos seguintes itens:

   - **Gerar novo certificado**. Esta opção será recomendada se você não tiver um certificado de navegador.
   - **Escolher certificado existente**. Você poderá selecionar esta opção se já tiver um certificado de navegador; nesse caso, especifique o caminho até ele.
   - Se optar por gerar um novo certificado, quando o Kaspersky Security Center Web Console for aberto, o navegador poderá informar que a conexão com o Kaspersky Security Center Web Console não é privada e o certificado do Kaspersky Security Center Web Console é inválido. Essa advertência aparece, porque o certificado do Kaspersky Security Center Web Console é autoassinado e gerado automaticamente pelo Kaspersky Security Center. Para remover essa advertência, crie um certificado confiável na infraestrutura e que atenda aos requisitos para certificados personalizados. A seguir, selecione a opção **Escolher certificado existente** na janela **Certificado de cliente** e, em seguida, especifique o caminho para o seu certificado personalizado.

   Não há compatibilidade para certificados em formato PFX no Kaspersky Security Center Web Console. Para usar esse certificado, primeiro é necessário convertê-lo para o formato PEM compatível usando um utilitário multiplataforma baseado em OpenSSL, como o OpenSSL para Windows.

9. Na janela **Servidores de Administração confiáveis**, verifique e confirme se o Servidor de Administração está na lista e clique em **Avançar** para prosseguir até a última janela do instalador.

   Se for necessário adicionar um novo Servidor de Administração na lista, clique no botão **Adicionar**. Na janela aberta, especifique as propriedades de um novo Servidor de Administração confiável:

   - **Nome do Servidor de Administração**

     O nome do Servidor de Administração que será exibido na janela de login do Kaspersky Security Center Web Console.

   - **Endereço do Servidor de Administração**

     O endereço IP do dispositivo no qual o Servidor de Administração é instalado.

   - **Porta do Servidor de Administração**

     A porta OpenAPI usada pelo Kaspersky Security Center Web Console para se conectar ao Servidor de Administração (o valor padrão é 13299).

   - **Certificado do Servidor de Administração**

     O arquivo do certificado fica armazenado no dispositivo no qual o Servidor de Administração está instalado. O caminho padrão para o certificado do Servidor de Administração:

     - Para Windows – %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
     - Para Linux – /var/opt/kaspersky/klnagent_srv/1093/cert/

     Caso o Kaspersky Security Center Web Console seja instalado no mesmo dispositivo no qual o Servidor de Administração está instalado, use um dos caminhos fornecidos acima. Caso contrário, copie o arquivo de certificado do dispositivo no qual o Servidor de Administração está instalado para o dispositivo no qual o Kaspersky Security Center Web Console foi instalado e especifique o caminho local para o certificado.

10. Na janela **Identity and Access Manager (IAM)**, especifique se deseja instalar o Gerenciador de Identidade e Acesso (também conhecido como IAM). Se você optar por instalar o Gerenciador de Identidade e Acesso, especifique os seguintes números de porta:

    - **Porta do administrador KAS**. Por padrão, a porta 4445 é usada para receber a configuração da porta do terminal de autorização do Kaspersky Security Center para o OAuth2.0.
    - **Porta de admin Facade**. Por padrão, a porta 2444 é usada para a configuração do Gerenciador de Identidade e Acesso.
    - **Porta de interação Facade**. Por padrão, a porta 2445 é usada para a conexão do Kaspersky OSMP KAS Service ao Kaspersky OSMP Facade Service.

    Se desejar, poderá modificar os números de porta padrão. Você não poderá alterá-los no futuro por meio do Kaspersky Security Center Web Console.

11. Na última janela do instalador, clique em **Instalar** para começar a instalação.

Após a instalação ser concluída com sucesso, é exibido um atalho na área de transferência e você pode fazer login no Kaspersky Security Center Web Console.

O Assistente de início rápido do Servidor de Administração será iniciado caso o Console de Administração baseado no Console de Gerenciamento Microsoft não tenha sido executado.

Solução de problemas

Se o Kaspersky Security Center Web Console não for exibido no navegador na URL digitada, tente o seguinte:

1. Verifique se você especificou o nome do host ou o endereço IP correto do dispositivo em que o Kaspersky Security Center Web Console está instalado.
2. Verifique se o dispositivo que deseja operar tem o acesso ao dispositivo em que o Kaspersky Security Center Web Console está instalado.
3. Verifique se as configurações de firewall no dispositivo em que o Kaspersky Security Center Web Console está instalado permitem conexões de entrada pela porta 8080 e para o aplicativo node.exe.
4. No Windows, abra **Serviços**. Verifique se o serviço Kaspersky Security Center Web Console está em execução.
5. Verifique se você pode acessar o Kaspersky Security Center usando o Console de Administração.
6. No Windows, abra o **Visualizador de Eventos** e selecione **Logs de Aplicativos e Serviços → Log de Eventos Kaspersky**. Certifique-se de que o log não contenha erros.

Instalação do Kaspersky Security Center Web Console em plataformas Linux

Esta seção explica como instalar o Kaspersky Security Center Web Console Server (também mencionado como Kaspersky Security Center Web Console) em dispositivos com o sistema operacional Linux (veja a lista de distribuições Linux compatíveis).

Instalar o Kaspersky Security Center Web Console em plataformas Linux

Esta seção descreve como instalar o Kaspersky Security Center Web Console Server (também mencionado como Kaspersky Security Center Web Console) em dispositivos que executam o sistema operacional Linux. Antes da instalação, é necessário instalar um DBMS e o Servidor de Administração do Kaspersky Security Center.

Use um dos seguintes arquivos de instalação que corresponda à distribuição Linux instalada em seu dispositivo:

- Para Debian: ksc-web-console-<número da compilação>.x86_64.deb
- Para sistemas operacionais baseados em RPM: ksc-web-console-<número da compilação>.x86_64.rpm
- Para ALT 8 SP: ksc-web-console-<número da compilação>-alt8p.x86_64.rpm

Para receber o arquivo de instalação, baixe-o do site da Kaspersky.

Para instalar o Kaspersky Security Center Web Console:

1. Certifique-se de que o dispositivo no qual você quer instalar o Kaspersky Security Center Web Console está executando uma das distribuições Linux compatíveis.
2. Leia o Contrato de Licença do Usuário Final (EULA). Caso o kit de distribuição do Kaspersky Security Center não inclua um arquivo TXT com o texto do EULA, é possível baixá-lo no site da Kaspersky. Se você não aceitar os termos do Contrato de Licença, não instale o aplicativo.

3. Crie um arquivo de resposta que contenha os parâmetros para conectar o Kaspersky Security Center Web Console ao Servidor de Administração. Nomeie esse arquivo ksc-web-console-setup.json e o coloque no seguinte diretório: /etc/ksc-web-console-setup.json.

   Exemplo de um arquivo de resposta que contém o conjunto mínimo de parâmetros e o endereço e a porta padrão:

   ```
   {
     "address": "ksc.example.com",
     "port": 8080,
     "trusted":
   "192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC
   Server",
     "acceptEula": true
   }
   ```

   Ao instalar o Kaspersky Security Center Web Console no sistema operacional Linux ALT, é necessário especificar um número de porta diferente de 8080, pois essa porta é usada pelo sistema operacional.

   Kaspersky Security Center Web Console não pode ser atualizado usando o mesmo arquivo de instalação .rpm. Se você deseja alterar as configurações em um arquivo de resposta e usar esse arquivo para reinstalar o aplicativo, primeiro remova o aplicativo e, em seguida, instale-o novamente com o novo arquivo de resposta.

4. Em uma conta com privilégios de raiz, use a linha de comando para executar o arquivo de configuração com a extensão .deb ou .rpm, dependendo da sua distribuição Linux.

   - Para instalar ou atualizar o Kaspersky Security Center Web Console a partir de um arquivo .deb, execute o seguinte comando:

     ```
     $ sudo dpkg -i ksc-web-console-<número da compilação>.deb
     ```

   - Para instalar o Kaspersky Security Center Web Console a partir de um arquivo .rpm, execute o seguinte comando:

     ```
     $ sudo rpm -ivh --nodeps ksc-web-console-<número da compilação>.x86_64.rpm
     ```

   - Para atualizar de uma versão anterior do Kaspersky Security Center Web Console, execute um dos seguintes comandos:

     - Para os dispositivos que executam sistema operacional baseado em RPM:

       ```
       $ sudo rpm -Uvh --nodeps --force ksc-web-console-<número da
       compilação>.x86_64.rpm
       ```

     - Para os dispositivos com sistema operacional baseado em Debian:

       ```
       $ sudo dpkg -i ksc-web-console-<número da compilação>.x86_64.deb
       ```

   Essa ação inicia a descompactação do arquivo de configuração. Espere até que a instalação seja concluída. Kaspersky Security Center Web Console está instalado no seguinte diretório: /var/opt/kaspersky/ksc-web-console.

Quando a instalação estiver concluída, você poderá usar o navegador para abrir e fazer login no Kaspersky Security Center Web Console.

Parâmetros de instalação do Kaspersky Security Center Web Console

Para instalar o Kaspersky Security Center Web Console Server em dispositivos que executam o Linux, é preciso criar um arquivo de resposta no formato JSON que contém os parâmetros para conectar o Kaspersky Security Center Web Console ao Servidor de Administração.

Exemplo de um arquivo de resposta que contém o conjunto mínimo de parâmetros e o endereço e a porta padrão:

```
{
  "address": "ksc.example.com",
  "port": 8080,
  "defaultLangId": 1049,
  "enableLog": false,
  "trusted":
"192.168.2.130|13299|/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer|KSC Server",
  "acceptEula": true,
  "certPath": "/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer",
  "webConsoleAccount": "Group1:User1",
  "managementServiceAccount": "Group1:User2",
  "serviceWebConsoleAccount": "Group1:User3",
  "pluginAccount": "Group1:User4",
  "messageQueueAccount": "Group1:User5"
}
```

Ao instalar o Kaspersky Security Center Web Console no sistema operacional Linux ALT, é necessário especificar um número de porta diferente de 8080, pois essa porta é usada pelo sistema operacional.

A tabela abaixo descreve os parâmetros que podem ser especificados em um arquivo de resposta.

Parâmetros para instalar o Kaspersky Security Center Web Console em dispositivos que executam o Linux

Parâmetro	Descrição	Valores disponíveis
`address`	Endereço do Kaspersky Security Center Web Console Server (necessário).	Valor da sequência de caracteres.
`port`	Número da porta que o Kaspersky Security Center Web Console Server usará para se conectar ao Servidor de Administração (necessário).	Valor numérico.

Parâmetro	Descrição	Valores disponíveis
`defaultLangId`	Idioma da interface do usuário (por padrão, `1033`).	Código numérico do idioma: • Alemão: `1031` • Inglês: `1033` • Espanhol: `3082` • Espanhol (México): `2058` • Francês: `1036` • Japonês: `1041` • Cazaque: `1087` • Polonês: `1045` • Português (Brasil): `1046` • Russo: `1049` • Turco: `1055` • Chinês simplificado: `4` • Chinês tradicional: `31748` Se nenhum valor for especificado, o idioma inglês será usado.
`enableLog`	Se ativar o registro da atividade do Kaspersky Security Center Web Console.	Valor booleano: • `true` – O registro é ativado (selecionado por padrão). • `false` – O registro é desativado.
`trusted`	Lista de Servidores de Administração de confiança permitidos para conexão com o Kaspersky Security Center Web Console (requerido). Cada Servidor de Administração deve ser definido com os seguintes parâmetros: • Administration Server address • Porta OpenAPI que é usada pelo Kaspersky Security Center Web Console para se conectar ao Servidor de Administração (por padrão, 13299) • Caminho para o certificado do Servidor de Administração • Nome do Servidor de Administração que será exibido na janela de login Os parâmetros são separados por barras verticais. Se vários Servidores de Administração forem especificados, separe-os por duas barras verticais (pipes).	Valor da sequência de caracteres no seguinte formato: `"< server address >|< port >|< certificate path >|< server name >"`. Exemplo: `"X.X.X.X|13299|/cert/server-1.cer|Server 1||Y.Y.Y.Y|13299|/cert/server-2.cer|Server 2"`.
`acceptEula`	Se você aceita ou não os termos do Contrato de Licença do Usuário Final (EULA). O arquivo que contém os termos do EULA é baixado junto com o arquivo de instalação (requerido).	Valor booleano: • `true` – Confirmo que li, entendi e aceito integralmente os termos e condições deste Contrato de Licença do Usuário Final. • `false` – Eu não aceito os termos do Contrato de Licença (selecionado por padrão).

Parâmetro	Descrição	Valores disponíveis
`certDomain`	Se você quiser gerar um novo certificado, use este parâmetro para especificar o nome de domínio para o qual um novo certificado deve ser gerado.	Valor da sequência de caracteres.
`certPath`	Se você quiser usar um certificado existente, use este parâmetro para especificar o caminho até o arquivo de certificado.	Valor da sequência de caracteres. Especifique o caminho `"/var/opt/kaspersky/klnagent_srv/1093/cert/klserver.cer"` para utilizar o certificado existente. Para um certificado personalizado, especifique o caminho onde o certificado personalizado está armazenado.
`keyPath`	Se você quiser usar um certificado existente, use este parâmetro para especificar o caminho até o arquivo de chave.	Valor da sequência de caracteres.
`webConsoleAccount`	Nome da conta sob a qual o serviço do Kaspersky Security Center Web Console é executado.	Valor da sequência de caracteres no seguinte formato: `"< nome do grupo >: < nome de usuário ">`. Exemplo: `"Group1:User1"`. Se nenhum valor for especificado, o instalador do Kaspersky Security Center Web Console criará uma nova conta com o nome padrão `user_management_%uid%`.
`managementServiceAccount`	Nome da conta privilegiada sob a qual o Serviço de gerenciamento do Kaspersky Security Center Web Console é executado.	Valor da sequência de caracteres no seguinte formato: `"< nome do grupo >: < nome de usuário ">`. Exemplo: `"Group1:User1"`. Se nenhum valor for especificado, o instalador do Kaspersky Security Center Web Console criará uma nova conta com o nome padrão `user_nodejs_%uid%`.
`serviceWebConsoleAccount`	Nome da conta sob a qual o serviço do Kaspersky Security Center Web Console é executado.	Valor da sequência de caracteres no seguinte formato: `"< nome do grupo >: < nome de usuário ">`. Exemplo: `"Group1:User1"`. Se nenhum valor for especificado, o instalador do Kaspersky Security Center Web Console criará uma nova conta com o nome padrão `user_svc_nodejs_%uid%`.
`pluginAccount`	Nome da conta sob a qual o serviço do Servidor de plug-ins de produto do Kaspersky Security Center é executado.	Valor da sequência de caracteres no seguinte formato: `"< nome do grupo >: < nome de usuário ">`. Exemplo: `"Group1:User1"`. Se nenhum valor for especificado, o instalador do Kaspersky Security Center Web Console criará uma nova conta com o nome padrão `user_web_plugin_%uid%`.
`messageQueueAccount`	Nome da conta sob a qual o serviço de Fila de mensagens do Kaspersky Security Center Web Console é executado.	Valor da sequência de caracteres no seguinte formato: `"< nome do grupo >: < nome de usuário ">`. Exemplo: `"Group1:User1"`. Se nenhum valor for especificado, o instalador do Kaspersky Security Center Web Console criará uma nova conta com o nome padrão `user_message_queue_%uid%`.

Por motivos de segurança, não recomendamos usar os parâmetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount` e `messageQueueAccount`.

Caso especifique os parâmetros `webConsoleAccount`, `managementServiceAccount`, `serviceWebConsoleAccount`, `pluginAccount`, ou `messageQueueAccount` verifique e confirme se as contas de usuário personalizadas pertencem ao mesmo grupo de segurança. Se esses parâmetros não forem especificados, o instalador do Kaspersky Security Center Web Console criará um grupo de segurança padrão e, em seguida, criará contas de usuário com nomes padrão nesse grupo.

Instalação do Kaspersky Security Center Web Console conectado ao Servidor de Administração instalado nos nós do cluster de failover

Esta seção descreve como instalar o Kaspersky Security Center Web Console Server (doravante também referido como Kaspersky Security Center Web Console), que se conecta ao Servidor de Administração instalado em nós do cluster de failover do Kaspersky Security Center ou nós do cluster de failover do Windows Server. Antes de instalar o Kaspersky Security Center Web Console, instale um DBMS e um Servidor de Administração do Kaspersky Security Center em nós do cluster de failover do Kaspersky Security Center ou em nós do cluster de failover do Windows Server.

Caso um cluster de failover do Windows Server seja usado, não recomendamos instalar o Kaspersky Security Center Web Console em um nó de cluster de failover. Em caso de falha do nó, o acesso ao Servidor de Administração será perdido.

Para instalar o Kaspersky Security Center Web Console que se conecta ao Servidor de Administração instalado nos nós do cluster de failover:

1. Execute as etapas de instalação do Kaspersky Security Center Web Console, começando na etapa 1 até a etapa 8.

2. Na etapa 9, na janela **Servidores de Administração confiáveis**, clique no botão **Adicionar** para adicionar um cluster de failover como um Servidor de Administração confiável.

   Na janela aberta, especifique as seguintes propriedades:

   - **Nome do Servidor de Administração**

     O nome do cluster que será exibido na janela de login do Kaspersky Security Center Web Console.

   - **Endereço do Servidor de Administração**

     Dependendo do tipo de cluster de failover, especifique o endereço do cluster:

     - **Cluster de failover do Kaspersky Security Center**. Especifique o endereço IP do adaptador de rede secundário como o endereço do cluster caso tenha criado o adaptador durante o preparo dos nós de cluster. Caso contrário, especifique o endereço IP do balanceador de carga de terceiros em uso.

     - **Cluster de failover do Windows Server**. Especifique o endereço do cluster obtido ao criar o cluster de failover do Windows Server.

   - **Porta do Servidor de Administração**

     A porta OpenAPI usada pelo Kaspersky Security Center Web Console para se conectar ao Servidor de Administração (o valor padrão é 13299).

   - **Certificado do Servidor de Administração**

     O certificado do Servidor de Administração está localizado no armazenamento de dados compartilhado do cluster de failover do Kaspersky Security Center ou do cluster de failover do Windows Server. O caminho padrão para o arquivo de certificado: <dados da pasta compartilhada>\1093\cert\klserver.cer. Copie o arquivo de certificado do armazenamento de dados compartilhado para o dispositivo onde o Kaspersky Security Center Web Console foi instalado. Especifique o caminho local para o certificado do Servidor de Administração.

3. Continue com a instalação padrão do Kaspersky Security Center Web Console.

Após a instalação ser concluída com sucesso, um atalho será exibido na área de transferência e será possível fazer login no Kaspersky Security Center Web Console.

Atualizar o Kaspersky Security Center Web Console

Caso deseje utilizar uma versão mais recente do Kaspersky Security Center Web Console sem remover a instância atualmente instalada, é possível usar o procedimento de atualização padrão fornecido no instalador do Kaspersky Security Center Web Console.

Para atualizar o Kaspersky Security Center Web Console:

1. Em uma conta com direitos de administrador, execute o arquivo de instalação ksc-web-console-<número da versão>.exe, onde <número da compilação> significa uma compilação do Kaspersky Security Center Web Console cujo número é posterior a sua instância atualmente instalada.

2. Na janela do Assistente de instalação que se abre, selecione um idioma e clique em **OK**.

3. Na janela de boas-vindas, selecione a opção **Efetuar upgrade** e, em seguida, clique em **Avançar**.

4. Na janela **Contrato de Licença**, leia e aceite os termos do Contrato de Licença do Usuário Final. A instalação continua depois que você aceita o EULA; caso contrário, o botão **Avançar** ficará indisponível.

5. Prossiga pelas etapas do assistente de instalação até concluir a instalação. Ao progredir, também é possível modificar as configurações do Kaspersky Security Center Web Console que foram especificadas durante a instalação anterior. Quando você chegar na etapa **Pronto para modificar o Kaspersky Security Center Web Console**, clique no botão **Efetuar upgrade**. Aguarde até que as novas configurações sejam aplicadas e, na próxima etapa do Assistente de Instalação, clique em **Concluir**. Também é possível clicar no link **Iniciar o Kaspersky Security Center Web Console no seu navegador** para iniciar a instância atualizada do Kaspersky Security Center Web Console imediatamente.

   > A modificação das configurações do Kaspersky Security Center Web Console durante a atualização está disponível apenas no Kaspersky Security Center Web Console versão 12.2 ou posterior.

   A sua instância do Kaspersky Security Center Web Console será atualizada.

Certificados para trabalhar com o Kaspersky Security Center Web Console

A seção descreve como emitir e substituir certificados para o Kaspersky Security Center Web Console e como renovar um certificado para o Servidor de Administração se o Servidor interagir com o Kaspersky Security Center Web Console.

Substituir o certificado do Kaspersky Security Center Web Console

Por padrão, quando você instala o Kaspersky Security Center Web Console Server, um certificado do navegador para o aplicativo é gerado automaticamente. Você pode substituir o certificado automaticamente gerado por um certificado personalizado.

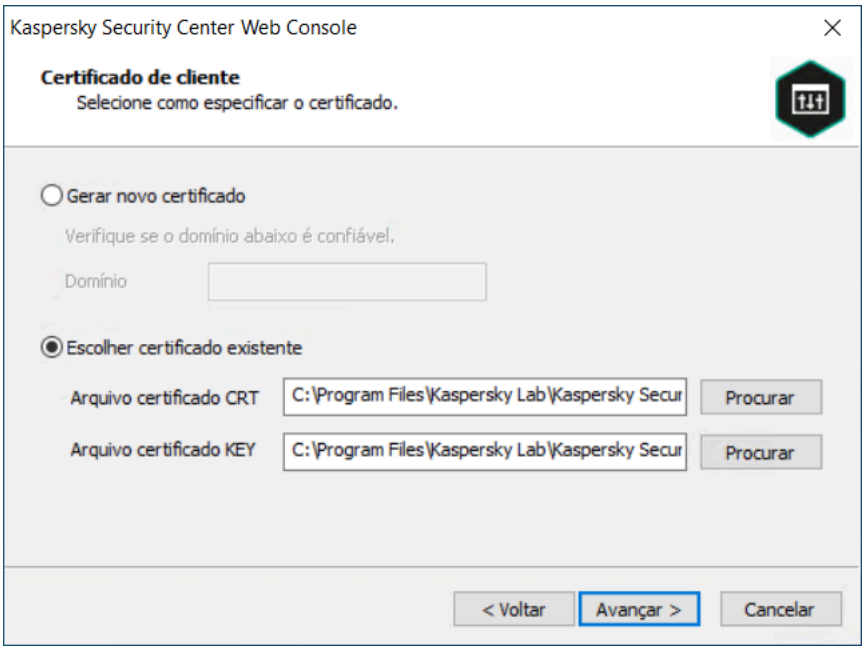
Para substituir o certificado do Kaspersky Security Center Web Console Server por um certificado personalizado:

1. No dispositivo em que o Kaspersky Security Center Web Console Server está instalado, execute o arquivo de instalação ksc-web-console-<número da versão>.<número da compilação>.exe em uma conta com direitos administrativos.

   Isso inicia o Assistente de instalação.

2. Na primeira página do assistente, selecione a opção **Atualizar**.

3. Na página **Certificado do cliente**, selecione a opção **Escolher certificado existente** e especifique o caminho para o certificado personalizado.



Especificar o certificado de cliente

4. Na última página do assistente, clique em **Modificar** para aplicar as novas configurações.

5. Após a conclusão com êxito da reconfiguração do aplicativo, clique no botão **Concluir**.

O Kaspersky Security Center Web Console funciona com o certificado especificado.

Especificar certificados para Servidores de Administração confiáveis no Kaspersky Security Center Web Console

O certificado existente do Servidor de Administração é automaticamente substituído pelo novo certificado antes da data de expiração do certificado. Você também pode substituir o certificado existente do Servidor de Administração por um personalizado. Cada vez que o certificado for substituído, o novo certificado deve ser especificado nas configurações do Kaspersky Security Center Web Console. Caso contrário, o Kaspersky Security Center Web Console não será capaz de se conectar ao Servidor de Administração.

Para especificar um novo certificado para o Servidor de Administração:

1. No dispositivo onde o Servidor de Administração estiver instalado, copie o arquivo do certificado, por exemplo, para um dispositivo de armazenamento em massa.

   Por padrão, o arquivo de certificado é armazenado na seguinte pasta:

   - Para Windows – %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert
   - Para Linux – /var/opt/kaspersky/klnagent_srv/1093/cert/

2. No dispositivo onde o Kaspersky Security Center Web Console está instalado, coloque o arquivo do certificado em uma pasta local.

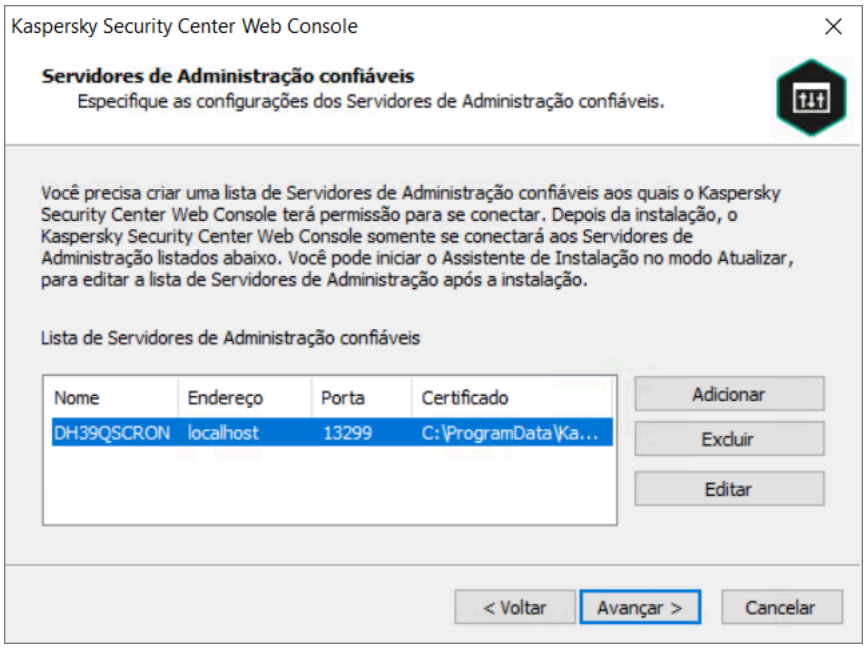
3. Execute o arquivo de instalação ksc-web-console-<número da versão>.<número da compilação>.exe em uma conta com privilégios administrativos.

   Isso inicia o Assistente de instalação.

4. Na primeira página do assistente, selecione a opção **Efetuar upgrade**.

   Siga as instruções do Assistente.

5. Na página **Servidores de Administração confiáveis** do assistente, selecione o Servidor de Administração necessário e clique no botão **Editar**.



Especificar os Servidores de Administração confiáveis

6. Na janela **Editar Servidor de Administração** que se abre, clique no botão **Procurar**, especifique o caminho para o novo arquivo de certificado e clique no botão **Atualizar** para aplicar as alterações.

7. Na página **Pronto para modificar o Kaspersky Security Center Web Console** no assistente, clique no botão **Efetuar upgrade** para iniciar o upgrade.

8. Após a conclusão com êxito da reconfiguração do aplicativo, clique no botão **Concluir**.

9. Login no Kaspersky Security Center Web Console.

O Kaspersky Security Center Web Console funciona com o certificado especificado.

Converter um certificado PFX para o formato PEM

Para usar um certificado PFX no Kaspersky Security Center Web Console, você deve primeiro convertê-lo para o formato PEM usando qualquer utilitário multiplataforma baseado em OpenSSL conveniente.

Para converter um certificado PFX para o formato PEM no sistema operacional Windows:

1. Em um utilitário multiplataforma baseado em OpenSSL, execute os seguintes comandos:

   ```
   openssl pkcs12 -in <nome do arquivo.pfx> -clcerts -nokeys -out server.crt
   openssl pkcs12 -in <nome do arquivo.pfx> -nocerts -nodes -out key.pem
   ```

   Como resultado, você obtém uma chave pública como um arquivo .crt e uma chave privada como um arquivo .pem protegido por senha.

2. Certifique-se de que os arquivos .crt e .pem sejam gerados na mesma pasta onde o arquivo .pfx está armazenado.

3. Se o arquivo .crt ou .pem contiver os "Atributos Bag", exclua esses atributos usando qualquer editor de texto conveniente e salve o arquivo.

4. Reinicie o serviço do Windows.

5. O Kaspersky Security Center Web Console não oferece suporte a certificados protegidos por senha. Portanto, execute o seguinte comando em um utilitário multiplataforma baseado em OpenSSL para remover uma senha do arquivo .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Não use o mesmo nome para os arquivos .pem de entrada e saída.

   Como resultado, o novo arquivo .pem não é criptografado. Você não precisa inserir uma senha para usá-lo.

Os arquivos .crt e .pem estão prontos para uso, então você pode especificá-los no instalador do Kaspersky Security Center Web Console.

Para converter um certificado PFX para o formato PEM no sistema operacional Linux:

1. Em um utilitário multiplataforma baseado em OpenSSL, execute os seguintes comandos:

   ```
   openssl pkcs12 -in <nome do arquivo.pfx> -clcerts -nokeys | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.crt
   ```

   ```
   openssl pkcs12 -in <nome do arquivo.pfx> -nocerts -nodes | sed -ne '/-BEGIN PRIVATE KEY-/,/-END PRIVATE KEY-/p' > key.pem
   ```

2. Certifique-se de que o arquivo de certificado e a chave privada sejam gerados no mesmo diretório onde o arquivo .pfx está armazenado.

3. O Kaspersky Security Center Web Console não oferece suporte a certificados protegidos por senha. Portanto, execute o seguinte comando em um utilitário multiplataforma baseado em OpenSSL para remover uma senha do arquivo .pem:

   ```
   openssl rsa -in key.pem -out key-without-passphrase.pem
   ```

   > Não use o mesmo nome para os arquivos .pem de entrada e saída.

   Como resultado, o novo arquivo .pem não é criptografado. Você não precisa inserir uma senha para usá-lo.

Os arquivos .crt e .pem estão prontos para uso, então você pode especificá-los no instalador do Kaspersky Security Center Web Console.

Migração do Kaspersky Security Center Windows

Esta seção descreve a migração de dispositivos gerenciados e objetos relacionados (políticas, tarefas, grupos, tags e outros objetos) do Kaspersky Security Center Windows para:

- Kaspersky Security Center Cloud Console
- Kaspersky Security Center Linux
- Kaspersky Next XDR Expert

Migração para o Kaspersky Security Center Cloud Console

É possível migrar manualmente do Kaspersky Security Center Web Console para o Kaspersky Security Center Cloud Console. Depois disso, o acesso ao Servidor de Administração e ao sistema de gerenciamento de banco de dados (DBMS), hospedados na infraestrutura da Kaspersky, é obtido. Não é necessário um servidor físico ou um DBMS – ambos são mantidos por especialistas da Kaspersky.

É possível migrar os dispositivos gerenciados que executam um sistema operacional Windows, Linux ou macOS sob o controle do Kaspersky Security Center Cloud Console. Caso a rede inclua uma hierarquia de Servidores de Administração, será possível salvá-la no Kaspersky Security Center Cloud Console. Além disso, é possível transferir:

- Tarefas e políticas de aplicativos gerenciados
- Tarefas globais
- Seleções de dispositivos personalizados
- Estrutura do grupo de administração e dispositivos incluídos
- Tags atribuídas aos dispositivos a serem migrados

Depois de concluir a migração, é possível gerenciar os dispositivos usando o Kaspersky Security Center Cloud Console. Ao mesmo tempo, os objetos transferidos são preservados e o agente de rede é reinstalado em todos os dispositivos gerenciados.

Para obter informações sobre como realizar a migração e uma lista dos pré-requisitos, consulte a *Ajuda do Kaspersky Security Center Cloud Console*.

Migração para o Kaspersky Next XDR Expert

Seguindo este cenário, é possível transferir a estrutura do grupo de administração, inclusive os dispositivos gerenciados e outros objetos de grupo (políticas, tarefas, tarefas globais, tags e seleções de dispositivos) do Kaspersky Security Center Windows sob o gerenciamento do Kaspersky Next XDR Expert.

Limitações:

- A migração só é possível do Kaspersky Security Center 14.2 Windows para o Kaspersky Next XDR Expert a partir da versão 1.0.
- Só é possível executar este cenário com o uso do Kaspersky Security Center Web Console.

Fases

O cenário de migração continua em estágios:

1. **Escolha um método de migração**

   É possível migrar para o Kaspersky Next XDR Expert pelo assistente de migração. As etapas do assistente de migração dependem de os Servidores de Administração do Kaspersky Security Center Windows e do Kaspersky Next XDR Expert estarem organizados em uma hierarquia:

   - Migração com o uso de uma hierarquia de Servidores de Administração

     Escolha esta opção se o Servidor de Administração do Kaspersky Security Center Windows atuar como secundário para o Servidor de Administração do Kaspersky Next XDR Expert. Você gerencia o processo de migração e alterna entre Servidores no Console OSMP. Caso prefira esta opção, é possível organizar os Servidores de Administração em uma hierarquia para simplificar o procedimento de migração. Para fazer isso, crie a hierarquia antes de iniciar a migração.

   - Migração com o uso de um arquivo de exportação (arquivo ZIP)

     Escolha esta opção caso os Servidores de Administração do Kaspersky Security Center Windows e do Kaspersky Next XDR Expert não estejam organizados em uma hierarquia. Você gerencia o processo de migração com dois Consoles: uma instância do Kaspersky Security Center Windows e o Console OSMP. Nesse caso, será necessário usar o arquivo de exportação criado e baixado durante a exportação do Kaspersky Security Center Windows e esse arquivo deverá ser importado para o Kaspersky Next XDR Expert.

2. **Exporte os dados do Kaspersky Security Center Windows**

   Abra o Kaspersky Security Center Windows e execute o Assistente de migração.

3. **Importar dados para o Kaspersky Next XDR Expert**

   Continue com o Assistente de migração para importar os dados exportados para o Kaspersky Next XDR Expert.

   Caso os Servidores estejam organizados em uma hierarquia, a importação será iniciada automaticamente após uma exportação bem-sucedida dentro do mesmo assistente. Caso os Servidores não estejam organizados em uma hierarquia, o assistente de migração continuará depois de alternar para o Kaspersky Next XDR Expert.

4. **Execute as ações adicionais para transferir manualmente objetos e configurações do Kaspersky Security Center Windows para o Kaspersky Next XDR Expert (etapa opcional)**

   O usuário também poderá desejar transferir os objetos e configurações que não podem ser transferidos pelo assistente de migração. Por exemplo, também é possível fazer o seguinte:

   - Configurar as tarefas globais do Servidor de Administração
   - Definir as configurações de política do Agente de Rede
   - Criar pacotes de instalação de aplicativos
   - Criar Servidores virtuais
   - Atribuir e configurar pontos de distribuição

- Configurar regras para mover dispositivos
- Configurar as regras para identificar dispositivos automaticamente
- Criar categorias de aplicativos

5. **Mova os dispositivos gerenciados importados sob gerenciamento do Kaspersky Next XDR Expert**

   Para concluir a migração, mova os dispositivos gerenciados e importados sob gerenciamento do Kaspersky Next XDR Expert. É possível fazer isso usando um dos seguintes métodos:

   - Por meio da tarefa de grupo do Kaspersky Security Center

     Use a tarefa Alterar Servidor de Administração para alterar o Servidor de Administração de dispositivos clientes específicos.

   - No utilitário klmover

     Use o utilitário klmover e especifique as configurações de conexão para o novo Servidor de Administração.

   - Na instalação ou reinstalação do Agente de Rede nos dispositivos gerenciados

     Crie um novo pacote de instalação do Agente de Rede e especifique as configurações de conexão para o novo Servidor de Administração nas propriedades do pacote de instalação. Use o pacote de instalação para instalar o Agente de Rede nos dispositivos gerenciados importados por uma tarefa de instalação remota.

     Também é possível criar e usar um pacote de instalação independente para instalar localmente o Agente de Rede.

6. **Atualize o Agente de Rede para a versão mais recente**

   Recomendamos atualizar o Agente de Rede para a mesma versão do Console OSMP.

7. **Verifique e confirme se os dispositivos gerenciados estão visíveis no novo Servidor de Administração**

   No Servidor de Administração do Kaspersky Next XDR Expert, abra a lista de dispositivos gerenciados (**Dispositivos** → **Dispositivos gerenciados**s) e verifique os valores nas colunas **Visível**, **Agente de Rede instalado** e as colunas **Última conexão com o Servidor de Administração**.

Outros métodos de migração de dados

Além do assistente de migração, também é possível transferir as tarefas e políticas específicas:

- Exporte as tarefas do Kaspersky Security Center Windows e, em seguida, importe as tarefas para o Kaspersky Next XDR Expert.
- Exporte as políticas do Kaspersky Security Center Windows e, em seguida, importe as políticas para o Kaspersky Next XDR Expert. Os perfis de política relacionados são exportados e importados juntamente com as políticas selecionadas.

Migração para o Kaspersky Security Center Linux

A migração do Kaspersky Security Center Windows para o Kaspersky Security Center Linux pode ser feita por meio do backup de dados do Servidor de Administração (com o utilitário klbackup) e o Assistente de migração.

A tabela abaixo permite a comparação dos recursos e limitações principais da migração realizada pelo backup de dados do Servidor de Administração e Assistente de Migração. Assim, é possível decidir qual é a melhor abordagem para a sua organização.

Comparação das abordagens de migração

Parâmetros	Backup de dados do Servidor de Administração	Assistente de migração
Processo de migração	Criação de um backup completo dos dados do Servidor de Administração do Kaspersky Security Center Windows e realização de restauração de dados em um Servidor de Administração do Kaspersky Security Center Linux	Seleção e exportação de dados do Servidor de Administração para migração, importação desses dados para o Servidor de Administração do Kaspersky Security Center Linux e mudança de dispositivos gerenciados sob o gerenciamento do Kaspersky Security Center Linux
Recursos do método de migração	• Migração de todos os dados do Servidor de Administração • Migração de qualquer quantidade de dispositivos gerenciados • Usado para obter uma cópia completa dos dados do Servidor de Administração do Kaspersky Security Center Windows e transferi-los para o Servidor de Administração do Kaspersky Security Center Linux	• Migração parcial dos dados do Servidor de Administração • A seleção de objetos para migração está disponível • O grupo ou subgrupo de administração a ser migrado não pode conter mais de 10 mil dispositivos • Usado para transferir parcialmente os dados do Servidor de Administração, incluindo apenas os objetos de grupo dentro do escopo de migração; objetos de grupo fora do escopo de migração devem ser restaurados manualmente
Escopo da migração	Transferência completa dos dados do Servidor de Administração com número ilimitado de dispositivos gerenciados	• Estrutura do grupo de administração • Dispositivos gerenciados incluídos em grupos de administração (**até 10 mil dispositivos**) • Tags atribuídas a dispositivos em migração • Tarefas globais do Agente de Rede e aplicativos gerenciados (não para o Servidor de Administração) • Tarefas de grupo do Agente de Rede e de aplicativos gerenciados • Políticas de aplicativos gerenciados • Modelos de relatório • Funções de usuário • Usuários internos e grupos de segurança • Categorias personalizadas de aplicativos com conteúdo adicionado manualmente • Seleções de dispositivos personalizados
Escopo não migrado	—	• Tarefas globais do Servidor de Administração • Eventos salvos no Servidor de Administração • Repositório dos pacotes de distribuição de aplicativos para instalação remota • Certificado do Servidor de Administração • Chaves de licença usadas pelo Servidor de Administração e aplicativos gerenciados • Servidores de Administração virtual • Configurações de política do Agente de Rede • Regras de migração de dispositivos • Regras para identificar dispositivos automaticamente • Pontos de distribuição • Configurações do aplicativo da Kaspersky salvas no Servidor de Administração

Versões do Kaspersky Security Center que são compatíveis com a migração	• Qualquer versão compatível do Kaspersky Security Center Windows • Kaspersky Security Center Linux versão 15.2 ou posterior	• Kaspersky Security Center Windows versão 14.2 ou posterior • Kaspersky Security Center Linux versão 15 ou posterior
DBMSs entre os quais a migração pode ser realizada	• Microsoft SQL Server → MySQL, MariaDB • Microsoft SQL Server → PostgreSQL, Postgres Pro (apenas para migração do Kaspersky Security Center Windows versão 14.2 ou posterior com o patch instalado para Kaspersky Security Center Linux versão 15.3 ou posterior) • MySQL → MySQL, MariaDB • MariaDB → MySQL, MariaDB	Migração entre DBMSs compatíveis e sem limitações

Migração para o Kaspersky Security Center Linux pelo Assistente de migração

Seguindo este cenário, é possível transferir a estrutura do grupo de administração, inclusive os dispositivos gerenciados e outros objetos de grupo (políticas, tarefas, tarefas globais, tags e seleções de dispositivos) do Kaspersky Security Center Windows sob o gerenciamento do Kaspersky Security Center Linux. Antes da migração, verifique e confirme se os recursos necessários do Kaspersky Security Center Windows são compatíveis com o Kaspersky Security Center Linux.

Limitações:

- A migração só é possível do Kaspersky Security Center Windows versão 14.2 ou posterior para o Kaspersky Security Center Linux versão 15 ou posterior.
- Só é possível executar este cenário com o uso do Kaspersky Security Center Web Console.

Fases

O cenário de migração continua em estágios:

1. **Escolha um método de migração**

   É possível migrar para o Kaspersky Security Center Linux pelo assistente de migração. As etapas do assistente de migração dependem de os Servidores de Administração do Kaspersky Security Center Windows e do Kaspersky Security Center Linux estarem organizados em uma hierarquia:

   - Migração com o uso de uma hierarquia de Servidores de Administração

     Escolha esta opção se o Servidor de Administração do Kaspersky Security Center Windows atuar como secundário para o Servidor de Administração do Kaspersky Security Center Linux. O processo de migração também é gerenciado e alterna entre servidores em uma única instância do Kaspersky Security Center Web Console. Caso prefira esta opção, é possível organizar os Servidores de Administração em uma hierarquia para simplificar o procedimento de migração. Para fazer isso, crie a hierarquia antes de iniciar a migração.

   - Migração com o uso de um arquivo de exportação (arquivo ZIP)

     Escolha esta opção caso os Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux não estejam organizados em uma hierarquia. O processo de migração é gerenciado com duas instâncias do Kaspersky Security Center Web Console, uma instância para o Kaspersky Security Center Windows e outra para o Kaspersky Security Center Linux. Nesse caso, será necessário usar o arquivo de exportação criado e baixado durante a exportação do Kaspersky Security Center Windows e esse arquivo deverá ser importado para o Kaspersky Security Center Linux.

2. **Faça backup do certificado e da chave privada do Servidor de Administração do Kaspersky Security Center Windows (etapa opcional)**

   É possível colocar os dispositivos gerenciados sob o gerenciamento do Servidor de Administração do Kaspersky Security Center Linux ao restaurar o certificado e a chave privada do Servidor de Administração por meio de uma cópia backup. Nesse caso, faça backup do certificado e da chave privada do Servidor de Administração do Kaspersky Security Center Windows. Em seguida, no estágio 6, restaure o certificado e a chave privada.

3. **Exporte os dados do Kaspersky Security Center Windows**

   Abra o Kaspersky Security Center Windows e execute o Assistente de migração.

4. **Importe os dados do Kaspersky Security Center Linux**

   Continue o assistente de migração para importar os dados exportados para o Kaspersky Security Center Linux. Caso os Servidores estejam organizados em uma hierarquia, a importação será iniciada automaticamente após uma exportação bem-sucedida dentro do mesmo assistente. Caso os Servidores não estejam organizados em uma hierarquia, o assistente de migração continua depois de alternar para o Kaspersky Security Center Linux.

5. **Execute as ações adicionais para transferir manualmente objetos e configurações do Kaspersky Security Center Windows para o Kaspersky Security Center Linux (etapa opcional)**

   O usuário também poderá desejar transferir os objetos e configurações que não podem ser transferidos pelo assistente de migração. Por exemplo, também é possível fazer o seguinte:

   - Transferir as chaves de licença usadas pelo Servidor de Administração e aplicativos gerenciados
   - Configurar as tarefas globais do Servidor de Administração
   - Definir as configurações de política do Agente de Rede
   - Criar pacotes de instalação de aplicativos
   - Criar Servidores virtuais
   - Atribuir e configurar pontos de distribuição
   - Configurar regras para mover dispositivos
   - Configurar as regras para identificar dispositivos automaticamente
   - Criar categorias de aplicativos

6. **Mover os dispositivos gerenciados importados sob gerenciamento do Kaspersky Security Center Linux**

   Para concluir a migração e mover os dispositivos gerenciados e importados sob gerenciamento do Kaspersky Security Center Linux. É possível fazer isso usando um dos seguintes métodos:

   - No utilitário klmover

     Use o utilitário klmover e especifique as configurações de conexão para o novo Servidor de Administração.

   - Pela tarefa *Alterar o Servidor de Administração*

     Crie uma tarefa *Alterar o Servidor de Administração*, especifique os dispositivos gerenciados importados, o novo Servidor de Administração e outras configurações da tarefa. Em seguida, execute a tarefa para colocar os dispositivos gerenciados sob o gerenciamento do Servidor de Administração do Kaspersky Security Center Linux.

   - Pela remoção (se já instalado) e posterior instalação do Agente de Rede nos dispositivos gerenciados

Crie um novo pacote de instalação do Agente de Rede e especifique as configurações de conexão para o novo Servidor de Administração nas propriedades do pacote de instalação. Remova o Agente de Rede nos dispositivos gerenciados importados e, em seguida, use o pacote de instalação para instalar o Agente de Rede nos dispositivos gerenciados importados por meio de uma tarefa de instalação remota. Também é possível criar e usar um pacote de instalação independente para instalar localmente o Agente de Rede. Para obter mais informações, consulte Alternando de dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux.

- Por meio da restauração do certificado e da chave privada do Servidor de Administração de uma cópia backup (apenas para migração para o Kaspersky Security Center Linux 15.1 ou posterior)

  Atribua ao dispositivo com o Servidor de Administração do Kaspersky Security Center Linux o mesmo endereço de rede que o Servidor de Administração do Kaspersky Security Center Windows. Para restaurar o certificado do Servidor de Administração e a chave privada da cópia backup salva no estágio 2, execute o utilitário klbackup com o parâmetro `-cert_only`. Na linha de comando, execute o seguinte comando: `/opt/kaspersky/ksc64/sbin/klbackup -path <caminho para a cópia de backup do certificado do Servidor de Administração> -restore -cert_only`. Para obter mais informações, consulte Uso do utilitário klbackup para mudar os dispositivos gerenciados sob gerenciamento de outro Servidor de Administração.

7. **Atualize o Agente de Rede para a versão mais recente**

   Recomendamos atualizar o Agente de Rede para Linux para a mesma versão do Kaspersky Security Center.

8. **Verifique e confirme se os dispositivos gerenciados estão visíveis no novo Servidor de Administração**

   No Servidor de Administração Kaspersky Security Center Linux, abra a lista de dispositivos gerenciados (**Dispositivos** → **Dispositivos gerenciados**) e verifique os valores nas colunas **Visível**, **Agente de Rede instalado** e as colunas **Última conexão com o Servidor de Administração**.

Outros métodos de migração de dados

Além do assistente de migração, também é possível transferir as tarefas e políticas específicas:

- Exporte as tarefas do Kaspersky Security Center Windows e, em seguida, importe as tarefas para o Kaspersky Security Center Linux.
- Exporte as políticas específicas do Kaspersky Security Center Windows e, em seguida, importe as políticas no Kaspersky Security Center Linux. Os perfis de política relacionados são exportados e importados juntamente com as políticas selecionadas.

Exportação de objetos de grupo a partir do Kaspersky Security Center Windows

A migração da estrutura do grupo de administração, incluindo os dispositivos gerenciados e outros objetos de grupo, do Kaspersky Security Center Windows para o Kaspersky Security Center Linux requer, primeiramente, a seleção dos dados para exportação e criação de um arquivo de exportação. O arquivo de exportação contém informações sobre todos os objetos de grupo que deseja migrar. O arquivo de exportação será usado para a importação subsequente para o Kaspersky Security Center Linux.

É possível exportar os seguintes objetos:

- Tarefas e políticas de aplicativos gerenciados
- Tarefas globais
- Seleções de dispositivos personalizados

- Estrutura do grupo de administração e dispositivos incluídos
- Tags atribuídas aos dispositivos a serem migrados

Antes de iniciar a exportação, leia as informações gerais sobre a migração para o Kaspersky Security Center Linux. Escolha o método de migração com ou sem a hierarquia de Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux.

Para exportar os dispositivos gerenciados e objetos de grupo relacionados por meio do assistente de migração:

1. Dependendo se os Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux estiverem ou não organizados em uma hierarquia, siga um destes procedimentos:
   - Caso os servidores estejam organizados em uma hierarquia, abra o Kaspersky Security Center Web Console e alterne para o servidor do Kaspersky Security Center Windows.
   - Caso os servidores não estejam organizados em uma hierarquia, abra o Kaspersky Security Center Web Console conectado ao Kaspersky Security Center Windows.
2. No menu principal, vá para **Operações** → **Migração**.
3. Para iniciar o assistente e seguir suas etapas, selecione para onde deseja transferir seus dados e configurações.
   - Se quiser transferir seus dados e configurações para o Kaspersky Security Center Cloud Console, selecione **Migração para o Kaspersky Security Center Cloud Console**.
   - Se você quiser transferir seus dados e configurações para o Kaspersky Security Center Linux ou Kaspersky Next XDR Expert, selecione **Migrar para o Kaspersky Security Center Linux**.
4. Selecione o grupo de administração ou o subgrupo para exportar. Certifique-se de que o grupo ou o subgrupo de administração selecionado não contenha mais de 10.000 dispositivos.
5. Selecione os aplicativos gerenciados cujas tarefas e políticas serão exportadas. Selecione apenas os aplicativos compatíveis com o Kaspersky Security Center Linux. Os objetos de aplicativos incompatíveis ainda serão exportados, mas não poderão ser operados.
6. Use os links à esquerda para selecionar as tarefas globais, as seleções de dispositivos e os relatórios a serem exportados. O link **Objetos do grupo** permite excluir da exportação funções personalizadas, usuários internos e grupos de segurança, bem como categorias de aplicativos personalizadas.

O arquivo de exportação (arquivo ZIP) é criado. Dependendo se a execução da migração é feita com suporte à hierarquia do Servidor de Administração ou não, o arquivo de exportação é salvo da seguinte forma:

- Caso os Servidores estejam organizados em uma hierarquia, o arquivo de exportação será salvo na pasta temporária no Kaspersky Security Center Web Console Server.
- Caso os Servidores não estejam organizados em uma hierarquia, o arquivo de exportação será baixado para o seu dispositivo.

Para migração com suporte à hierarquia do Servidor de Administração, a importação começa automaticamente após uma exportação bem-sucedida. Para migração sem suporte à hierarquia do Servidor de Administração, é possível importar manualmente o arquivo de exportação salvo para o Kaspersky Security Center Linux.

Importação do arquivo de exportação no Kaspersky Security Center Linux

Para transferir informações sobre dispositivos gerenciados, objetos e suas configurações exportadas do Kaspersky Security Center Windows, é necessário importá-las para o para o Kaspersky Security Center Linux ou Kaspersky Next XDR Expert.

Para importar os dispositivos gerenciados e objetos de grupo relacionados usando o assistente de migração:

1. Dependendo se os Servidores de Administração do Kaspersky Security Center Windows e Kaspersky Security Center Linux estiverem ou não organizados em uma hierarquia, siga um destes procedimentos:

   - Caso os Servidores estejam organizados em uma hierarquia, prossiga para a próxima etapa do assistente de migração após a conclusão da exportação. A importação é iniciada automaticamente após uma exportação bem-sucedida dentro deste assistente (consulte a etapa 2 desta instrução).

   - Caso os Servidores não estejam organizados em uma hierarquia:

     a. Abra o Kaspersky Security Center Web Console conectado com o Kaspersky Security Center Linux ou Kaspersky Next XDR Expert.

     b. No menu principal, vá para **Operações** → **Migração**.

     c. Selecione o arquivo de exportação (arquivo ZIP) criado e baixado durante a exportação do Kaspersky Security Center Windows. O upload do arquivo de exportação é iniciado.

2. Depois que o arquivo de exportação for carregado com êxito, será possível continuar a importação. Caso queira especificar outro arquivo de exportação, clique no link **Alterar** e selecione o arquivo desejado.

3. A hierarquia inteira de grupos de administração do Kaspersky Security Center Linux é exibida.

   Marque a caixa de seleção ao lado do grupo de administração de destino para o qual os objetos do grupo de administração exportado (dispositivos gerenciados, políticas, tarefas e outros objetos de grupo) devem ser restaurados.

4. A importação de objetos do grupo é iniciada. Não é possível minimizar o assistente de Migração nem executar nenhuma operação simultânea durante a importação. Aguarde até que os ícones de atualização (🔄) ao lado de todos os itens na lista de objetos sejam substituídos por marcas de seleção verdes (✓) e a importação será concluída.

5. Quando a importação for concluída, a estrutura exportada dos grupos de administração, inclusive os detalhes dos dispositivos, aparecerá no grupo de administração de destino selecionado. Se o nome do objeto restaurado for idêntico ao nome de um objeto existente, será adicionado ao objeto restaurado um sufixo incremental.

> Se em uma tarefa migrada os detalhes da conta sob a qual a tarefa é executada forem especificados, será necessário abrir a tarefa e inserir a senha novamente após a conclusão da importação.

Caso a importação tenha sido concluída com um erro, será possível executar uma das seguintes ações:

- Para a migração com suporte à hierarquia do Servidor de Administração, é possível começar a importar o arquivo de exportação novamente.
- Para a migração sem suporte à hierarquia do Servidor de Administração, é possível iniciar o assistente de migração para selecionar outro arquivo de exportação e importá-lo novamente.

É possível verificar se os objetos do grupo incluídos no escopo da exportação foram importados com êxito para o Kaspersky Security Center Linux. Para fazer isso, vá para a seção **Dispositivos**, verifique e confirme se os objetos importados aparecem nas subseções correspondentes.

Observe que os dispositivos gerenciados importados são exibidos na subseção **Dispositivos gerenciados**, mas eles são invisíveis na rede e o Agente de Rede não está instalado e em execução neles (o valor *No* nas colunas **Visível**, **Agente de Rede instalado** e **Agente de Rede em execução**).

Para concluir a migração, é preciso mudar os dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux.

Alternância entre dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux

Após uma importação bem-sucedida das informações sobre os dispositivos gerenciados, objetos e suas configurações para o Kaspersky Security Center Linux, é preciso mudar os dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux para concluir a migração.

É possível migrar os dispositivos gerenciados para o Kaspersky Security Center Linux com o uso de um dos seguintes métodos:

- Uso do utilitário klmover.
- Com o uso da tarefa *Alterar o Servidor de Administração*.
- Instalação do Agente de Rede nos dispositivos gerenciados por meio de uma tarefa de instalação remota.

Para mudar os dispositivos gerenciados para serem gerenciados pelo Kaspersky Security Center Linux pela instalação do Agente de Rede:

1. Remova o Agente de Rede nos dispositivos gerenciados importados que serão alternados sob o gerenciamento do Kaspersky Security Center Linux.
2. Mude para o Servidor de Administração do Kaspersky Security Center Windows.
3. Vá para **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação** e abra as propriedades de um pacote de instalação existente do Agente de Rede.

   Caso o pacote de instalação do Agente de Rede esteja ausente na lista de pacotes, baixe um novo.

   Também é possível criar e usar um pacote de instalação independente para instalar localmente o Agente de Rede.
4. Na guia **Configurações**, selecione a seção **Conexão**. Especifique as configurações de conexão do Servidor de Administração do Kaspersky Security Center Linux.

5. Crie uma tarefa de instalação remota para os dispositivos gerenciados e importados, e especifique o pacote de instalação do Agente de Rede reconfigurado.

   É possível instalar o Agente de Rede por meio do Servidor de Administração do Kaspersky Security Center Windows ou por meio de um dispositivo baseado no Windows que atue como um ponto de distribuição. Caso use o Servidor de Administração, ative a opção **Usando recursos do sistema operacional através do Servidor de Administração**. Caso use um ponto de distribuição, ative a opção **Usando recursos do sistema operacional através de pontos de distribuição**.

6. Executar a tarefa de instalação remota.

Depois que a tarefa de instalação remota for concluída com êxito, vá para o Servidor de Administração do Kaspersky Security Center Linux, verifique e confirme se os dispositivos gerenciados estão visíveis na rede e se o Agente de Rede está instalado e sendo executado neles (o valor *Yes* nas colunas **Visível**, **Agente de Rede instalado** e **Agente de Rede em execução**).

Migração para o Kaspersky Security Center Linux com o uso do backup de dados do Servidor de Administração

Você pode usar um backup de dados para migrar os dados do Servidor de Administração do Kaspersky Security Center no Windows para o Kaspersky Security Center no Linux. Antes da migração, verifique e confirme se os recursos necessários do Kaspersky Security Center Windows são compatíveis com o Kaspersky Security Center Linux.

Limitações:

- Os DBMSs abaixo podem realizar a migração:
  - Microsoft SQL Server → MySQL, MariaDB
  - Microsoft SQL Server → PostgreSQL, Postgres Pro
  - MySQL → MySQL, MariaDB
  - MariaDB → MySQL, MariaDB
- A migração dos dados do Servidor de Administração armazenados nos bancos de dados Microsoft SQL Server, MySQL ou MariaDB para MySQL ou MariaDB é compatível para migração de qualquer versão compatível do Kaspersky Security Center Windows para o Kaspersky Security Center Linux versão 15.2 ou posterior.

- A migração de dados do Servidor de Administração armazenados no banco de dados Microsoft SQL para o PostgreSQL ou Postgres Pro é compatível com a migração do Kaspersky Security Center Windows (versão 14.2 ou posterior) para o Kaspersky Security Center Linux (versão 15.3 ou posterior).

  Para ser compatível com a migração para o PostgreSQL ou Postgres Pro, você precisa instalar o patch do Servidor de Administração do Kaspersky Security Center Windows. Execute um dos seguintes patches:

  - Para o Kaspersky Secure Mobility Management baseado no Kaspersky Security Center Windows 14.2: 14.2.0.48079-pf5
  - Para o Kaspersky Security Center Windows 14.2: 14.2.0.26967-pf5

  Entre em contato com o Suporte Técnico da Kaspersky para obter o patch necessário.

- Caso queira usar o MySQL ou o MariaDB como um DBMS para o Kaspersky Security Center Windows e para o Kaspersky Security Center Linux, o parâmetro `lower_case_table_names` deve corresponder ao DBMS atual e ao novo.

  Antes de criar um backup de dados, verifique o parâmetro `lower_case_table_names`. Em seguida, ao instalar o MySQL ou o MariaDB para o Kaspersky Security Center Linux, é necessário definir esse parâmetro com o mesmo valor especificado para o parâmetro no Windows.

Fases

A migração utilizando o backup de dados do Servidor de Administração prossegue em etapas:

1. **Verificação de que você possui a conta de usuário interna do administrador com a qual é possível fazer login no Servidor de Administração**

   A conta do administrador será usada para fazer login no Servidor de Administração do Kaspersky Security Center Linux. Se você não tiver essa conta e estiver conectado apenas com uma conta local do Windows ou uma conta de domínio, não será possível realizar o login no Servidor de Administração do Kaspersky Security Center Linux após a restauração do backup. O Servidor de Administração do Kaspersky Security Center Linux não oferece suporte ao login com uma conta local do Windows. É possível fazer login com uma conta de domínio, mas isso pode exigir configuração adicional do Servidor de Administração.

   Se você não tiver a conta do administrador, será necessário criá-la após a restauração da cópia de backup, usando o utilitário kladduser.

2. **Criação de uma cópia backup atualizada dos dados do Servidor de Administração do Kaspersky Security Center Windows**

   Realize uma das seguintes ações considerando o tipo de DBMS usado pelo Kaspersky Security Center Windows ou Kaspersky Security Center Linux:

   - Para a migrar do MySQL ou MariaDB para MySQL ou MariaDB: crie uma cópia backup com o utilitário klbackup ou com uma tarefa de backup de dados no dispositivo que tenha o Servidor de Administração instalado.
   - Para migração do Microsoft SQL Server para MySQL ou MariaDB: crie uma cópia backup com o utilitário klbackup com a opção **Migrar para o formato MySQL/MariaDB** ativada.
   - Para migração do Microsoft SQL Server para o PostgreSQL ou Postgres Pro:

     1. Instale o patch do Servidor de Administração para compatibilidade com a migração para PostgreSQL e Postgres Pro. Entre em contato com o Suporte Técnico da Kaspersky para obter esse patch.

     1. Crie uma cópia backup usando o utilitário klbackup.

        Se você executar o klbackup na linha de comando, use o sinalizador `-migrate postgres`.

Se você usar a interface klbackup, ative a opção **Migrar para o formato Postgres**.

Após criar a cópia backup, desconecte o Servidor de Administração do Kaspersky Security Center Windows da rede.

3 Preparação de um dispositivo novo para instalação do Kaspersky Security Center Linux

Nesta etapa do cenário, faça o seguinte:

1. Selecione um novo dispositivo no qual instalar o Servidor de Administração. Este dispositivo deve atender aos requisitos de hardware e software. Verifique também se as portas usadas no Servidor de Administração estão disponíveis.

2. Atribua o mesmo endereço ao novo dispositivo.

   O novo Servidor de Administração pode ser atribuído ao nome NetBIOS, FQDN e endereço IP estático. Isso depende de qual endereço do Servidor de Administração foi definido no pacote de instalação do Agente de Rede quando os Agentes de Rede foram implementados. Como alternativa, é possível usar o endereço de conexão que determina o Servidor de Administração ao qual o Agente de Rede se conecta (esse endereço pode ser obtido em dispositivos gerenciados usando o utilitário klnagchk).

4 Instalação e configuração do DBMS

Nesta etapa do cenário, faça o seguinte:

1. Selecione o tipo de DBMS que fornece desempenho ideal. Leve em consideração o número de dispositivos, a topologia e a carga de trabalho de rede. Você pode selecionar um dos DBMSs compatíveis.

2. Instale o DBMS de acordo com o tipo de DBMS selecionado ao criar um backup. Para obter informações sobre como instalar o DBMS selecionado, consulte a sua documentação.

   > Uma nova versão do banco de dados não deve ser inferior à atual.

3. Configure o DBMS para uso com o Kaspersky Security Center Linux.

5 Instalação do Kaspersky Security Center Linux

Instale o Kaspersky Security Center Linux no novo dispositivo.

A conta de usuário interna do administrador criada durante a instalação, assim como outros objetos (grupos, políticas, tarefas, usuários) criados antes da restauração dos dados do Servidor de Administração do backup, serão perdidos após a restauração. Esses objetos serão substituídos pelos objetos contidos no backup.

6 Restauração dos dados do Servidor de Administração da cópia de backup

Nesta etapa do cenário, faça o seguinte:

1. Restaure os dados do Servidor de Administração no novo dispositivo usando o utilitário klbackup.

2. Se você não tiver a conta de usuário interna do administrador com a qual estava conectado ao Servidor de Administração do Kaspersky Security Center para Windows, e estiver usando uma conta local do Windows ou uma conta de domínio, crie uma conta de administrador usando o utilitário kladduser, da seguinte forma:

   ```
   /opt/kaspersky/ksc64/sbin/kladduser -n ksc -p <password>
   ```

   em que o parâmetro `<senha>` atende aos seguintes requisitos:

   - A senha de usuário não pode ter menos de 8 nem mais de 256 caracteres.
   - A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:

- Letras maiúsculas (A-Z)
- Letras minúsculas (a-z)
- Números (0-9)
- Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)

7. **Instalação do Kaspersky Security Center Web Console e configuração do Servidor de Administração**

   Nesta etapa do cenário, faça o seguinte:

   1. Instale o Kaspersky Security Center Web Console.

      Caso o Kaspersky Security Center Web Console tenha sido instalado anteriormente, basta reinstalá-lo com o mesmo arquivo de resposta.

      Faça login no Kaspersky Security Center Web Console com a conta de usuário interna do administrador.

      O processo de inicialização de dados geralmente leva até 15 minutos após a restauração de dados do Servidor de Administração, mas o tempo depende do desempenho do hardware e do tamanho de dados do Servidor de Administração. Durante esse período, o Kaspersky Security Center Web Console talvez não consiga se conectar e exibir os erros.

   2. Verifique a funcionalidade dos principais recursos do Servidor de Administração quando a inicialização dos dados no banco de dados estiver concluída. Verifique se o Servidor de Administração está sincronizado com os dispositivos gerenciados e se os dados do Servidor de Administração estão recuperados.

   3. Sonde controladores de domínio para restaurar as informações sobre a estrutura do domínio, contas de usuário, grupos de segurança e nomes DNS dos dispositivos incluídos no domínio.

   4. Caso necessário, desinstale o Servidor de Administração e o servidor de banco de dados do dispositivo anterior.

      Não deve haver vários Servidores de Administração na mesma rede com o mesmo endereço de conexão e certificado do Servidor de Administração.

O administrador terá acesso aos dados do Servidor de Administração e aos dispositivos gerenciados pelo Kaspersky Security Center Windows, considerando as funcionalidades compatíveis com o Kaspersky Security Center Linux.

Login no Kaspersky Security Center Web Console e logout

É possível fazer login no Kaspersky Security Center Web Console após instalar o Servidor de Administração e o Web Console Server. Você deve saber o endereço da Web do Servidor de Administração e o número de porta especificado durante a instalação (por padrão, a porta é 8080). No navegador, o JavaScript deve ser ativado.

É possível fazer login no Kaspersky Security Center Web Console usando os seguintes métodos:

- Por meio da autenticação de domínio

  Caso esse método seja escolhido, confirme se a sondagem do Active Directory foi ativada e os usuários do domínio foram adicionados no Servidor de Administração.

- Por meio da especificação do nome de usuário e da senha do administrador

Fazer login usando a autenticação de domínio

Para fazer login no Kaspersky Security Center Web Console usando a autenticação do domínio:

1. No navegador, acesse https://<Endereço do Kaspersky Security Center Web Console>:<Número da porta>

   A página de login é exibida.

2. Se tiver adicionado vários servidores confiáveis, selecione, na lista Servidores de Administração, o Servidor de Administração ao qual deseja se conectar.

   Caso tenha adicionado apenas um único Servidor de Administração, a lista de Servidores de Administração estará bloqueada.

3. Execute uma das seguintes ações:

   - Clique no botão **Autenticação do domínio**.
   - Caso um ou mais Servidores de Administração virtuais sejam criados no Servidor e o usuário desejar fazer login no Servidor virtual usando a autenticação do domínio:

     a. Clique em **Configurações avançadas**.

     b. Digite o nome do Servidor de Administração virtual que você especificou enquanto criava o servidor virtual.

     c. Clique no botão **Autenticação do domínio**.

Após o login, o painel será exibido contendo o idioma e o tema que você usou pela última vez. Você pode navegar pelo Kaspersky Security Center Web Console e usá-lo para uso com o Kaspersky Security Center.

Fazer login especificando o nome de usuário e a senha do administrador

Para fazer login no Kaspersky Security Center Web Console especificando o nome de usuário e a senha do administrador:

1. No navegador, acesse https://<Endereço do Kaspersky Security Center Web Console>:<Número da porta>

   A página de login é exibida.

2. Se tiver adicionado vários servidores confiáveis, selecione, na lista Servidores de Administração, o Servidor de Administração ao qual deseja se conectar.

   Caso tenha adicionado apenas um único Servidor de Administração, a lista de Servidores de Administração estará bloqueada.

3. Execute uma das seguintes ações:

   - Para fazer login no Servidor de Administração:

     a. Insira o nome de usuário e a senha do Administrador local.

     b. Clique no botão **Login**.

   - Se um ou mais Servidores de Administração virtuais forem criados no Servidor e o usuário desejar fazer login no Servidor virtual:

     a. Clique em **Configurações avançadas**.

     b. Digite o nome do Servidor de Administração virtual que você especificou enquanto criava o servidor virtual.

     c. Digite o nome de usuário e a senha do administrador que tem direitos no Servidor de Administração virtual.

     d. Clique no botão **Login**.

Após o login, o painel será exibido contendo o idioma e o tema que você usou pela última vez. Você pode navegar pelo Kaspersky Security Center Web Console e usá-lo para trabalhar com o Kaspersky Security Center.

Fazer logout

Para fazer o logout do Kaspersky Security Center Web Console,

No menu principal, acesse as configurações da conta e selecione **Sair**.

O Kaspersky Security Center Web Console é fechado, e a página de login é exibida.

Gerenciador de Identidade e Acesso no Kaspersky Security Center Web Console

Esta seção fornece informações sobre o Gerenciador de Identidade e Acesso (também conhecido como IAM).

Sobre o Gerenciador de Identidade e Acesso

O *gerenciador de identidade e acesso* (também conhecido como IAM) é um componente do Kaspersky Security Center Web Console que permite usar um login único (SSO) entre o Kaspersky Security Center Web Console e a interface da Web do Kaspersky Industrial CyberSecurity for Networks. O IAM usa o protocolo OAuth 2.0 para garantir a autorização do Kaspersky Industrial CyberSecurity for Networks no Kaspersky Security Center Web Console.

Nesse caso, o Kaspersky Industrial CyberSecurity for Networks, acessível por meio do Kaspersky Security Center Web Console, é conhecido como um *servidor de recursos*, e o Kaspersky Security Center Web Console e a interface da Web do Kaspersky Industrial CyberSecurity for Networks são conhecidos como *clientes OAuth 2.0*. Um servidor de recursos é um programa que funciona com vários usuários e requer autorização. O cliente usa um *token* para autorização no servidor de recursos. Um token é uma sequência única de bytes. Quando um token expira, ele é reemitido automaticamente. O IAM atua como um único servidor de autorização para vários clientes OAuth 2.0.

Você pode instalar o IAM ao instalar o Kaspersky Security Center Web Console. Você pode ativá-lo mais tarde a qualquer momento nas configurações do Kaspersky Security Center Web Console. Caso o Kaspersky Industrial CyberSecurity Server ou a interface da Web do Kaspersky Industrial CyberSecurity estejam instalados em um dispositivo gerenciado pelo mesmo Servidor de Administração, o IAM detecta o programa e uma notificação com as informações é exibida no Kaspersky Security Center Web Console. É possível registrar o Kaspersky Industrial CyberSecurity for Networks e depois usar o SSO para o Kaspersky Security Center Web Console e a interface da Web do Kaspersky Industrial CyberSecurity for Networks.

Caso o usuário saia do Kaspersky Security Center Web Console, a sessão na interface da Web do Kaspersky Industrial CyberSecurity for Networks será encerrada e será preciso fazer login no Kaspersky Security Center Web Console novamente.

Ativando o Gerenciador de Identidade e Acesso: cenário

Pré-requisitos

Antes de começar, certifique-se de ter acesso ao Kaspersky Industrial CyberSecurity for Networks versão 3.1 ou posterior.

Fases

Ativar o Gerenciador de Identidade e Acesso (também conhecido como IAM) é feito em etapas:

1. **Verificando as portas necessárias**

   Certifique-se de que as portas 3333, 4004 e 4444 estejam abertas no dispositivo onde o Kaspersky Security Center Web Console está instalado. Essas portas são necessárias para usar o OAuth 2.0. Caso queira, é possível alterar os números de porta padrão na janela de configurações do Kaspersky Security Center Web Console.

   Além das portas 3333, 4004 e 4444, o Kaspersky Security Center Web Console também usa as portas 4445, 2444 e 2445 para várias finalidades.

2. **Instalando o Gerenciador de Identidade e Acesso**

Durante a instalação do Kaspersky Security Center Web Console, especifique que deseja instalar o Gerenciador de Identidade e Acesso. Se ainda não o fez, execute o Assistente de instalação do Kaspersky Security Center Web Console novamente.

3. **Configurando o Gerenciador de Identidade e Acesso**

   Na janela do Kaspersky Security Center Web Console, certifique-se de que o botão de alternância do **Identity and Access Manager (IAM)** está ativado. Além disso, especifique o nome DNS do dispositivo em que o Kaspersky Security Center Web Console está instalado: os aplicativos cliente serão conectados nesse dispositivo.

4. **Especificando as configurações de token**

   Na janela de configurações do Kaspersky Security Center Web Console, especifique o tempo de vida útil dos tokens e o tempo limite de autorização que o Gerenciador de Identidade e Acesso usará. Você pode usar os valores padrão ou especificar seus próprios valores, de acordo com suas necessidades.

5. **Concessão de certificados**

   Caso queira usar os certificados gerados pelo Servidor de Administração, então, na janela de configurações do Kaspersky Security Center Web Console, baixe os certificados raiz para as portas usadas pelo IAM e distribua-os para as estações de trabalho dos usuários do Kaspersky Security Center Web Console. Caso contrário, os navegadores dos usuários exibirão mensagens de erro ao tentarem se conectar ao Kaspersky Security Center Web Console.

6. **Registro das interfaces da web do Kaspersky Industrial CyberSecurity for Networks Servers e do Kaspersky Industrial CyberSecurity for Networks**

   Quando o IAM é instalado, o Kaspersky Security Center Web Console exibe uma mensagem informando que um servidor Industrial CyberSecurity for Networks Servers e um ou mais interfaces da web do Kaspersky Industrial CyberSecurity for Networks aguardam para serem registrados. Clique na mensagem para registrar o Kaspersky Industrial CyberSecurity for Networks Server (ou vários servidores) e interface da Web (ou várias interfaces da web).

Resultados

Depois de concluir este cenário, você será capaz de usar SSO e o IAM para o Kaspersky Industrial CyberSecurity for Networks e o Kaspersky Security Center Web Console.

Configurando o Gerenciador de Identidade e Acesso no Kaspersky Security Center Web Console

Para configurar o Gerenciado de acordo com suas necessidades:

1. No menu principal, vá para **Configurações do console** → **Integração**.
2. Na seção **Identity and Access Manager**, certifique-se de que o Identity and Access Manager esteja ativado.
3. Clique no link **Configurações** na linha do **Nome da rede do dispositivo do Gerenciador de Identidade e Acesso**.
4. Especifique o nome DNS do dispositivo no qual você instalou o Gerenciador de Identidade e Acesso. Os aplicativos cliente irão se conectar a este dispositivo.
5. Se quiser, mude as configurações de token padrão, as configurações de certificado, e os números de porta clicando no link **Configurações** no grupo de configurações relevante.

O Gerenciador de Identidade e Acesso está ativado e funcionando de acordo com suas necessidades.

Registrar o aplicativo Kaspersky Industrial CyberSecurity for Networks no Kaspersky Security Center Web Console

Para começar a trabalhar com o aplicativo Kaspersky Industrial CyberSecurity for Networks por meio do Kaspersky Security Center Web Console, primeiro é necessário registrá-lo no Kaspersky Security Center Web Console.

Para registrar o aplicativo Kaspersky Industrial CyberSecurity for Networks:

1. Certifique-se de que o seguinte procedimento seja feito:

   - Você baixou e instalou o plug-in da Web do Kaspersky Industrial CyberSecurity for Networks.

     No entanto, é possível fazer isso posteriormente, enquanto a sincronização com Kaspersky Industrial CyberSecurity for Networks Server é aguardada com o Servidor de Administração.

   - O cenário de preparação de uso da tecnologia de Conexão única (SSO) foi concluído.

   - As configurações necessárias na interface da Web do Kaspersky Industrial CyberSecurity for Networks são especificadas na página do Kaspersky Security Center. Para detalhes, consulte a Ajuda on-line do Kaspersky Industrial CyberSecurity for Networks.

   - O usuário está conectado ao Kaspersky Security Center Web Console com uma conta de administrador.

   - IAM está configurado.

2. Mova o dispositivo onde o Kaspersky Industrial CyberSecurity for Networks Server estiver instalado do grupo dispositivos não atribuídos para o grupo dispositivos gerenciados:

   a. No menu principal, vá para **Descoberta e implementação** → **Dispositivos não atribuídos**.

   b. Marque a caixa de seleção ao lado do dispositivo onde o Kaspersky Industrial CyberSecurity for Networks Server estiver instalado.

   c. Clique no botão **Migrar para grupo**.

   d. Na hierarquia de grupos de administração, marque a caixa de seleção ao lado do grupo de dispositivos gerenciados.

   e. Clique no botão **Migrar**.

3. Acesse as propriedades do dispositivo em que o Kaspersky Industrial CyberSecurity for Networks Server está instalado.

4. Na página de propriedades do dispositivo, na seção **Geral**, selecione a opção **Não desconecte do Servidor de Administração** e, em seguida, clique no botão **Salvar**.

5. Na janela de propriedades do dispositivo, selecione a seção **Aplicativos**.

6. Na seção **Aplicativos**, selecione Agente de Rede da Kaspersky.

7. Caso o status atual do aplicativo seja *Interrompido*, espere até que mude para *Executando*.

   O processo leva até 15 minutos. Caso ainda não tenha instalado o plug-in da Web do Kaspersky Industrial CyberSecurity for Networks, pode fazê-lo agora, enquanto espera.

8. No menu principal, vá para **Configurações do console → Integração**.

   No campo **Solicitações de registro**, uma solicitação pendente é exibida.

9. Clique no link **Configurações** sob o campo **Solicitações de registro**.

10. Na lista aberta de clientes registrados, marque a caixa de seleção ao lado do nome do Kaspersky Industrial CyberSecurity for Networks Server, com o status *Pendente* e, em seguida, clique no botão **Aprovar**.

    Caso não queira registrar o Kaspersky Industrial CyberSecurity for Networks Server, é possível clicar no botão Recusar e voltar a esta lista mais tarde.

    Depois de clicar no botão **Aprovar**, o status muda para *Aprovado*, e depois para *Pronto*. Caso o status não mude, é possível clicar no botão Atualizar.

11. Feche a lista de clientes registrados e certifique-se de que o valor no campo **Clientes registrados** aumentou.

12. Para adicionar o widget Kaspersky Industrial CyberSecurity for Networks ao painel:

    a. No menu principal, vá para **Monitoramento e relatórios → Painel**.

    b. No painel, clique no botão **Adicionar ou restaurar widget da Web**.

    c. No widget do menu aberto, selecione **Outro**.

    d. Selecione o widget Kaspersky Industrial CyberSecurity for Networks.

    Agora, é possível prosseguir até a interface da Web do Kaspersky Industrial CyberSecurity for Networks usando o link no widget.

Após concluir o procedimento de registro, um novo botão, **Kaspersky Security Center**, aparece na página de login da interface da Web do Kaspersky Industrial CyberSecurity for Networks. É possível clicar no botão para fazer login na interface da Web do Kaspersky Industrial CyberSecurity for Networks com as credenciais do Kaspersky Security Center.

Tempo de vida útil de tokens e tempo limite de autorização para Gerenciador de Identidade e Acesso

Ao configurar o Gerenciador de Identidade e Acesso (também conhecido como IAM), você deve especificar as configurações para o tempo de vida útil do token e o tempo limite de autorização. As configurações padrão são projetadas para refletir os padrões de segurança e a carga do servidor. No entanto, você pode alterar essas configurações de acordo com as políticas da sua organização.

O IAM reemite automaticamente um token quando este está prestes a expirar.

A tabela a seguir lista as configurações de vida útil do token padrão.

Configurações de tempo de vida útil do token

Token	Vida útil padrão (em segundos)	Descrição
Token de identidade (id_token)	86400	O token de identidade usado pelo cliente OAuth 2.0 (ou seja, Kaspersky Security Center Web Console ou console do Kaspersky Industrial CyberSecurity). O IAM envia o ID token ao cliente contendo as informações sobre o usuário (ou seja, o perfil do usuário).
Token de acesso (access_token)	86400	O token de acesso usado pelo cliente OAuth 2.0 para acessar o servidor de recursos em nome do proprietário do recurso identificado pelo IAM.
Token de atualização (refresh_token)	172800	O cliente OAuth 2.0 usa esse token para reemitir o token de identidade e o token de acesso.

A tabela a seguir lista os tempos limite para auth_code e login_consent_request.

Configurações de tempo limite de autorização

Configuração	Tempo limite padrão (em segundos)	Descrição
Código de autorização (auth_code)	3600	Tempo limite para troca de código pelo token. O cliente OAuth 2.0 envia esse código ao servidor de recursos e obtém o token de acesso em troca.
Tempo limite para consentimento de login (login_consent_request)	3600	Tempo limite para delegar direitos de usuário ao cliente OAuth 2.0.

Para obter mais informações sobre tokens, consulte o Site OAuth.

Baixando e distribuindo os certificados IAM

Por padrão, o Gerenciador de Identidade e Acesso usa os certificados gerados pelo Servidor de Administração para conceder aos navegadores acesso ao Kaspersky Security Center Web Console. No entanto, se desejar, você pode usar certificados personalizados. Qualquer que seja o certificado usado, é preciso garantir que todas as estações de trabalho usadas pelos usuários para acessar o Kaspersky Security Center Web Console confiem neste certificado.

Para baixar e distribuir certificados:

1. No menu principal, vá para **Configurações do console** → **Integração**.
2. Para cada certificado, clique no link **Definições** no grupo de configurações relevante e, em seguida, execute uma das seguintes ações:
   - Se deseja usar o certificado que o Servidor de Administração gerou durante a instalação do Kaspersky Security Center Web Console:
     1. Selecione **Certificado gerado pelo Servidor de Administração** na janela aberta de propriedades do certificado.
     2. Clique no botão **Baixar** para baixar o certificado.
     3. Distribua o certificado baixado para todas as estações de trabalho nas quais os usuários usam para acessar o Kaspersky Security Center Web Console.
   - Se tiver um certificado que deseja usar:
     1. Selecione **Certificado TLS personalizado** na janela aberta de propriedades do certificado.
     2. Selecione o arquivo de certificado e a chave privada.
     3. Clique no botão **OK**.
     4. Distribua o certificado para todas as estações de trabalho que os usuários usam para acessar o Kaspersky Security Center Web Console o ou Kaspersky Industrial CyberSecurity Console.

Os certificados concedem aos usuários acesso ao Kaspersky Security Center Web Console e ao Kaspersky Industrial CyberSecurity Console.

É necessário reemitir todos os certificados em tempo hábil. Os certificados gerados pelo Servidor de Administração devem ser gerados novamente manualmente. Os certificados gerados pelo instalador do Kaspersky Security Center Web Console devem ser gerados novamente usando o instalador.

Desativando o Gerenciador de Identidade e Acesso

Caso queira, é possível desativar o gerenciador de identidade e acesso (também conhecido como IAM).

Para desativar a IAM:

Na janela de configurações do Kaspersky Security Center Web Console, mude o botão de alternância IAM para desativado.

Você pode habilitar o IAM a qualquer momento depois.

Se você atualizar o Kaspersky Security Center Web Console por meio do instalador e especificar que não deseja instalar o IAM, o Kaspersky Security Center Web Console será atualizado e o IAM não será instalado. Todas as informações sobre a integração com o Kaspersky Industrial CyberSecurity for Networks serão excluídas do computador, assim como os arquivos de configuração e log do IAM.

Configurando a autenticação de domínio usando os protocolos NTLM e Kerberos

O Kaspersky Security Center 14.2 permite usar a autenticação de domínio no OpenAPI usando os protocolos NTLM e Kerberos. O uso da autenticação de domínio permite que um usuário do Windows ative a autenticação segura no Kaspersky Security Center Web Console sem ter que inserir novamente a senha na rede corporativa (autenticação única).

A autenticação de domínio em OpenAPI sobre o protocolo Kerberos tem as seguintes restrições:

- O usuário do Kaspersky Security Center Web Console deve ser autenticado no Active Directory usando o protocolo Kerberos. O usuário deve ter um tíquete de concessão de tíquete Kerberos válido (também conhecido como TGT). Um TGT é emitido automaticamente quando você se autentica no domínio.
- Você deve configurar a autenticação Kerberos no navegador. Para obter detalhes, consulte a documentação do navegador que você está usando.

Se deseja usar a autenticação de domínio usando protocolos Kerberos, sua rede deve atender às seguintes condições:

- O Servidor de Administração deve ser executado com o nome da conta de domínio.
- Kaspersky Security Center Web Console Server deve ser instalado no mesmo dispositivo em que o Servidor de Administração está instalado.
- É preciso especificar os seguintes nomes do serviço principal (SPN) para a conta do Servidor de Administração:
  - "http/<server.fqnd.name>"
  - "http/<server>"

  Aqui, <server> é o nome da rede do dispositivo do Servidor de Administração, e <server.fqnd.name> é o nome FQDN do dispositivo do Servidor de Administração.
- Ao conectar-se ao Console de Administração ou ao Kaspersky Security Center Web Console, o endereço do servidor deve ser especificado exatamente como o endereço para o qual o Nome Principal do Serviço (SPN) está registrado. É possível especificar <server.fqnd.name> ou <server>.
- Para um login sem senha, o processo do navegador no qual o Kaspersky Security Center Web Console é aberto como navegador deve ser executado em uma conta de domínio.

Os protocolos Kerberos e NTLM são compatíveis apenas no OpenAPI para Kaspersky Security Center 14.2. Eles não são compatíveis no OpenAPI para Kaspersky Security Center Linux.

Configurando o Servidor de Administração

Esta seção descreve o processo de configuração e as propriedades do Servidor de Administração do Kaspersky Security Center.

Configuração da conexão do Kaspersky Security Center Web Console ao Servidor de Administração

Para definir as portas de conexão do Servidor de Administração:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Portas de conexão**.

O aplicativo exibe as configurações de conexão principais do servidor selecionado.

O Kaspersky Security Center Web Console está conectado ao Servidor de Administração pela porta SSL TCP 13299. A mesma porta pode ser usada por objetos de automação klakaut.

A Porta TCP 14000 pode ser usada para conectar o Kaspersky Security Center Web Console, pontos de distribuição, Servidores de Administração secundários e objetos de automação klakaut, além de receber dados de dispositivos cliente.

Normalmente, a porta SSL TCP 13000 pode ser usada somente pelo Agente de Rede, um Servidor de Administração secundário e o Servidor de Administração principal na DMZ. Em alguns casos, o Kaspersky Security Center Web Console precisa ser conectado pela porta SSL 13000:

- Caso uma porta SSL única for provavelmente usada tanto para o Kaspersky Security Center Web Console como para outras atividades (receber dados de dispositivos de cliente, conectar pontos de distribuição, conectar Servidores de Administração secundários).
- Se um objeto de automação klakaut não estiver conectado ao Servidor de Administração diretamente, mas através de um ponto de distribuição na DMZ.

Configuração do registro em log de eventos de conexão do Servidor de Administração

O histórico das conexões e tentativas de conexão ao Servidor de Administração durante a operação pode ser salvo em um arquivo de registro. As informações no arquivo permitem que você rastreie não só as conexões dentro sua infraestrutura de rede, mas também as tentativas não autorizadas de acessar o servidor.

Para registrar eventos da conexão ao Servidor de Administração:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Portas de conexão**.

3. Ative a opção **Criar log de eventos de conexão do Servidor de Administração**.

Todos os eventos adicionais das conexões de entrada com o Servidor de Administração, resultados de autenticação e erros de SSL serão salvos no arquivo %ProgramData%\KasperskyLab\adminkit\logs\sc.syslog.

Definição das configurações de acesso à Internet para o Servidor de Administração

É preciso configurar o acesso à Internet para usar a Kaspersky Security Network e baixar atualizações de bancos de dados de antivírus para o Kaspersky Security Center e aplicativos Kaspersky gerenciados.

Para especificar as configurações de acesso à Internet para o Servidor de Administração:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurando acesso à internet**.

3. Ative a opção **Usar o servidor proxy** caso queira usar um servidor proxy para se conectar com a Internet. Caso essa opção esteja ativada, os campos estarão disponíveis para inserir as configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:

   - **Endereço**

     Endereço do servidor proxy usado para conexão do Kaspersky Security Center à Internet.

   - **Número da porta**

     Número da porta pela qual a conexão proxy do Kaspersky Security Center será estabelecida.

   - **Ignorar servidor proxy para endereços locais**

     Nenhum servidor proxy será usado para conectar-se aos dispositivos na rede local.

   - **Autenticação do servidor proxy**

     Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

     Este campo de entrada está disponível se a caixa de seleção **Usar o servidor proxy** estiver marcada.

   - **Nome do usuário**

     Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

   - **Senha**

     A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

     Para ver a senha inserida, mantenha pressionado o botão **Exibir** pelo tempo que você desejar.

Também é possível configurar o acesso à Internet usando o assistente de início rápido.

Configuração do número máximo de eventos no repositório de eventos

Na seção **Repositório de eventos** da janela Propriedades do Servidor de Administração, você pode editar as configurações de armazenamento do evento no banco de dados do Servidor de Administração ao limitar o número de registros de evento ou o tempo de armazenamento do registro. Quando você especifica o número máximo de eventos, o aplicativo calcula um volume aproximado do espaço de armazenamento necessário para o número especificado. Você pode usar esse cálculo aproximado para avaliar se você tem espaço livre suficiente no disco para evitar sobrecarga do banco de dados. A capacidade padrão do banco de dados do Servidor de Administração é de 400.000 eventos. A capacidade máxima recomendada do banco de dados é de 45 milhões de eventos.

O aplicativo verifica o banco de dados a cada 10 minutos. Caso o número de eventos atinja o valor máximo especificado em mais de 10.000, o aplicativo exclui os eventos mais antigos para que apenas o número máximo de eventos especificado permaneça.

Quando o Servidor de Administração exclui eventos antigos, não pode salvar novos eventos no banco de dados. Durante esse período de tempo, as informações sobre eventos rejeitados são gravadas no Log de Eventos Kaspersky. Os novos eventos são colocados em fila e salvos no banco de dados depois que a operação de exclusão é concluída.

Para limitar o número de eventos que podem ser armazenados no repositório de eventos no Servidor de Administração:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Repositório de eventos**. Especifique o número máximo de eventos armazenados no banco de dados.

3. Clique no botão **Salvar**.

Você também pode fazer o seguinte:

- Alterar as configurações de qualquer tarefa para salvar eventos relacionados ao andamento da tarefa ou salvar apenas os resultados de execução da tarefa.

- Reduzir ou desabilitar o período de armazenamento para os eventos do Servidor de Administração, Agente de Rede e aplicativos da Kaspersky instalados em dispositivos gerenciados.

Ao fazer isso, você reduzirá o número de eventos no banco de dados, aumentará a velocidade da execução dos cenários associados com a análise da tabela de eventos no banco de dados e abaixará o risco de que os eventos críticos sejam substituídos por um grande número de eventos.

Configurações de conexão de dispositivos de proteção UEFI

Um *dispositivo de proteção UEFI* é um dispositivo com uma solução ou aplicativo da Kaspersky para UEFI integrado no nível da BIOS. A proteção integrada assegura a segurança do dispositivo do momento do início do sistema, enquanto a proteção nos dispositivos sem software integrado somente começa a funcionar após o início do aplicativo de segurança. O Kaspersky Security Center suporta o gerenciamento destes dispositivos.

Para modificar as configurações de conexão de dispositivos de proteção UEFI:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Portas adicionais**.

3. Modifique as configurações relevantes:

   - Abrir porta para os dispositivos de proteção UEFI e dispositivos KasperskyOS

     Os dispositivos de proteção UEFI poderão ser conectados ao Servidor de Administração.

   - Porta para os dispositivos de proteção UEFI e dispositivos KasperskyOS

     Você pode alterar o número da porta se a opção **Abrir porta para os dispositivos de proteção UEFI e dispositivos KasperskyOS** estiver ativada. O número da porta padrão é 13294.

4. Clique no botão **Salvar**.

Os dispositivos de proteção UEFI poderão agora ser conectados ao Servidor de Administração.

Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário

Adição de Servidor de Administração secundário (executada no futuro Servidor de Administração principal)

Você pode adicionar um Servidor de Administração como um Servidor de Administração secundário, portanto, estabelecendo uma hierarquia "principal/secundário".

Para adicionar um Servidor de Administração secundário que está disponível para conexão por meio do Kaspersky Security Center Web Console:

1. Assegure-se de que a porta 13000 do Servidor de Administração principal futuro esteja disponível para o recebimento de conexões de Servidores de Administração secundário.

2. No futuro Servidor de Administração principal, clique no ícone de configurações ( ).

3. Na página de propriedades aberta, clique na guia **Servidores de Administração**.

4. Selecionar a caixa de seleção ao lado do nome do grupo de administração ao qual deseja adicionar o Servidor de Administração.

5. Na linha de menu, clique em **Conectar Servidor de Administração secundário**.

   O assistente para Adicionar Servidor de Administração secundário é iniciado. Navegue pelo assistente usando o botão **Avançar**.

6. Preencha os campos a seguir:

   - **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ**

     Selecione esta opção se o Servidor de Administração secundário estiver em uma zona desmilitarizada (DMZ).

     Se esta opção estiver selecionada, você precisará especificar o parâmetro **endereço do Servidor secundário**.

     Caso esta opção seja selecionada, o Servidor de Administração principal inicia a conexão com o Servidor de Administração secundário. Caso contrário, o Servidor de Administração secundário inicia a conexão com o Servidor de Administração principal.

   - **Nome de exibição do Servidor de Administração secundário**

     O nome designado para o Servidor de Administração secundário será exibido na hierarquia. Se desejar, você pode inserir o endereço IP como um nome ou pode usar um nome como "Servidor secundário para o grupo 1".

   - **Endereço do Servidor de Administração secundário (opcional)**

     Especifique o endereço IP ou o nome de domínio do Servidor de Administração secundário.

     Esse parâmetro será obrigatório se a opção **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ** estiver ativada.

   - **Porta SSL do Servidor de Administração**

     Especifique o número da porta SSL no Servidor de Administração principal. O número da porta padrão é 13000.

   - **Porta API do Servidor de Administração**

     Especifique o número da porta no Servidor de Administração principal para receber conexões através do OpenAPI. O número da porta padrão é 13299.

7. Especifique o certificado para o Servidor de Administração secundário. Se você especificou o parâmetro **endereço do Servidor secundário**, clique no botão **Obter do Servidor de Administração secundário** para receber o certificado. Caso contrário, clique no botão **Procurar o arquivo de certificado** e localize o arquivo de certificado.

8. Especifique as configurações da conexão:

   - Insira o endereço do futuro Servidor de Administração principal.

   - Se o futuro Servidor de Administração secundário usar um servidor proxy, digite o endereço do servidor proxy e as credenciais do usuário para se conectar a ele.

9. Insira as credenciais do usuário que possui direitos de acesso no futuro Servidor de Administração secundário.

10. Se a verificação em duas etapas estiver ativada e configurada, especifique o código de segurança gerado pelo app autenticador.

    Se a verificação em duas etapas estiver ativada, mas não configurada para a conta especificada, crie a hierarquia a partir do futuro Servidor secundário (consulte as instruções abaixo).

Se as configurações de conexão estiverem corretas, a conexão com o futuro Servidor secundário será estabelecida e a hierarquia "principal/secundário" será construída. Se a conexão falhar, verifique as configurações de conexão ou especifique o certificado do futuro Servidor secundário manualmente.

A conexão entre os Servidores de Administração principal e secundário é estabelecida pela porta 13000. As tarefas e as políticas do Servidor de Administração principal são recebidas e aplicadas. O Servidor de Administração secundário é exibido no Servidor de Administração principal, no grupo de administração ao qual foi adicionado.

Adição de Servidor de Administração secundário (executada no futuro Servidor de Administração principal)

Se não conseguir se conectar ao futuro Servidor de Administração secundário (por exemplo, porque estava temporariamente desconectado ou indisponível), você ainda poderá adicionar um Servidor de Administração secundário.

Para adicionar como secundário um Servidor de Administração que não está disponível para a conexão através do Kaspersky Security Center Web Console:

1. Envie o arquivo de certificado do futuro Servidor de Administração principal para o administrador do sistema do escritório onde o futuro Servidor de Administração secundário está localizado. (Você pode, por exemplo, gravar o arquivo em um dispositivo externo, como um pendrive, ou enviá-lo por e-mail.)

   O arquivo de certificado está localizado no futuro Servidor de Administração principal, em %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert\klserver.cer.

2. Solicita que administrador de sistema responsável pelo futuro Servidor de Administração secundário faça o seguinte:

   a. Clique no ícone de configurações ( ).

   b. Na página de propriedades que se abre, prossiga para a seção **Hierarquia de Servidores de Administração** da guia **Geral**.

   c. Selecione a opção **Esse Servidor de Administração é secundário na hierarquia**.

   d. No campo **Endereço do Servidor de Administração Principal**, insira o nome da rede do Servidor de Administração principal futuro.

   e. Selecione o arquivo com o certificado do Servidor de Administração principal futuro anteriormente salvo ao clicar em **Procurar**.

   f. Se necessário, marque a caixa de seleção **Conectar o Servidor de Administração principal ao Servidor de Administração secundário na DMZ**.

   g. Caso a conexão ao futuro servidor de administração secundário seja executada por meio de um servidor proxy, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão.

   h. Clique em **Salvar**.

A hierarquia "principal/secundário" é construída. O Servidor de Administração principal começa a receber a conexão do Servidor de Administração secundário usando a porta 13000. As tarefas e as políticas do Servidor de Administração principal são recebidas e aplicadas. O Servidor de Administração secundário é exibido no Servidor de Administração principal, no grupo de administração ao qual foi adicionado.

Visualizar a lista de Servidores de administração secundários

Para visualizar a lista de Servidores de administração secundários (incluindo virtuais):

No menu principal, clique no nome do Servidor de Administração ao lado do ícone de configurações ( ).

A lista suspensa dos Servidores de administração secundários (incluindo virtuais) é exibida.

Você pode prosseguir para qualquer um desses Servidores de Administração clicando no nome.

Os grupos de administração também são exibidos, mas estão em cinza e indisponíveis para gerenciamento neste menu.

Se você estiver conectado ao seu Servidor de Administração principal no Kaspersky Security Center Web Console e não puder se conectar a um Servidor de Administração virtual gerenciado por um Servidor de Administração secundário, poderá usar uma das seguintes formas:

- **Modifique a instalação existente do Kaspersky Security Center Web Console para adicionar o Servidor secundário à lista de Servidores de Administração confiáveis**. Em seguida, você poderá se conectar ao Servidor de Administração virtual no Kaspersky Security Center Web Console.

  1. No dispositivo em que o Kaspersky Security Center Web Console está instalado, execute o arquivo de instalação ksc-web-console-<número da versão>.<número da compilação>.exe em uma conta com direitos administrativos.

     O Assistente de Instalação será iniciado. Navegue pelo assistente usando o botão **Avançar**.

  2. Selecione a opção **Atualizar**.

  3. Na etapa **Tipo de modificação**, selecione a opção **Editar as configurações de conexão**.

  4. Na etapa **Servidores de Administração confiáveis**, adicione o Servidor de Administração secundário necessário.

  5. Na última etapa, clique em **Modificar** para aplicar as novas configurações.

  6. Após a conclusão com êxito da reconfiguração do aplicativo, clique no botão **Concluir**.

- Use o Kaspersky Security Center Web Console para conectar-se diretamente ao Servidor de Administração secundário em que o servidor virtual foi criado. Em seguida, você poderá trocar o Servidor de Administração virtual no Kaspersky Security Center Web Console.

- Use o Console de Administração baseado em MMC para conectar-se diretamente ao Servidor virtual.

Excluir uma hierarquia de Servidores de Administração

Se você não quiser mais ter uma hierarquia de Servidores de Administração, você poderá desconectá-los dessa hierarquia.

Para excluir uma hierarquia de Servidores de Administração:

1. No menu principal, clique no ícone de Configurações ( ) ao lado do nome do Servidor de Administração principal.

2. Na página que se abre, prossiga para a guia **Servidores de Administração**.

3. No grupo de administração do qual deseja excluir o Servidor de administração secundário, selecione o Servidor de administração secundário.

4. Na linha de menu, clique em **Excluir**.

5. Na janela que se abre, clique em **OK** para confirmar que deseja excluir o Servidor de administração secundário.

Os antigos Servidores de administração principal e secundário agora são independentes um do outro. A hierarquia não existe mais.

Manutenção do Servidor de Administração

A manutenção do Servidor de Administração permite liberar espaço na pasta do Servidor de Administração e reduzir o volume do banco de dados excluindo objetos que não são mais necessários. Isso ajuda a melhorar o desempenho e a confiabilidade da operação do aplicativo. Nós recomendamos que você efetue a manutenção do Servidor de Administração ao menos uma vez por semana.

A manutenção do Servidor de Administração é executada usando uma tarefa dedicada. O aplicativo executa as seguintes ações ao efetuar a manutenção do Servidor de Administração:

- Exclui pastas e arquivos desnecessários da pasta de armazenamento.
- Exclui registros desnecessários das tabelas (também conhecidos como "ponteiros pendentes").
- Limpa o cache.
- Mantém o banco de dados (se você usar o SQL Server ou PostgreSQL como um DBMS):
  - Verifica se há erros no banco de dados (disponível somente para o SQL Server).
  - Reorganiza os índices do banco de dados.
  - Atualiza as estatísticas do banco de dados.
  - Diminui o banco de dados (se necessário).

A tarefa Manutenção do Servidor de Administração oferece suporte às versões 10.3 e posteriores do MariaDB. Caso as versões 10.2 ou anteriores do MariaDB sejam usadas, os administradores terão que manter esse DBMS por conta própria.

A tarefa Manutenção do Servidor de Administração é criada automaticamente quando você instala o Kaspersky Security Center. Se a tarefa Manutenção do Servidor de Administração for excluída, você poderá criá-la manualmente.

Para criar uma tarefa Manutenção do Servidor de Administração:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia.
3. Na janela **Nova tarefa** do assistente, selecione **Manutenção do Servidor de Administração** como tipo de tarefa e clique no botão **Avançar**.
4. Siga o restante das instruções do assistente.

A tarefa recém-criada é exibida na lista de tarefas. Somente uma tarefa Manutenção do Servidor de Administração pode ser executada para um único Servidor de Administração. Se uma tarefa de Manutenção do Servidor de Administração já tiver sido criada para um Servidor de Administração, nenhuma nova tarefa de Manutenção do Servidor de Administração poderá ser criada.

Configurar interface

Você pode configurar a interface do Kaspersky Security Center Web Console para exibir e ocultar seções e elementos da interface, dependendo dos recursos que estão sendo usados.

Para configurar a interface do Kaspersky Security Center Web Console de acordo com o conjunto de recursos usados no momento:

1. No menu principal, acesse as configurações da conta e selecione **Opções da interface.**
2. Na janela **Opções da interface** exibida, ative ou desative as opções exigidas.
3. Clique em **Salvar**.

Depois disso, o console exibirá seções no menu principal de acordo com as opções habilitadas. Por exemplo, se você habilitar **Exibir alertas EDR**, a seção **Monitoramento e relatórios** → **Alertas** aparecerá no menu principal.

Gerenciar Servidores de Administração virtuais

Esta seção descreve as seguintes ações para gerenciar Servidores de Administração virtuais:

- Criar Servidores de Administração virtuais
- Ativar ou desativar de Servidores de Administração virtuais
- Atribuir um administrador para um Servidor de Administração virtual
- Alterar o Servidor de Administração para dispositivos cliente
- Excluir Servidores de Administração virtuais

Criar um Servidor de Administração virtual

Você pode criar Servidores de Administração virtuais e adicioná-los a grupos de administração.

Quando um Servidor de Administração virtual é criado, ele herda a lista de usuários e todos os direitos de usuário do Servidor de Administração principal. Caso um usuário tenha direitos de acesso ao servidor principal, esse usuário também terá direitos de acesso ao servidor virtual. Após a criação, é necessário configurar os direitos de acesso para os Servidores de maneira independente.

Para criar e adicionar um Servidor de Administração virtual:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.
2. Na página que se abre, prossiga para a guia **Servidores de Administração**.

3. Selecione o grupo de administração ao qual você deseja adicionar um Servidor de Administração virtual.
   O Servidor de Administração virtual gerenciará os dispositivos do grupo selecionado (incluindo os subgrupos).

4. Na linha de menu, clique em **Novo Servidor de Administração virtual**.

5. Na página que se abre, defina as propriedades do novo Servidor de Administração virtual:

   - **Nome do Servidor de Administração virtual**.

   - **Endereço de conexão do Servidor de Administração**

     É possível especificar o nome ou o endereço IP do Servidor de Administração.

6. Na lista de usuários, selecione o administrador do Servidor de Administração virtual. Se quiser, você poderá editar uma das contas existentes antes de atribuir a ela a função de administrador ou criar uma nova conta de usuário.

7. Clique em **Salvar**.

O novo Servidor de Administração virtual é criado, adicionado ao grupo de administração e exibido na guia **Servidores de Administração**.

Se você estiver conectado ao seu Servidor de Administração principal no Kaspersky Security Center Web Console e não puder se conectar a um Servidor de Administração virtual gerenciado por um Servidor de Administração secundário, poderá usar uma das seguintes formas:

- Modifique a instalação existente do Kaspersky Security Center Web Console para adicionar o Servidor secundário à lista de Servidores de Administração confiáveis. Em seguida, você poderá se conectar ao Servidor de Administração virtual no Kaspersky Security Center Web Console.

  1. No dispositivo em que o Kaspersky Security Center Web Console está instalado, execute o arquivo de instalação ksc-web-console-<número da versão>.<número da compilação>.exe em uma conta com direitos administrativos.

     O Assistente de Instalação será iniciado. Navegue pelo assistente usando o botão **Avançar**.

  2. Selecione a opção **Atualizar**.

  3. Na etapa **Tipo de modificação**, selecione a opção **Editar as configurações de conexão**.

  4. Na etapa **Servidores de Administração confiáveis**, adicione o Servidor de Administração secundário necessário.

  5. Na última etapa, clique em **Modificar** para aplicar as novas configurações.

  6. Após a conclusão com êxito da reconfiguração do aplicativo, clique no botão **Concluir**.

- Use o Kaspersky Security Center Web Console para conectar-se diretamente ao Servidor de Administração secundário em que o servidor virtual foi criado. Em seguida, você poderá trocar o Servidor de Administração virtual no Kaspersky Security Center Web Console.

- Use o Console de Administração baseado em MMC para conectar-se diretamente ao Servidor virtual.

Ativando ou desativando um Servidor de Administração virtual

Ao criar um novo Servidor de Administração virtual, ele é ativado por padrão. Você pode desativá-lo ou ativá-lo novamente a qualquer momento. Desativar ou ativar um Servidor de Administração virtual é igual a desligar ou ligar um Servidor de Administração físico.

Para ativar ou desativar um Servidor de Administração virtual:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

2. Na página que se abre, prossiga para a guia **Servidores de Administração**.

3. Selecione o Servidor de Administração virtual que deseja ativar ou desativar.

4. Na linha do menu, clique no botão **Ativar/desativar Servidor de Administração virtual**.

   O estado do Servidor de Administração virtual é alterado para ativado ou desativado, dependendo da condição anterior. O estado atualizado é exibido próximo ao nome do Servidor de Administração.

Atribuição de um administrador para um Servidor de Administração virtual

Ao usar Servidores de Administração virtuais em sua organização, convém atribuir um administrador dedicado para cada Servidor de Administração virtual. Por exemplo, isso pode ser útil quando os Servidores de Administração virtuais são criados para gerenciar escritórios ou departamentos separados de sua organização, ou se você for um provedor de MSP e gerenciar locatários por meio de Servidores de Administração virtuais.

Quando um Servidor de Administração virtual é criado, ele herda a lista de usuários e todos os direitos de usuário do Servidor de Administração principal. Caso um usuário tenha direitos de acesso ao servidor principal, esse usuário também terá direitos de acesso ao servidor virtual. Após a criação, é preciso configurar os direitos de acesso aos Servidores de forma independente. Caso queira apenas atribuir um administrador para um Servidor de Administração virtual, verifique e confirme se o administrador não tem os direitos de acesso no Servidor de Administração principal.

É possível atribuir um administrador para um Servidor de Administração virtual concedendo os direitos de acesso de administrador ao Servidor de Administração virtual. É possível conceder os direitos de acesso necessários das seguintes formas:

- Configure os direitos de acesso para o administrador manualmente
- Atribua uma ou mais funções de usuário ao administrador

Para entrar no Kaspersky Security Center Web Console, um administrador de um Servidor de Administração virtual especifica nome, nome de usuário e senha do Servidor de Administração virtual. O Kaspersky Security Center Web Console autentica o administrador e abre o Servidor de Administração virtual ao qual o administrador tem direitos de acesso. O administrador não pode alternar entre os Servidores de Administração.

Pré-requisitos

Antes de iniciar, certifique-se de que as seguintes condições sejam atendidas:

- O Servidor de Administração virtual foi criado.
- No Servidor de Administração principal, foi criada uma conta para o administrador que se deseja atribuir ao Servidor de Administração virtual.
- O usuário tem o direto de **Modificar os objetos ACLs** na área funcional **Funcionalidades gerais → Permissões do usuário**.

Configuração dos direitos de acesso manualmente

Para atribuir um administrador para um Servidor de Administração virtual:

1. No menu principal, alterne para o Servidor de Administração virtual necessário:
   a. Clique no ícone de sinalização ( ) à direita do nome atual do Servidor de Administração.
   b. Selecione o Servidor de Administração necessário.
2. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.
   A janela Propriedades do Servidor de Administração é aberta.
3. Na guia **Direitos de acesso**, clique no botão **Adicionar**.
   Uma lista unificada de usuários do Servidor de Administração principal e do Servidor de Administração virtual atual é aberta.
4. Na lista de usuários, selecione a conta do administrador que deseja atribuir ao Servidor de Administração virtual e clique no botão **OK**.
   O aplicativo adiciona o usuário selecionado à lista de usuários na aba **Direitos de acesso**.
5. Marque a caixa de seleção ao lado de conta adicionada e clique no botão **Direitos de acesso**.
6. Configure os direitos que o administrador terá no Servidor de Administração virtual.
   Para uma autenticação bem-sucedida, no mínimo, o administrador deve ter os seguintes direitos:
   - Direito de **Ler** na área funcional **Funcionalidades gerais → Funcionalidade básica**
   - Direito de **Ler** na área funcional **Funcionalidades gerais → Servidores de Administração virtuais**

O aplicativo salva os direitos de usuário modificados na conta do administrador.

Configuração de direitos de acesso com a atribuição de uma função de usuário

Como alternativa, é possível conceder direitos de acesso a um administrador do Servidor de Administração virtual por meio de funções de usuário. Por exemplo, isso pode ser útil caso se queira atribuir vários administradores no mesmo Servidor de Administração virtual. Se esse for o caso, é possível atribuir às contas dos administradores a mesma função de usuário, em vez de configurar os mesmos direitos de usuário para vários administradores.

Para atribuir um administrador para um Servidor de Administração virtual por meio da atribuição da função de usuário:

1. No Servidor de Administração principal, crie uma nova função de usuário e especifique todos os direitos de acesso necessários que um administrador deve ter no Servidor de Administração virtual. É possível criar várias funções, por exemplo, caso queira separar o acesso a diferentes áreas funcionais.

2. No menu principal, alterne para o Servidor de Administração virtual necessário:

   a. Clique no ícone de sinalização (▶) à direita do nome atual do Servidor de Administração.

   b. Selecione o Servidor de Administração necessário.

3. Atribuir a nova função ou diversas funções à conta de administrador.

O aplicativo atribui as funções à conta de administrador.

Configuração de direitos de acesso no nível do objeto

Além de atribuir os direitos de acesso no nível de uma área funcional, é possível configurar o acesso a objetos específicos no Servidor de Administração virtual, por exemplo, para um grupo de administração específico ou uma tarefa. Para isso, alterne para o Servidor de Administração virtual e configure os direitos de acesso nas propriedades do objeto.

Alterar o Servidor de Administração para dispositivos clientes

É possível alterar o Servidor de Administração que gerencia os dispositivos cliente por outro, usando a tarefa *Alterar o Servidor de Administração*. Após a conclusão da tarefa, os dispositivos clientes selecionados serão colocados sob o gerenciamento do Servidor de Administração especificado por você.

Não é possível usar a tarefa *Alterar o Servidor de Administração* para dispositivos cliente conectados ao Servidor de Administração por meio de gateways de conexão. Para esses dispositivos, é necessário reconfigurar o Agente de Rede ou reinstalar o Agente de Rede e especificar o gateway de conexão.

Para alterar o Servidor de Administração que gerencia dispositivos cliente para outro servidor:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na etapa **Nova tarefa** do assistente, especifique as seguintes configurações:

   a. Na lista suspensa **Aplicativo**, selecione **Kaspersky Security Center**.

   b. No campo **Tipo de tarefa**, selecione **Alterar o Servidor de Administração**.

   c. No campo **Nome da tarefa**, especifique o nome para a tarefa que vai criar.

      O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).

   d. Selecione os dispositivos aos quais a tarefa será atribuída:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

     Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

     Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

   - **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**

     Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

     Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

   - **Atribuir a tarefa a uma seleção de dispositivos**

     A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

     Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

4. Na etapa **Escopo da tarefa** do assistente, especifique um grupo de administração, dispositivos com endereços específicos ou uma seleção de dispositivos gerenciados.

5. Na próxima etapa do assistente, confirme que concorda com os termos de alteração do Servidor de Administração para dispositivos do cliente.

6. Na próxima etapa do assistente, selecione o Servidor de Administração que deseja usar para gerenciar os dispositivos selecionados:

- Mudar para outro Servidor de Administração principal

  Para mover dispositivos cliente para outro Servidor de Administração principal, especifique as seguintes configurações de conexão do Servidor de Administração:

  1. No campo **Endereço do Servidor de Administração**, especifique o endereço do novo Servidor de Administração principal.
  2. No campo **Número da porta**, especifique o número da porta para conexão com o Servidor de Administração.

     O número da porta padrão é 14000.
  3. No campo **Porta SSL**, especifique o número da porta SSL no Servidor de Administração principal.

     O número da porta padrão é 13000.
  4. Se necessário, ative a opção **Usar o servidor proxy**.

     Se essa opção estiver desativada, a conexão direta será usada para conectar o dispositivo ao Servidor de Administração.

     Se essa opção estiver ativada, especifique os parâmetros do servidor proxy:

     - **Endereço do servidor proxy**
     - **Porta do servidor proxy**

     Se o servidor proxy exigir autenticação, nos campos **Nome do usuário** e **Senha**, especifique as credenciais da conta sob a qual a conexão com o servidor proxy será estabelecida. Recomendamos que você especifique as credenciais de uma conta que tenha privilégios mínimos necessários apenas para a autenticação do servidor proxy.
  5. Se necessário, carregue um novo certificado do Servidor de Administração.

- Mudar para outro Servidor de Administração virtual neste Servidor principal

  Selecione essa opção para mover dispositivos cliente para o Servidor de Administração virtual no Servidor de Administração principal atual. Para fazer isso, na lista suspensa **Nome do Servidor de Administração virtual**, selecione o Servidor de Administração virtual desejado.

7. Na etapa **Selecionar uma conta para executar a tarefa**, especifique as configurações da conta:

   - **Conta padrão**

     A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

     Por padrão, esta opção está selecionada.

   - **Especificar conta**

     Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

     - **Conta**

       Conta sob a qual a tarefa é executada.

     - **Senha**

       Senha da conta sob a qual a tarefa será executada.

8. Se você quiser alterar as configurações padrão da tarefa, na etapa **Concluir a criação da tarefa** do assistente, ative a opção **Abrir detalhes da tarefa quando a criação for concluída**.

   Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode alterar as configurações padrão depois, a qualquer momento.

9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.

10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

11. Se você quiser alterar as configurações padrão da tarefa, na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com suas necessidades.

12. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

13. Execute a tarefa criada.

Após a conclusão da tarefa, os dispositivos cliente, para os quais a mesma foi criada, são colocados sob gerenciamento pelo Servidor de Administração especificado nas configurações da tarefa.

Excluindo um Servidor de Administração virtual

Ao excluir um Servidor de Administração virtual, todos os objetos criados no Servidor de Administração, incluindo políticas e tarefas, também são excluídos. Os dispositivos gerenciados dos grupos de administração gerenciados pelo Servidor de Administração virtual serão removidos dos grupos de administração. Para retornar os dispositivos sob gerenciamento do Kaspersky Security Center, execute a sondagem de rede e migre os dispositivos encontrados do grupo Dispositivos não atribuídos para os grupos de administração.

Para excluir um Servidor de Administração virtual:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.
2. Na página que se abre, prossiga para a guia **Servidores de Administração**.
3. Selecione o Servidor de Administração virtual que deseja excluir.
4. Na linha do menu, clique no botão **Excluir**.

O Servidor de Administração virtual é excluído.

Ativando a proteção da conta contra modificações não autorizadas

Você pode ativar uma opção adicional para proteger uma conta de usuário contra modificações não autorizadas. Se essa opção for ativada, a modificação das configurações da conta do usuário requer autorização do usuário com direitos para modificação.

Para ativar ou desativar a proteção da conta contra modificações não autorizadas:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Clique no nome da conta de usuário interno para a qual você deseja especificar a proteção da conta contra modificações não autorizadas.
3. Na janela aberta de configurações do usuário, clique na guia **Proteção da conta**.
4. Na guia **Proteção da conta**, selecione a opção **Solicitar autenticação para verificar permissão para modificar contas de usuário** se quiser solicitar credenciais sempre que as configurações de conta forem alteradas ou modificadas. Caso contrário, selecione a opção **Permitir que os usuários modifiquem esta conta sem autenticação adicional**.
5. Clique no botão **Salvar**.

A proteção da conta contra modificação não autorizada está ativada para uma conta de usuário.

Verificação em duas etapas

Esta seção descreve como você pode usar a verificação em duas etapas para reduzir o risco de acesso não autorizado ao Kaspersky Security Center Web Console.

Sobre a verificação em duas etapas

Quando a verificação em duas etapas estiver ativada para uma conta, um código de segurança de uso único é necessário, além do nome de usuário e senha, para fazer login no Console de Administração ou no Kaspersky Security Center Web Console. Com a autenticação do domínio ativada, o usuário precisa inserir apenas o código de segurança de uso único.

Para usar a verificação em duas etapas, instale um app autenticador que gere códigos de segurança de uso único no dispositivo móvel ou computador. É possível usar qualquer aplicativo compatível com o Algoritmo de Senha Avulsa por Tempo Limitado (TOTP), como:

- Autenticador do Google
- Autenticador da Microsoft
- Bitrix24 OTP
- Chave Yandex
- Autenticador da Avanpost
- Aladdin 2FA

Para verificar se o Kaspersky Security Center é compatível com o app autenticador que deseja usar, ative a verificação em duas etapas para todos os usuários ou para um usuário específico.

Uma das etapas sugere a especificação do código de segurança gerado pelo app autenticador. Em caso de êxito, o Kaspersky Security Center será compatível com o autenticador selecionado.

É altamente recomendável salvar a chave secreta ou código QR e mantê-la em um lugar seguro. Isso ajudará a restaurar o acesso ao Kaspersky Security Center Web Console, caso o dispositivo móvel seja perdido.

Para proteger o uso do Kaspersky Security Center, você pode ativar a verificação em duas etapas para sua própria conta e depois ativá-la para todos os usuários.

Você pode excluir contas da verificação em duas etapas. Isso pode ser necessário para contas de serviço que não podem receber um código de segurança para autenticação.

Regras e limitações

Para ativar a verificação em duas etapas para todos os usuários e desativar a verificação em duas etapas para usuários específicos:

- Verifique e confirme se sua conta tem o direito de modificar ACLs de objetos na área funcional **Recursos gerais: permissões do usuário**.
- Ative a verificação em duas etapas para sua conta.

Para poder desativar a verificação em duas etapas para todos os usuários:

- Verifique e confirme se sua conta tem o direito de modificar ACLs de objetos na área funcional **Recursos gerais: permissões do usuário**.
- Faça login no Kaspersky Security Center Web Console usando a verificação em duas etapas.

Caso a verificação em duas etapas esteja ativada para uma conta de usuário no Servidor de Administração do Kaspersky Security Center versão 13 ou posterior, o usuário não poderá fazer login no Kaspersky Security Center Web Console das versões 12, 12.1 ou 12.2.

Reemissão da chave secreta

Qualquer usuário pode reemitir a chave secreta usada para a verificação em duas etapas. Quando um usuário fizer login no Servidor de Administração com a chave secreta reemitida, a nova chave secreta será salva para a conta de usuário. Caso o usuário insira a nova chave secreta incorreta, a nova chave secreta não será salva e a chave secreta atual permanecerá válida.

Um código de segurança possui um identificador conhecido como *nome do emissor*. O nome do emissor do código de segurança é usado como um identificador do Servidor de Administração no app autenticador. O nome do emissor do código de segurança possui um valor padrão que é igual ao nome do Servidor de Administração. Você pode alterar o nome do emissor do código de segurança. Caso você tenha alterado o nome do emissor do código de segurança, será necessário emitir uma nova chave secreta e passá-la para o app autenticador.

Configuração da verificação em duas etapas para todos os usuários

Este cenário descreve como ativar a verificação em duas etapas para todos os usuários e como excluir contas de usuário da verificação em duas etapas. Se você não ativou a verificação em duas etapas para sua conta antes de ativá-la para outros usuários, o aplicativo abre a janela para ativando a verificação em duas etapas para sua própria conta, primeiro. Este cenário também descreve como ativar a verificação em duas etapas para a sua própria conta.

Se você ativou a verificação em duas etapas para sua conta, pode prosseguir para a ativação da verificação em duas etapas para todos os usuários.

Pré-requisitos

Antes de começar:

- Certifique-se de que sua conta de usuário tenha o direito de Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões de usuário** para modificar as configurações de segurança para contas de outros usuários.
- Verifique e confirme se os outros usuários do Servidor de Administração instalaram um app autenticador em seus dispositivos.

Fases

Ativar a verificação em duas etapas para todos os usuários é feita com os seguintes passos:

1. **Instalação de um app autenticador em um dispositivo**

   É possível instalar qualquer aplicativo compatível com o Algoritmo de Senha Avulsa por Tempo Limitado (TOTP), como:

   - Autenticador do Google
   - Autenticador da Microsoft
   - Bitrix24 OTP
   - Chave Yandex
   - Autenticador da Avanpost
   - Aladdin 2FA

   Para verificar se o Kaspersky Security Center é compatível com o app autenticador que deseja usar, ative a verificação em duas etapas para todos os usuários ou para um usuário específico.

   Uma das etapas sugere a especificação do código de segurança gerado pelo app autenticador. Em caso de êxito, o Kaspersky Security Center será compatível com o autenticador selecionado.

   > É altamente recomendável não instalar o app autenticador no mesmo dispositivo no qual a conexão com o Servidor de Administração é estabelecida.

2. **Sincronização da hora do app autenticador com a hora do dispositivo no qual o Servidor de Administração está instalado**

   Verifique e confirme se a hora no dispositivo com o app autenticador e a hora no dispositivo com o Servidor de Administração estão sincronizadas com UTC usando fontes de tempo externas. Caso contrário, falhas podem ocorrer durante a autenticação e a ativação da verificação em duas etapas.

3. **Ativando a verificação em duas etapas para sua conta e recebendo a chave secreta para sua conta**

   Instruções de como proceder:

   - Para o Console de Administração baseado em MMC: Ativando a verificação em duas etapas para sua própria conta
   - Para Kaspersky Security Center Web Console: Ativando a verificação em duas etapas para sua própria conta

   Após ativar a verificação em duas etapas para sua conta, você pode fazer a verificação em duas etapas para todos os usuários.

4. **Ativando a verificação em duas etapas para todos os usuários**

   Os usuários com a verificação em duas etapas ativada devem usá-la para fazer login no Servidor de Administração.

   Instruções de como proceder:

   - Para o Console de Administração baseado em MMC: Ativando a verificação em duas etapas para todos os usuários
   - Para Kaspersky Security Center Web Console: Ativando a verificação em duas etapas para todos os usuários

5. **Editando o nome de um emissor do código de segurança**

Se você tiver vários Servidores de Administração com nomes semelhantes, pode ser necessário alterar os nomes do emissor do código de segurança para melhor identificação de diferentes Servidores de Administração.

Instruções de como proceder:

- Para Console de Administração baseado em MMC: Editando o nome de um emissor de código de segurança
- Para Kaspersky Security Center Web Console: Editando o nome de um emissor de código de segurança

6. **Excluindo contas de usuário para as quais você não precisa ativar a verificação em duas etapas**

   Caso necessário, exclua os usuários da verificação em duas etapas. Os usuários com contas excluídas não precisam usar a verificação em duas etapas para fazer login no Servidor de Administração.

   Instruções de como proceder:

   - Para Console de Administração baseado em MMC: Excluindo contas da verificação em duas etapas
   - Para Kaspersky Security Center Web Console: Excluindo contas da verificação em duas etapas

7. **Configurando a verificação em duas etapas para sua própria conta**

   Caso os usuários não sejam excluídos da verificação em duas etapas e ela ainda não tenha sido configurada para suas contas, eles precisarão configurá-la na janela aberta ao fazer login no Kaspersky Security Center. Do contrário, eles não poderão acessar o Servidor de Administração de acordo com seus direitos.

   Instruções de como proceder:

   - Para o Console de Administração baseado em MMC: configurando a verificação em duas etapas para sua própria conta
   - Para Kaspersky Security Center Web Console: configuração da verificação em duas etapas para sua própria conta

Resultados

Após a conclusão deste cenário:

- A verificação em duas etapas está ativada para a sua conta.
- A verificação em duas etapas é ativada para todas as contas de usuário do Servidor de Administração, exceto para contas de usuário excluídas.

Ativar a verificação em duas etapas para sua própria conta (Web Console)

Nesta etapa, você pode ativar a verificação em duas etapas apenas para sua própria conta.

Antes de ativar a verificação em duas etapas para sua conta, verifique e confirme se um app autenticador está instalado no dispositivo móvel. Verifique e confirme se a hora definida no app autenticador está sincronizada com a hora definida do dispositivo no qual o Servidor de Administração está instalado.

Para ativar a verificação em duas etapas para uma conta de usuário:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Clique no nome da sua conta.
3. Na janela aberta de configurações do usuário, clique na guia **Segurança de autenticação**.
4. Na guia **Segurança de autenticação**:
   a. Selecione a opção **Solicitar nome de usuário, senha e código de segurança (verificação em duas etapas)**. Clique no botão **Salvar**.
   b. Na janela de verificação em duas etapas que se abre, clique em **Veja como configurar a verificação em duas etapas**.
      Insira a chave secreta no app autenticador ou clique em **Ver código QR** e leia o código QR pelo app autenticador no dispositivo móvel para receber o código de segurança de uso único.
   c. Na janela de verificação em duas etapas, especifique o código de segurança gerado pelo app autenticador e clique no botão **Verificar e aplicar**.
5. Clique no botão **Salvar**.

A verificação em duas etapas está ativada para a sua conta.

Ativar a verificação em duas etapas obrigatória para todos os usuários (Web Console)

Você pode ativar a verificação em duas etapas para todos os usuários do Servidor de Administração se sua conta tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões do usuário** e se você fizer a autenticação usando a verificação em duas etapas.

Para ativar a verificação em duas etapas para vários usuários:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.
   A janela Propriedades do Servidor de Administração é aberta.
2. Na guia **Segurança de autenticação** da janela de propriedades, mude o botão seletor da opção de **verificação em duas etapas para todos os usuários** para a posição ativada.
3. Caso não tenha ativado a verificação em duas etapas para sua conta, o aplicativo abre a janela para ativar a verificação em duas etapas para sua própria conta.
   a. Na janela de verificação em duas etapas, clique em **Veja como configurar a verificação em duas etapas**.
   b. Insira a chave secreta no aplicativo autenticador manualmente ou clique em **Ver código QR** e leia o código QR pelo aplicativo autenticador em seu dispositivo móvel para receber o código de segurança de uso único.
   c. Na janela de verificação em duas etapas, especifique o código de segurança gerado pelo aplicativo autenticador e clique no botão **Verificar e aplicar**.

A verificação em duas etapas está ativada para todos os usuários. A partir de agora, os usuários do Servidor de Administração, incluindo os usuários que foram adicionados após ativar a verificação em duas etapas para todos os usuários, devem configurar a verificação em duas etapas para suas contas, exceto os usuários excluídos do processo.

Desativar a verificação em duas etapas para uma conta de usuário (Web Console)

Você pode desativar a verificação em duas etapas para sua própria conta, bem como para contas de quaisquer outros usuários.

É possível desativar a verificação em duas etapas da conta de outro usuário se sua conta tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões do usuário** e se a autenticação for feita com o uso da verificação em duas etapas.

Para desativar a verificação em duas etapas para uma conta de usuário:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Clique no nome da conta de usuário interna para a qual deseja desativar a verificação em duas etapas. Esta pode ser sua própria conta ou a de qualquer outro usuário.
3. Na janela aberta de configurações do usuário, clique na guia **Proteção da conta**.
4. Na guia **Proteção da conta**, selecione a opção **Solicitar apenas nome de usuário e senha** se deseja desativar a verificação em duas etapas para uma conta de usuário.
5. Clique no botão **Salvar**.

A verificação em duas etapas é desativada para a conta do usuário.

Caso queira restaurar o acesso de um usuário que não pode fazer login no Kaspersky Security Center Web Console com o uso da verificação em duas etapas, desative a verificação em duas etapas para essa conta de usuário e selecione a opção **Solicitar apenas nome de usuário e senha**, conforme descrito acima. Depois disso, faça login no Kaspersky Security Center Web Console com a conta de usuário para a qual a verificação em duas etapas foi desativada e, em seguida, ative a verificação novamente.

Desativar a verificação obrigatória em duas etapas para todos os usuários (Web Console)

É possível desativar a verificação em duas etapas obrigatória para todos os usuários caso o recurso esteja ativado para sua conta e ela tenha o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões de usuário**. Se a verificação em duas etapas não estiver ativada, você deve ativar a verificação em duas etapas para a sua conta antes de desativá-la para todos os usuários.

Para desativar a verificação em duas etapas:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Segurança de autenticação** da janela de propriedades, mude o botão seletor da opção **verificação em duas etapas para todos os usuários** para a posição desativada.

A verificação em duas etapas está desativada para todos os usuários. A desativação da verificação em duas etapas para todos os usuários não se aplica a contas específicas para as quais a verificação em duas etapas foi anteriormente ativada separadamente.

Excluindo contas da verificação em duas etapas

Você pode excluir contas de usuário da verificação em duas etapas se tiver o direito Modificar ACLs de objeto na área funcional **Recursos gerais: Permissões de usuário**.

Se uma conta de usuário for excluída da lista de verificação em duas etapas para todos os usuários, esse usuário não precisará usar a verificação em duas etapas.

> A exclusão de contas da verificação em duas etapas pode ser necessária para contas de serviço que não podem passar o código de segurança durante a autenticação.

Se deseja excluir algumas contas de usuário da verificação em duas etapas:

1. Você deve executar a sondagem do Active Directory para atualizar a lista de usuários do Servidor de Administração, se desejar excluir contas do Active Directory.

2. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

3. Na guia **Segurança de autenticação** da janela de propriedades, na tabela de exclusões da verificação em duas etapas, clique no botão **Adicionar**.

4. Na janela aberta:

   a. selecione as contas de usuário que deseja exportar.

   b. Clique no botão **OK**.

As contas de usuário selecionadas são excluídas da verificação em duas etapas.

Gerando uma nova chave secreta

Você pode gerar uma nova chave secreta para verificação em duas etapas para sua conta apenas tiver autorização para usar esse recurso.

Para gerar uma nova chave secreta para uma conta de usuário:

1. No menu principal, vá para **Usuários e funções → Usuários**.
2. Clique no nome da conta de usuário para a qual você deseja gerar uma nova chave secreta para a verificação em duas etapas.
3. Na janela aberta de configurações do usuário, clique na guia **Proteção da conta**.
4. Na guia **Proteção da conta**, clique no link **Gerar uma nova chave secreta**.
5. Na janela aberta de verificação em duas etapas, especifique uma nova chave de segurança gerada pelo app autenticador.
6. Clique no botão **Verificar e aplicar**.

Uma nova chave secreta é gerada para o usuário.

Em caso de perda do dispositivo móvel, é possível instalar um aplicativo autenticador em outro dispositivo e gerar uma nova chave secreta para restaurar o acesso ao Kaspersky Security Center Web Console.

Editar o nome de um emissor do código de segurança (Web Console)

Você pode ter várias tags (chamadas de emissores) para diferentes Servidores de Administração. Você pode alterar o nome de um emissor de código de segurança no caso, por exemplo, se o Servidor de Administração já usa um nome semelhante de emissor para outro Servidor de Administração. Por padrão, o nome de um emissor de código de segurança é igual ao nome do Servidor de Administração.

Depois de alterar o nome do emissor do código de segurança, será necessário emitir novamente uma nova chave secreta e passá-la para o app autenticador.

Para especificar um novo nome de emissor do código de segurança:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.
2. Na janela aberta de configurações do usuário, clique na guia **Proteção da conta**.
3. Na guia **Proteção da conta**, clique no link **Editar**.

   A seção **Editar emissor do código de segurança** é aberta.
4. Especifique um novo nome de emissor do código de segurança.
5. Clique no botão **OK**.

Um novo nome de emissor de código de segurança é especificado para o Servidor de Administração.

Configurar a verificação em duas etapas para sua própria conta (Web Console)

Na primeira vez que o usuário fizer login no Kaspersky Security Center depois que a verificação em duas etapas estiver ativada, a janela para configurar a verificação em duas etapas para sua própria conta será aberta.

Antes de ativar a verificação em duas etapas para sua conta, verifique e confirme se o aplicativo autenticador está instalado no seu dispositivo móvel.

Verifique e confirme se a hora no dispositivo com o app autenticador e a hora no dispositivo com o Servidor de Administração estão sincronizadas com UTC usando fontes de tempo externas.

Para configurar a verificação em duas etapas para sua conta:

1. Gere um código de segurança de uso único usando o aplicativo autenticador em seu dispositivo móvel. Para fazer isso, execute um das seguintes ações:

   - Insira manualmente a chave secreta no app autenticador.
   - Clique em **Ver código QR** e leia o código QR usando o app autenticador.

   Um código de segurança será exibido no dispositivo móvel.

2. Na janela de configuração da verificação em duas etapas, especifique o código de segurança gerado pelo app autenticador e clique no botão **Verificar e aplicar**.

A verificação em duas etapas está configurada para a sua conta. É possível acessar o Servidor de Administração de acordo com seus direitos.

Cópia backup e restauração dos dados do Servidor de Administração

O backup de dados permite mover um Servidor de Administração de um dispositivo para outro, sem perda de dados. Usando o backup, você pode restaurar dados ao mover o banco de dados de um Servidor de Administração para outro dispositivo ou ao atualizar para uma versão mais recente do Kaspersky Security Center. Além disso, é possível usar o backup de dados para mover dados do Servidor de Administração do Kaspersky Security Center Windows sob gerenciamento do Kaspersky Security Center Linux (não há suporte para mover dados do Kaspersky Security Center Linux para o Kaspersky Security Center Windows).

Observe que não é feito backup dos plugins de gerenciamento instalados. Depois de restaurar os dados do Servidor de Administração a partir de uma cópia backup, você precisará fazer download e reinstalar plug-ins para aplicativos gerenciados.

Antes de fazer backup dos dados do Servidor de Administração, verifique se um Servidor de Administração virtual foi adicionado ao grupo de administração. Caso um Servidor de Administração virtual seja adicionado, verifique e confirme se um administrador foi atribuído para esse Servidor de Administração virtual antes do backup. Não é possível conceder ao administrador direitos de acesso ao Servidor de Administração virtual após o backup. Observe que, caso as credenciais da conta do administrador sejam perdidas, não será possível atribuir um novo administrador ao Servidor de Administração virtual.

Você pode criar uma cópia backup dos dados do Servidor de Administração em uma das seguintes formas:

- Criando e executando uma tarefa de backup de dados através do Console de Administração.
- Executando o utilitário klbackup no dispositivo que tenha o Servidor de Administração instalado. Este utilitário está incluído no kit de distribuição do Kaspersky Security Center. Após a instalação do Servidor de Administração, o utilitário estará localizado na raiz da pasta de destino especificada na instalação do aplicativo.

Os seguintes dados são salvos em uma cópia backup do Servidor de Administração:

- O banco de dados do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração).
- Detalhes da configuração da estrutura dos grupos de administração e dispositivos cliente.
- Repositório dos pacotes de distribuição de aplicativos para a instalação remota.
- Certificado do Servidor de Administração.

A recuperação dos dados do Servidor de Administração só é possível usando o utilitário klbackup.

Reemissão do certificado do Kaspersky Security Center Web Console

A maioria dos navegadores impõe um limite no prazo de validade de um certificado. Para se enquadrar neste limite, o prazo de validade do certificado do Kaspersky Security Center Web Console é limitado a 397 dias. Você pode substituir um certificado existente recebido de uma autoridade de certificação (CA) emitindo um novo certificado autoassinado manualmente. Como alternativa, você pode emitir novamente o certificado expirado do Kaspersky Security Center Web Console.

A reemissão automática do certificado do Kaspersky Security Center Web Console não é compatível. É necessário reemitir manualmente o certificado expirado.

Se você já usa um certificado autoassinado, também é possível emiti-lo novamente atualizando o Kaspersky Security Center Web Console por meio do procedimento padrão da opção do instalador (**Efetuar upgrade**).

Quando o Web Console é aberto, o navegador pode informar que a conexão com o Web Console não é privada e o certificado do Web Console é inválido. Essa advertência aparece porque o certificado do Web Console é autoassinado e gerado automaticamente pelo Kaspersky Security Center. Para remover ou evitar esse aviso, é possível fazer o seguinte:

- Especifique um certificado personalizado ao reemiti-lo (opção recomendada). Crie um certificado confiável na infraestrutura e que atenda aos requisitos para certificados personalizados.
- Adicione o certificado do Web Console na lista de certificados de navegador confiáveis depois de reemiti-lo. Recomendamos usar essa opção somente se não puder criar um certificado personalizado.

Para emitir um novo certificado ao instalar o Kaspersky Security Center Web Console pela primeira vez:

1. Execute a instalação de rotina do Kaspersky Security Center Web Console.
2. Quando você chegar na etapa do Assistente de Instalação **Certificado de cliente**, selecione a opção **Gerar novo certificado** e, em seguida, clique no botão **Avançar**.
3. Avance pelas etapas restantes do Assistente de instalação até concluir a instalação.

   Um novo certificado para o Kaspersky Security Center Web Console é emitido com prazo de validade de 397 dias.

Para reemitir o certificado expirado do Kaspersky Security Center Web Console:

1. Em uma conta com direitos de administrador, execute o arquivo de instalação ksc-web-console-<número da versão>.<número da compilação>.exe.
2. Na janela do Assistente de instalação que se abre, selecione um idioma e clique em **OK**.
3. Na janela de boas-vindas, selecione a opção **Reemitir o certificado** e, em seguida, clique em **Avançar**.
4. Na próxima etapa, aguarde até que a reconfiguração do Kaspersky Security Center Web Console seja concluída e, então, clique em **Concluir**.

   O certificado do Kaspersky Security Center Web Console é reemitido por outro período de validade de 397 dias.

Se você usar o Gerenciador de Identidade e Acesso, também deve emitir novamente todos os certificados TLS para as portas que usadas pelo Gerenciador de Identidade e Acesso. O Kaspersky Security Center Web Console exibe uma notificação quando um certificado expira. Você deve seguir as instruções de notificação.

Criação de uma tarefa de backup de dados

As tarefas de backup são tarefas do Servidor de Administração; elas são criadas por meio do Assistente de início rápido. Se uma tarefa de backup criada pelo Assistente de início rápido tiver sido excluída, você pode criar uma manualmente.

Para criar uma tarefa de backup de dados do Servidor de Administração:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia.
3. Na janela **Nova tarefa** do assistente, selecione o tipo de tarefa chamado **Backup de dados do Servidor de Administração**.
4. Siga o restante das instruções do assistente.

A tarefa **Backup de dados do Servidor de Administração** pode ser criada somente em uma cópia única. Se a tarefa de backup de dados do Servidor de Administração já tiver sido criada para o Servidor de Administração, ela não será exibida na janela de seleção de tipo de tarefa do Assistente de criação da tarefa de backup.

Para configurar a tarefa Backup de dados do Servidor de Administração:

1. No menu principal, vá para **Dispositivos** → **Tarefas** e selecione a tarefa **Backup de dados do Servidor de Administração**.
2. Clique na tarefa **Backup de dados do Servidor de Administração**.

   A janela de propriedades da tarefa é aberta.
3. Se necessário, especifique as configurações gerais da tarefa de acordo com suas necessidades.
4. Na seção **Configurações do aplicativo**, especifique o caminho para a pasta para armazenamento de cópias backup dos dados do Servidor de Administração, defina a senha de proteção de backup e o número de cópias backup, se necessário.
5. Clique em **Salvar** para aplicar as alterações.

A tarefa *Backup de dados do Servidor de Administração* está configurada.

Mover Servidor de Administração para outro dispositivo

Se precisar usar o Servidor de Administração em um novo dispositivo, poderá movê-lo de uma das seguintes maneiras:

- Mova o Servidor de Administração e o servidor de banco de dados para um novo dispositivo (o servidor de banco de dados pode ser instalado no novo dispositivo juntamente com o Servidor de Administração ou em outro dispositivo).
- Mantenha o servidor de banco de dados no dispositivo anterior e mova apenas o Servidor de Administração para um novo dispositivo.

Para mover o Servidor de Administração e um servidor de banco de dados para um novo dispositivo:

1. No dispositivo anterior, crie um backup de dados do Servidor de Administração.

   Para fazer isso, você pode executar a tarefa de backup de dados por meio do Kaspersky Security Center Web Console ou executar o utilitário klbackup.

   > Se você usa o SQL Server como um DBMS para o Servidor de Administração, é possível migrar os dados do SQL Server para o MySQL ou o MariaDB DBMS. Para fazer isso, execute o utilitário klbackup no modo interativo para criar um backup de dados. Ative a opção **Migrar para o formato MySQL/MariaDB** na janela **Configurações de backup** do Assistente de backup e restauração. O Kaspersky Security Center criará um backup compatível com o MySQL e o MariaDB. Depois disso, é possível restaurar os dados do backup para o MySQL ou o MariaDB.

   > Você também pode ativar a opção **Migrar para o formato do Azure** se você quiser migrar os dados do SQL Server para o Azure SQL DBMS.

2. No dispositivo anterior, desconecte o Servidor de Administração da rede.

3. Selecione um novo dispositivo no qual instalar o Servidor de Administração. Certifique-se de que o hardware e o software do dispositivo selecionado atendam aos requisitos para Servidor de Administração, Kaspersky Security Center Web Console e Agente de Rede. Verifique também se as portas usadas no Servidor de Administração estão disponíveis.

4. Atribua o mesmo endereço ao novo dispositivo.

   O novo Servidor de Administração pode ser atribuído ao nome NetBIOS, FQDN e endereço IP estático. Isso depende de qual endereço do Servidor de Administração foi definido no pacote de instalação do Agente de Rede quando os Agentes de Rede foram implementados. Como alternativa, é possível usar o endereço de conexão que determina o Servidor de Administração ao qual o Agente de Rede se conecta (esse endereço pode ser obtido em dispositivos gerenciados usando o utilitário klnagchk).

5. Caso necessário, em outro dispositivo, instale o sistema de gerenciamento de banco de dados (DBMS) a ser usado pelo Servidor de Administração.

   O banco de dados pode ser instalado no novo dispositivo juntamente com o Servidor de Administração ou em outro dispositivo. Verifique e confirme se este dispositivo atende aos requisitos de hardware e software. Ao selecionar um DBMS, considere o número de dispositivos cobertos pelo Servidor de Administração.

6. Execute a instalação do Servidor de Administração no novo dispositivo.

7. Durante a instalação do Servidor de Administração, defina as configurações de conexão do servidor de banco de dados.



Exemplo da janela de configurações de conexão para Microsoft SQL Server

Dependendo de onde você precisa localizar o servidor de banco de dados, siga um destes procedimentos:

- Mantenha o servidor de banco de dados no dispositivo anterior

  1. Clique no botão **Procurar** ao lado do campo **Nome da instância do SQL Server** e, em seguida, selecione o nome do dispositivo anterior na lista que aparece.

     Observe que o dispositivo anterior deve estar disponível para conexão com o novo Servidor de Administração.

  2. Digite o nome do banco de dados anterior no campo **Nome do banco de dados**.

- Mova o servidor de banco de dados para outro dispositivo

  1. Clique no botão **Procurar** ao lado do campo **Nome da instância do SQL Server** e, em seguida, selecione o novo nome do dispositivo na lista que aparece.

  2. Digite o novo nome do banco de dados no campo **Nome do banco de dados**.

     Observe que o novo nome do banco de dados deve corresponder ao nome do banco de dados do dispositivo anterior. Os nomes dos bancos de dados devem ser idênticos, para que você possa usar o backup do Servidor de Administração. O nome padrão do banco de dados é *KAV*.

8. Após a conclusão da instalação, recupere os dados do Servidor de Administração no novo dispositivo usando o utilitário klbackup.

   Se usar o SQL Server como um DBMS nos dispositivos anteriores e novos, observe que a versão do SQL Server instalada no novo dispositivo deverá ser igual ou posterior à versão do SQL Server instalada no dispositivo anterior. Caso contrário, não será possível recuperar os dados do Servidor de Administração no novo dispositivo.

9. Abra o Kaspersky Security Center Web Console e conecte-se ao Servidor de Administração.

10. Verifique se todos os dispositivos gerenciados estão conectados com o Servidor de Administração.

11. Desinstale o Servidor de Administração e o servidor de banco de dados do dispositivo anterior.

Você também pode usar o Console de Administração para mover o Servidor de Administração e um servidor de banco de dados para outro dispositivo.

Verificar a integridade dos módulos usando os utilitários klscmodchk e integrity_checker

O Kaspersky Security Center contém vários módulos binários na forma de bibliotecas vinculadas dinamicamente, arquivos executáveis, arquivos de configuração e arquivos de interface. Os invasores podem substituir um ou mais módulos executáveis ou arquivos de aplicativos por outros arquivos contendo código malicioso. Para evitar a substituição de módulos e arquivos, o Kaspersky Security Center fornece uma verificação de integridade de componentes usando os utilitários klscmodchk e integrity_checker. Esses utilitários verificam módulos e arquivos em busca de alterações não autorizadas ou danos. Se um módulo ou arquivo de aplicativo tiver uma soma de verificação incorreta, ele será considerado danificado.

O utilitário klscmodchk executa verificações de integridade para os seguintes componentes do Kaspersky Security Center:

- Servidor de Administração
- Agente de Rede
- Plug-ins de gerenciamento para o Console de Administração com arquivos de manifesto

O utilitário integrity_checker executa verificações de integridade para os seguintes componentes do Kaspersky Security Center:

- Servidor de Administração
- Agente de Rede
- Kaspersky Security Center Web Console

Ambos os utilitários verificam a integridade do módulo com base no arquivo de manifesto kl_file_integrity_manifest.xml, que faz parte da compilação do Kaspersky Security Center e está localizado na pasta de instalação. O arquivo de manifesto do componente contém arquivos cuja integridade é importante para a operação correta do contêiner Kaspersky Security Center. A integridade dos próprios arquivos de manifesto também é verificada.

Não é recomendável, de forma alguma, modificar o arquivo de manifesto kl_file_integrity_manifest.xml, pois isso invalidará a assinatura digital e fará com que a verificação de integridade falhe.

Para verificar a integridade do componente do Kaspersky Security Center, execute um dos seguintes comandos:

- `$ klscmodchk [ parâmetros ]`

  O utilitário klscmodchk inicia o utilitário integrity_checker com o parâmetro `--verbose` e verifica a integridade dos módulos.

  Parâmetros para o utilitário klscmodchk:

  - `-logfile <caminho_do_arquivo_de_log>`: especifique o caminho para um arquivo no disco para registro. Por padrão, as informações são enviadas para o console.
  - `-chkplugins`: verifique a integridade dos módulos de plug-in de gerenciamento instalados para o Console de Administração que incluem arquivos de manifesto. Por padrão, os plug-ins de gerenciamento não são verificados.
  - `-verbose`: exibir informações detalhadas durante a verificação de integridade.

- `$ integrity_checker [ parâmetros ] <caminho_do_arquivo_de_manifesto>`

  Parâmetros para o utilitário integrity_checker:

  - `--help`: exibe a ajuda do utilitário integrity_checker.
  - `--version`: exibe a versão do utilitário integrity_checker.
  - `--verbose`: exibe informações sobre a operação do utilitário. Ao executar uma verificação de integridade, é suficiente usar esse parâmetro no comando.

O resultado da verificação de cada arquivo de manifesto é exibido ao lado do nome do arquivo de manifesto no seguinte formato:

- SUCESSO: integridade do arquivo confirmada (código de retorno 0).
- FALHA: integridade do arquivo não confirmada (código de retorno diferente de zero).

Instalação e configuração inicial do Kaspersky Security Center Web Console

Esta seção descreve as etapas necessárias para prosseguir depois da instalação do Kaspersky Security Center Web Console e executar a configuração inicial.

Assistente de início rápido (Kaspersky Security Center Web Console)

Esta seção fornece informações sobre o Assistente de início rápido do Servidor de Administração.

O assistente requer acesso à Internet. Se seu Servidor de Administração não tiver acesso à Internet, recomendamos executar todas as etapas do assistente manualmente por meio da interface do Kaspersky Security Center Web Console.

O Kaspersky Security Center lhe permite ajustar uma seleção mínima de configurações necessárias para criar um sistema de gerenciamento centralizado para proteger a rede contra ameaças à segurança. Esta configuração é executada por meio do Assistente de início rápido. Quando o assistente estiver em execução, você pode fazer as seguintes modificações ao aplicativo:

- Adicione arquivos de chaves ou insira códigos de ativação que podem ser distribuídas automaticamente para os dispositivos dentro de grupos de administração.
- Configure a interação com a Kaspersky Security Network (KSN). Se você permitiu o uso da KSN, o assistente ativa o serviço de servidor proxy da KSN que garante a conexão entre a KSN e os dispositivos.
- Defina entrega de notificações por e-mail sobre os eventos que ocorrem durantes a operação do Servidor de Administração e de aplicativos gerenciados (a entrega com êxito da notificação requer que o serviço Messenger continue a estar em execução no Servidor de Administração e nos dispositivos de todos os destinatários).
- Crie uma política de proteção para estações de trabalho e servidores, assim como tarefas de verificação de malwares, tarefas de download de atualização e tarefas de backup dos dados, para o nível superior da hierarquia de dispositivos gerenciados.

  O Assistente de início rápido cria políticas somente para aplicativos para os quais a pasta **Dispositivos gerenciados** não contém nenhuma política. O Assistente de início rápido não cria tarefas se algumas já tiverem sido criadas com os mesmos nomes para o nível superior da hierarquia dos dispositivos gerenciados.

O aplicativo solicita automaticamente que você execute o Assistente de início rápido após a instalação do Servidor de Administração, na primeira conexão a ele. Você também pode iniciar o Assistente de início rápido manualmente a qualquer momento.

Para iniciar o Assistente de Início Rápido manualmente:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Geral**.

3. Clique em **Iniciar o assistente de início rápido**.

O assistente solicita que você execute a configuração inicial do Servidor de Administração. Siga as instruções do Assistente. Prossiga pelo assistente usando o botão **Avançar**.

Etapa 1. Especificando as configurações de conexão da Internet

Especifique as configurações de acesso à Internet para o Servidor de Administração. Você deve configurar o acesso à Internet para usar a Kaspersky Security Network e baixar atualizações de bancos de dados antivírus para o Kaspersky Security Center e aplicativos Kaspersky gerenciados.

Ative a opção **Usar o servidor proxy** caso queira usar um servidor proxy para se conectar com a Internet. Caso essa opção esteja ativada, os campos estarão disponíveis para inserir as configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:

- **Endereço**

  Endereço do servidor proxy usado para conexão do Kaspersky Security Center à Internet.

- **Número da porta**

  Número da porta pela qual a conexão proxy do Kaspersky Security Center será estabelecida.

- **Ignorar servidor proxy para endereços locais**

  Nenhum servidor proxy será usado para conectar-se aos dispositivos na rede local.

- **Autenticação do servidor proxy**

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

  Este campo de entrada está disponível se a caixa de seleção **Usar o servidor proxy** estiver marcada.

- **Nome do usuário**

  Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

- **Senha**

  A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

  Para ver a senha inserida, mantenha pressionado o botão **Exibir** pelo tempo que você desejar.

É possível configurar o acesso à Internet posteriormente, de modo separado, a partir do assistente de início rápido.

Etapa 2. Download das atualizações necessárias

As atualizações necessárias são baixadas dos servidores da Kaspersky automaticamente.

Etapa 3. Seleção dos ativos a serem protegidos

Selecione as áreas de proteção e os sistemas operacionais que estão em uso na sua rede. Ao selecionar essas opções, você especifica os filtros para plugins de gerenciamento de aplicativos e pacotes de distribuição nos servidores da Kaspersky que podem ser baixados para instalação nos dispositivos clientes em sua rede.

Selecione as opções:

- **Áreas**

  Você pode selecionar as seguintes áreas de proteção:

  - **Estações de trabalho**. Selecione esta opção se desejar proteger as estações de trabalho na sua rede. Por padrão, a opção Estação de trabalho está selecionada.
  - **Servidores de arquivos e armazenamento**. Selecione esta opção se desejar proteger servidores de arquivos na sua rede.
  - **Dispositivos móveis**. Selecione esta opção se desejar proteger os dispositivos móveis pertencentes à empresa ou aos seus funcionários. Se você selecionar essa opção, mas não tiver fornecido uma licença com o recurso de Gerenciamento de Dispositivos Móveis, será exibida uma mensagem informando sobre a necessidade de fornecer uma licença com o recurso Gerenciamento de Dispositivos Móveis. Se você não fornecer uma licença, não poderá usar o recurso de dispositivo móvel.
  - **Virtualização**. Selecione esta opção se você quiser proteger máquinas virtuais em sua rede.
  - **Kaspersky Anti-Spam**. Selecione esta opção se desejar proteger os servidores de correio da sua organização contra spam, fraude e malware.
  - **Sistemas incorporados**. Selecione essa opção caso queira proteger os sistemas integrados baseados no Windows, como caixa eletrônico (ATM).
  - **Redes industriais**. Selecione essa opção caso queira monitorar os dados de segurança em sua rede industrial e os pontos de extremidade de rede protegidos por aplicativos Kaspersky.
  - **Endpoints industriais**. Selecione esta opção caso queira proteger nós individuais dentro da rede industrial.

- **Sistemas operacionais**

  Você pode selecionar as seguintes plataformas:

  - Microsoft Windows
  - macOS
  - Android
  - Linux
  - Outro

  Para obter informações sobre os sistemas operacionais compatíveis, consulte os Requisitos de hardware e software para o Kaspersky Security Center Web Console.

Você pode selecionar os pacotes de aplicativos Kaspersky na lista de pacotes disponíveis posteriormente, separadamente do Assistente de início rápido. Para simplificar a busca pelos pacotes necessários, é possível filtrar a lista de pacotes disponíveis por diversos critérios.

Etapa 4. Selecionar a criptografia em soluções

A janela **Criptografia em soluções** é exibida apenas se você tiver selecionado **Estações de trabalho** como escopo de proteção.

O Kaspersky Endpoint Security for Windows inclui ferramentas de criptografia para as informações armazenadas nos dispositivos cliente baseados em Windows. Essas ferramentas de criptografia têm Advanced Encryption Standard (AES) implementado com comprimento de chave de 256 ou 56 bits.

O download e o uso do pacote de distribuição com um comprimento de chave de 256 bits devem ser executados em conformidade com as leis e regulamentos aplicáveis. Para baixar um pacote de distribuição do Kaspersky Endpoint Security for Windows que seja válido para as necessidades da sua organização, consulte a legislação do país em que os dispositivos clientes da sua organização estejam localizados.

Na janela **Criptografia em soluções**, selecione um dos seguintes tipos de criptografia:

- Criptografia leve. Esse tipo de criptografia usa um comprimento de chave de 56 bits.
- Criptografia forte. Esse tipo de criptografia usa um comprimento de chave de 256 bits.

É possível selecionar o pacote de distribuição para o Kaspersky Endpoint Security for Windows com o tipo de criptografia necessário posteriormente, de modo separado, a partir do assistente de início rápido.

Etapa 5. Configurar a instalação dos plugins para os aplicativos gerenciados

Selecione os plugins para os aplicativos gerenciados a ser instalados. Uma lista de plugins localizados nos servidores da Kaspersky é exibida. A lista é filtrada de acordo com as opções selecionadas na etapa anterior do assistente. Por padrão, uma lista completa inclui plugins de todos os idiomas. Para exibir apenas o plugin de um idioma específico, use o filtro.

A lista de plugins inclui as seguintes colunas:

- **Área para proteger**

  As áreas selecionadas para receber proteção são exibidas nesta coluna.

- **Tipo**

  Os tipos de plug-in são exibidos nesta coluna.

- **Nome**

  Os plugins, dependendo das áreas de proteção e das plataformas que você selecionou na etapa anterior, são selecionados.

- **Versão**

  A lista inclui plugins de todas as versões colocadas nos servidores da Kaspersky. Por padrão, os plugins das versões mais recentes são selecionados.

- **Versão mais recente**

  Esta coluna indica se uma versão do plug-in é a mais recente. Caso o valor **true** seja exibido, o plug-in corresponde à versão mais recente. Se o valor **false** for exibido, o plug-in corresponde a uma versão posterior.

- **Sistema operacional**

  Essa coluna exibe os sistemas operacionais dos plug-ins.

- **Idioma**

  Por padrão, o idioma de localização de um plugin é definido pelo idioma do Kaspersky Security Center que você selecionou na instalação. Você pode especificar outros idiomas na lista suspensa **Mostrar o idioma localizado do Console de Administração ou**.

Após os plugins serem selecionados, clique em **Avançar** para iniciar a instalação.

É possível instalar os plug-ins de gerenciamento para aplicativos da Kaspersky manualmente, de modo separado do assistente de início rápido.

O assistente de início rápido instala automaticamente os plug-ins selecionados. Para instalar alguns plugins, você deve aceitar os termos do EULA. Leia o texto do EULA exibido, selecione, a caixa de seleção **Concordo em usar a Kaspersky Security Network** e clique no botão **Instalar**. Se você não aceitar os termos do EULA, o plugin não será instalado.

Quando todos os plugins selecionados estiverem instalados, o Assistente de início rápido direcionará você automaticamente para a próxima etapa.

Etapa 6. Baixando os pacote de distribuição e criando pacotes de instalação

Selecione os pacotes de distribuição para baixar.

As distribuições de aplicativos gerenciados podem exigir a instalação de uma versão mínima específica do Kaspersky Security Center.

Após selecionar um tipo de criptografia para o Kaspersky Endpoint Security for Windows, a lista dos pacotes de distribuição dos dois tipos de criptografia é exibida. Um pacote de distribuição com o tipo de criptografia selecionado está selecionado na lista. Você pode selecionar pacotes de distribuição de qualquer tipo de criptografia. O idioma do pacote de distribuição corresponde ao idioma do Kaspersky Security Center. Se não existir um pacote de distribuição do Kaspersky Endpoint Security for Windows para o idioma do Kaspersky Security Center, o pacote de distribuição em inglês será selecionado.

Para concluir o download de alguns pacotes de distribuição, você deve aceitar o EULA. Quando você clica no botão **Aceitar**, o texto do EULA é exibido. Para prosseguir para a próxima etapa do assistente, você deve aceitar os termos e condições do EULA e os termos e condições da Política de Privacidade da Kaspersky. Se você não aceitar os termos e condições, o download do pacote será cancelado.

Após aceitar os termos e condições do EULA e os termos e condições da Política de Privacidade da Kaspersky, o download dos pacotes de distribuição continua. Posteriormente, você pode suar os pacotes de instalação para implementar aplicativos Kaspersky em dispositivos cliente.

É possível baixar pacotes de distribuição e criar pacotes de instalação posteriormente, de modo separado, a partir do assistente de início rápido.

Etapa 7. Configurar a Kaspersky Security Network

Especifique as configurações para encaminhar informações sobre as operações do Kaspersky Security Center à Base de conhecimento da Kaspersky Security Network.

Selecione uma das seguintes opções:

- **Concordo em usar a Kaspersky Security Network**

  O Kaspersky Security Center e os aplicativos gerenciados instalados nos dispositivos cliente transferem automaticamente seus detalhes de operação para o Kaspersky Security Network. A participação na Kaspersky Security Network assegura atualizações mais rápidas dos bancos de dados que contêm informações sobre vírus e outras ameaças, que assegura uma resposta mais rápida a ameaças de segurança emergentes.

- **Não concordo em usar a Kaspersky Security Network**

  O Kaspersky Security Center e os aplicativos gerenciados não fornecerão informações ao Kaspersky Security Network.

  Se você selecionar esta opção, o uso da Kaspersky Security Network será desativado.

É possível configurar o acesso a Kaspersky Security Network (KSN) posteriormente, de modo separado, a partir do assistente de início rápido.

Etapa 8. Selecionando o método de ativação do aplicativo

Selecione uma das seguintes opções de ativação do Kaspersky Security Center:

- **Inserindo o seu código de ativação**

  Código de ativação é uma sequência única de 20 caracteres alfanuméricos. Você insere um código de ativação para adicionar uma chave que ativa o Kaspersky Security Center. Você recebe o código de ativação através do endereço de e-mail especificado após a compra do Kaspersky Security Center.

  Para ativar o aplicativo com um código de ativação, é necessário acesso à Internet para estabelecer a conexão com os servidores de ativação da Kaspersky.

  Caso tenha selecionado essa opção de ativação, é possível ativar a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

  Se esta opção estiver ativada, a chave de licença será implementada automaticamente para os dispositivos gerenciados.

  Se esta opção estiver desativada, você pode implementar a chave de licença para dispositivos gerenciados posteriormente, no nó **Licenças Kaspersky** na árvore do Console de Administração.

- **Especificando um arquivo de chave**

  O *Arquivo de chave* é um arquivo com a extensão .key fornecido a você pela Kaspersky. O objetivo do arquivo de chave é adicionar uma chave que ativa o aplicativo.

  Os métodos de obtenção de arquivos de chave são descritos na seção a seguir: Sobre o arquivo de chave.

  Para ativar o aplicativo usando um arquivo de chave, não é necessário conectar-se aos servidores de ativação da Kaspersky.

  Caso tenha selecionado essa opção de ativação, é possível ativar a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

  Se esta opção estiver ativada, a chave de licença será implementada automaticamente para os dispositivos gerenciados.

  Se esta opção estiver desativada, você pode implementar a chave de licença para dispositivos gerenciados posteriormente, no nó **Licenças Kaspersky** na árvore do Console de Administração.

- **Ao adiar a ativação do aplicativo**

  O aplicativo não funcionará com a funcionalidade básica, sem o Gerenciamento de Dispositivos Móveis e sem o Gerenciamento de patches e vulnerabilidades.

Se você decidiu adiar a ativação do aplicativo, poderá adicionar uma chave de licença depois a qualquer momento selecionando **Operações** → **Licenciamento**.

Ao trabalhar com o Kaspersky Security Center implementado via AMI paga ou em SKU com base em faturamento mensal, você não pode especificar um arquivo de chave ou inserir um código.

Etapa 9. Especificar as configurações de gerenciamento de atualização de terceiros

Esta etapa não será exibida se você não tiver a licença de Gerenciamento de patches e vulnerabilidades e se a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* já existir.

Para atualizações de software de terceiros, selecione uma das seguintes opções:

- **Pesquisar por atualizações necessárias**

  A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente, caso você não tenha uma.

  Esta opção está marcada por padrão.

- **Encontrar e instalar as atualizações necessárias**

  As tarefas *Encontrar as vulnerabilidades e as atualizações necessárias* e *Instalar as atualizações necessárias e corrigir vulnerabilidades* são criadas automaticamente, se ainda não existirem.

  Esta opção está disponível apenas sob a licença de Gerenciamento de patches e vulnerabilidades.

Para atualizações do Windows Update, selecione uma das seguintes opções:

- **Usar as origens de atualização definidas na política do domínio**

  Os dispositivos clientes baixarão as atualizações do Windows Update, de acordo com as configurações de diretiva de domínio. A política do Agente de Rede é criada automaticamente, se você não tiver uma.

- **Usar Servidor de Administração como servidor WSUS**

  Os dispositivos clientes baixarão as atualizações do Windows Update no Servidor de Administração. A tarefa *Executar a sincronização com o Windows Update* e a política do Agente de Rede são criadas automaticamente, se ainda não existirem.

  Esta opção está disponível apenas sob a licença de Gerenciamento de Patches e Vulnerabilidades.

É possível criar as tarefas *Encontrar vulnerabilidades e atualizações necessárias*, *Instalar as atualizações necessárias e corrigir as vulnerabilidades* separadamente a partir do assistente de início rápido. Para usar o Servidor de Administração como o servidor WSUS, crie a tarefa *Executar sincronização de atualização do Windows* e, então, selecione a opção **Usar Servidor de Administração como servidor WSUS** na política do Agente de Rede.

Etapa 10. Criar uma configuração básica de proteção de rede

Você poderá verificar a lista de políticas e tarefas que foram criadas.

Espere pela conclusão da criação de políticas e tarefas antes de prosseguir à etapa seguinte do assistente.

É possível criar as tarefas e as políticas necessárias posteriormente, separado do assistente de início rápido.

Etapa 11. Configurar notificações por e-mail

Configure a entrega de notificações sobre os eventos registrados durante a operação dos aplicativos Kaspersky em dispositivos clientes. Essas configurações serão usadas como as configurações padrão para as políticas de aplicativo.

Para configurar a entrega de notificações sobre os eventos que ocorrem nos aplicativos Kaspersky, use as seguintes configurações:

- **Destinatários (endereços de e-mail)**

  Os endereços de e-mail de usuários aos quais o aplicativo enviará notificações. Você pode inserir um ou vários endereços; se inserir mais de um endereço, separe-os com um ponto-e-vírgula.

- **Endereço do servidor SMTP**

  O endereço ou os endereços dos servidores de e-mail da sua organização.

  Se você inserir mais de um endereço, separe-os com um ponto-e-vírgula. Você pode usar os seguintes parâmetros:

  - Endereço IPv4 ou IPv6
  - Nome da rede Windows (nome NetBIOS) do dispositivo
  - Nome de DNS do servidor SMTP

- **Porta do servidor SMTP**

  Número da porta de comunicação do servidor SMTP. Se você usar vários servidores SMTP, a conexão com eles será estabelecida por meio da porta de comunicação especificada. O número da porta padrão é 25.

- **Usar a autenticação ESMTP**

  Ativa o suporte da autenticação ESMTP. Após selecionar a caixa de seleção, nos campos **Nome do usuário** e **Senha**, você poderá especificar as configurações de autenticação ESMTP. Por padrão, esta caixa de seleção está desmarcada.

- **Usar TLS**

Você pode especificar as configurações de TLS de conexão com um servidor SMTP:

- **Não usar TLS**

  Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.

- **Usar TLS se compatível com servidor SMTP**

  Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.

- **Sempre usar TLS e verificar a validade do certificado do servidor**

  Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

  > Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

  Se você selecionar o valor **Sempre usar TLS e verificar a validade do certificado do servidor**, pode especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar certificados para uma conexão TLS clicando no link **Especificar certificados**:

- Procurar por um arquivo de certificado do servidor SMTP:

  Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

- Procurar um arquivo de certificado de cliente:

  Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer autoridade de certificação confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

  - Certificado X-509:

    Você deve especificar um arquivo com o certificado e um arquivo com a chave privada. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Quando os dois arquivos são carregados, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

  - Contêiner pkcs12:

    Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

Você pode testar as novas configurações de notificação por e-mail clicando no botão **Enviar mensagem de teste**.

Também é possível configurar notificações de eventos posteriormente, de modo separado, a partir do assistente de início rápido.

Etapa 12. Executar uma pesquisa de rede

O Servidor de Administração executa uma sondagem inicial. Durante a amostragem, um barra de andamento é exibida. Quando a amostragem é concluída, o link **Visualizar dispositivos detectados** fica disponível. Você pode clicar nesse link para exibir dispositivos de rede detectados pelo Servidor de Administração. Para voltar ao Assistente de início rápido, pressione a tecla **Escape**.

É possível sondar a rede posteriormente, de modo separado, a partir do assistente de início rápido. Use o Kaspersky Security Center Web Console para configurar a sondagem de domínios do Windows, Active Directory, intervalos de IP e redes IPv6.

Etapa 13. Fechar o Assistente de início rápido

Na página de conclusão do assistente de início rápido, marque a caixa de seleção **Executar o Assistente de Implementação de Proteção** se quiser iniciar a instalação automática de aplicativos antivírus ou Agente de Rede em dispositivos na sua rede.

Para fechar o assistente, pressione o botão **Concluir**.

Conectando dispositivos fora do escritório

Esta seção descreve como conectar dispositivos externos (ou seja, dispositivos gerenciados localizados fora da rede principal) ao Servidor de Administração.

Cenário: Conectando dispositivos externos por meio de um gateway de conexão

Este cenário descreve como conectar dispositivos gerenciados localizados fora da rede principal ao Servidor de Administração.

Pré-requisitos

O cenário tem os seguintes prerrequisitos:

- Uma zona desmilitarizada (DMZ) é organizada na rede da organização.
- O Servidor de Administração do Kaspersky Security Center é implementado na rede corporativa.

Fases

O cenário segue em etapas:

1 **Selecionando um dispositivo cliente na DMZ**

Este dispositivo será usado como um gateway de conexão. O dispositivo selecionado deve atender aos requisitos de gateways de conexão.

2 **Instalando o Agente de Rede na função de gateway de conexão**

Recomendamos que você use a instalação local para instalar o Agente de Rede no dispositivo selecionado.

Por padrão, o arquivo de instalação está localizado em: \\<nome do servidor.>\KLSHARE\PkgInst\NetAgent_<número da versão>

Na janela **Gateway de conexão** do Assistente de Instalação do Agente de Rede, selecione **Usar o Agente de Rede como um gateway de conexão na DMZ**. Esse modo ativa simultaneamente a função de gateway de conexão e sinaliza ao Agente de Rede para aguardar as conexões do Servidor de Administração em vez de estabelecer conexões com o Servidor de Administração.

Alternativamente, você pode instalar o Agente de Rede em um dispositivo Linux e configurá-lo para funcionar como um gateway de conexão, mas atente para a lista de limitações do Agente de Rede em execução em dispositivos Linux.

3 **Permitindo conexões em firewalls no gateway de conexão**

Para certificar-se de que o Servidor de Administração pode realmente se conectar ao gateway de conexão na DMZ, permita conexões com a porta TCP 13000 em todos os firewalls entre o Servidor de Administração e o gateway de conexão.

Se o gateway de conexão não tiver um endereço IP real na Internet, mas estiver localizado atrás da Tradução de Endereço de Rede (NAT), configure uma regra para encaminhar as conexões por meio da NAT.

4 **Criando um grupo de administração para dispositivos externos**

Criar um novo grupo no grupo **Dispositivos gerenciados**. Esse novo grupo conterá dispositivos externos gerenciados.

5 **Conectando o gateway de conexão a um Servidor de Administração**

O gateway de conexão configurado está esperando por uma conexão vinda do Servidor de Administração. No entanto, o Servidor de Administração não lista o dispositivo com o gateway de conexão entre os dispositivos gerenciados. Isso ocorre porque o gateway de conexão não tentou estabelecer uma conexão com o Servidor de Administração. Portanto, você precisa de um procedimento especial para garantir que o Servidor de Administração inicie uma conexão com o gateway de conexão.

Faça o seguinte:

1. Adicione o gateway de conexão como um ponto de distribuição.
2. Mover o gateway de conexão do grupo **Dispositivos não atribuídos** para o grupo criado para os dispositivos externos.

O gateway de conexão está conectado e configurado.

6 **Conexão de dispositivos de desktop externos ao Servidor de Administração**

Normalmente, os dispositivos de desktop externos não são movidos dentro do perímetro. Portanto, você precisa configurá-los para se conectarem ao Servidor de Administração por meio do gateway ao instalar o Agente de Rede.

7 **Configuração de atualizações para os dispositivos de desktop externos**

Se as atualizações de aplicativos de segurança forem configuradas para serem baixadas do Servidor de Administração, os dispositivos externos baixarão as atualizações por meio do gateway de conexão. Isso apresenta duas desvantagens:

- Tráfego desnecessário é gerado, o que ocupa a largura de banda do canal de comunicação via Internet da empresa.
- Essa não é necessariamente a maneira mais rápida de obter atualizações. É muito provável que seja mais barato e rápido para os dispositivos externos receberem atualizações dos servidores de atualização Kaspersky.

Faça o seguinte:

1. Mova todos os dispositivos externos para o grupo de administração separado criado anteriormente.
2. Exclua o grupo com dispositivos externos da tarefa de atualização.
3. Crie uma tarefa de atualização separada para o grupo com dispositivos externos.

8 **Conectando laptops em trânsito ao Servidor de Administração**

Laptops itinerantes encontram-se às vezes dentro da rede e fora e outras ocasiões. Para um gerenciamento eficaz, é necessário que eles se conectem ao Servidor de Administração de maneira diferente dependendo de sua localização. Para um uso eficiente do tráfego, eles também precisam receber atualizações de diferentes fontes dependendo de sua localização.

É necessário configurar regras para usuários ausentes: perfis de conexão e descrições de local de rede. Cada regra define o Servidor de Administração, a instância à qual os laptops itinerantes devem se conectar, dependendo de sua localização e do Servidor de Administração a partir do qual devem receber atualizações.

Cenário: conectando dispositivos ausentes do escritório por meio de um Servidor de Administração secundário na DMZ

Caso queira conectar dispositivos gerenciados e localizados fora da rede principal ao Servidor de Administração, é possível fazer isso usando um Servidor de Administração secundário localizado na zona desmilitarizada (DMZ).

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- Uma DMZ é organizada na rede da organização.
- O Servidor de Administração do Kaspersky Security Center é implementado na rede corporativa.

Fases

O cenário segue em etapas:

1 **Selecionando um dispositivo cliente na DMZ**

Na DMZ, selecione um dispositivo cliente que será usado como um Servidor de Administração secundário.

2 **Instalando o Servidor de Administração do Kaspersky Security Center**

Instale o Servidor de Administração do Kaspersky Security Center neste dispositivo cliente.

3 **Criar uma hierarquia de Servidores de Administração**

Caso queira colocar um Servidor de Administração secundário na DMZ, o Servidor de Administração secundário deve receber uma conexão do Servidor de Administração principal. É possível adicionar um novo Servidor de administração como secundário para que o Servidor de Administração principal se conecte ao Servidor de Administração secundário pela porta 13000. Ao combinar dois Servidores de Administração em uma hierarquia, verifique e confirme se a porta 13299 está acessível em ambos os Servidores de Administração. O Kaspersky Security Center Web Console se conecta a um Servidor de Administração pela porta 13299.

4. **Conectando dispositivos gerenciados e ausentes do escritório ao Servidor de Administração secundário**

   É possível conectar dispositivos ausentes do escritório ao Servidor de Administração localizado na DMZ da mesma maneira que a conexão é estabelecida entre o Servidor de Administração e os dispositivos gerenciados localizados na rede principal. Os dispositivos gerenciados e ausentes do escritório iniciam a conexão pela porta 13000.

Sobre a conexão de dispositivos externos

Alguns dispositivos gerenciados encontram-se sempre localizados fora da rede principal (por exemplo, dispositivos nas filiais regionais da empresa; quiosques, caixas eletrônicos e terminais instalados em vários pontos de venda; dispositivos de funcionários em home-office). Alguns dispositivos saem do perímetro de vez em quando (por exemplo, laptops de usuários que visitam filiais regionais ou o escritório de um cliente).

Ainda é necessário monitorar e gerenciar a proteção de dispositivos ausentes – receber informações reais sobre seu status de proteção e manter os aplicativos de segurança neles atualizados. Isso é necessário porque, por exemplo, se tal dispositivo for comprometido enquanto estiver longe da rede principal, ele pode se tornar uma plataforma para a propagação de ameaças assim que se conectar à rede principal. Para conectar dispositivos externos ao Servidor de Administração, você pode usar dois métodos:

- Gateway de conexão na zona desmilitarizada (DMZ)

  Consulte o esquema de tráfego de dados: Servidor de Administração na LAN, dispositivos gerenciados na Internet, gateway de conexão em uso

- Servidor de Administração na DMZ

  Veja o esquema de tráfego de dados: Servidor de Administração na DMZ, dispositivos gerenciados na Internet

Um gateway de conexão na DMZ

Um método recomendado para conectar dispositivos externos ao Servidor de Administração é organizar uma DMZ na rede da organização e instalar um gateway de conexão na DMZ. Os dispositivos externos se conectarão ao gateway de conexão e o Servidor de Administração dentro da rede iniciará uma conexão aos dispositivos por meio do gateway de conexão.

Em comparação com o outro método, esse é mais seguro:

- Você não precisa abrir o acesso ao Servidor de Administração de fora da rede.
- Um gateway de conexão comprometido não representa um alto risco para a segurança dos dispositivos de rede. Na verdade, um gateway de conexão não realiza nenhum gerenciamento e não estabelece nenhuma conexão.

Além disso, um gateway de conexão não requer muitos recursos de hardware.

No entanto, esse método tem um processo de configuração mais complicado:

- Para fazer um dispositivo atuar como um gateway de conexão na DMZ, você precisa instalar o Agente de Rede e conectá-lo ao Servidor de Administração de uma maneira muito específica.
- Você não poderá usar o mesmo endereço para se conectar ao Servidor de Administração em todas as situações. Fora do perímetro, você precisará usar não apenas um endereço diferente (endereço do gateway de conexão), mas também um modo de conexão diferente: por meio de um gateway de conexão.
- Você também precisa definir configurações de conexão diferentes para laptops em locais diferentes.

Para adicionar um gateway de conexão a uma rede configurada anteriormente:

1. Instale o Agente de Rede na função de gateway de conexão.
2. Reinstale o Agente de Rede em dispositivos que deseja conectar ao gateway de conexão recém-adicionado.

Servidor de Administração na DMZ

Outro método é instalar um único Servidor de Administração na DMZ.

Essa configuração é menos segura do que o outro método. Para gerenciar laptops externos, neste caso, o Servidor de Administração deve aceitar conexões de qualquer endereço na Internet. Ele ainda irá gerenciar todos os dispositivos na rede interna, mas na DMZ. Portanto, um servidor comprometido pode causar uma enorme quantidade de danos, apesar da baixa probabilidade de tal evento.

O risco é significativamente reduzido se o Servidor de Administração na DMZ não gerenciar os dispositivos na rede interna. Essa configuração pode ser usada, por exemplo, por um provedor de serviços para gerenciar os dispositivos dos clientes.

Você pode querer usar esse método nos seguintes casos:

- Se tiver familiaridade com a instalação e configuração do Servidor de Administração e não deseja executar outro procedimento para instalar e configurar um gateway de conexão.
- Se precisar gerenciar mais dispositivos. A capacidade máxima do Servidor de Administração é de 100.000 dispositivos, enquanto um gateway de conexão pode suportar até 10.000 dispositivos.

Esta solução também tem possíveis dificuldades:

- O Servidor de Administração requer mais recursos de hardware e mais um banco de dados.
- As informações sobre os dispositivos serão armazenadas em dois bancos de dados não relacionados (para o Servidor de Administração dentro da rede e outro na DMZ), o que complica o monitoramento.
- Para gerenciar todos os dispositivos, o Servidor de Administração precisa ser unido em uma hierarquia, o que complica não apenas o monitoramento, mas também o gerenciamento. Uma instância do Servidor de Administração secundário impõe limitações às estruturas possíveis de grupos de administração. Você deve decidir como e quais tarefas e políticas distribuir para uma instância secundária do Servidor de Administração.

- Configurar dispositivos externos para usar o Servidor de Administração na DMZ externamente e para usar o Servidor de Administração principal internamente não é mais simples do que apenas configurá-los para usar uma conexão condicional por meio de um gateway.

- Riscos de segurança elevados. Uma instância do Servidor de Administração comprometida torna mais fácil comprometer seus laptops gerenciados. Se isso acontecer, os hackers precisam apenas esperar que um dos laptops retorne à rede corporativa para que possam continuar seu ataque à rede local.

Conexão de dispositivos de desktop externos ao Servidor de Administração

Os dispositivos de desktop que estão sempre fora da rede principal (por exemplo, computadores nas filiais regionais da empresa; quiosques, caixas eletrônicos e terminais instalados em vários pontos de venda; dispositivos de funcionários em home-office) não podem ser conectados diretamente ao Servidor de Administração. Esses devem ser conectados ao Servidor de Administração por meio de um gateway de conexão instalado na zona desmilitarizada (DMZ). Essa configuração é feita ao instalar o Agente de Rede nesses dispositivos.

Para conectar dispositivos de desktop externos ao Servidor de Administração:

1. Crie um novo pacote de instalação para o Agente de Rede.

2. Abra as propriedades do pacote de instalação criado, acesse a seção **Configurações** → **Avançado** e, então, selecione a opção **Conectar-se ao Servidor de Administração usando o gateway de conexão**.

   A configuração **Conectar-se ao Servidor de Administração usando o gateway de conexão** é incompatível com a configuração **Usar o Agente de Rede como um gateway de conexão na DMZ**. Não é possível ativar essas duas configurações ao mesmo tempo.

3. No campo **Endereço de gateway de conexão**, especifique o endereço público do gateway de conexão.

   Se o gateway de conexão estiver localizado atrás da Tradução de Endereço de Rede (NAT) e não tiver seu próprio endereço público, configure uma regra de gateway NAT para encaminhar conexões do endereço público para o endereço interno do gateway de conexão.

4. Crie um pacote de instalação independente com base no pacote de instalação criado.

5. Forneça o pacote de instalação independente aos dispositivos de destino por meio eletrônico ou de uma unidade removível.

6. Instale o Agente de Rede a partir do pacote independente.

Os dispositivos de desktop externos são conectados com o Servidor de Administração.

Sobre a configuração de perfis de conexão para usuários ausentes

Os usuários ausentes de laptops (aqui também referidos como "dispositivos") podem precisar alterar o método da conexão a um Servidor de Administração ou alternar entre Servidores de Administração dependendo da localização atual do dispositivo na rede corporativa.

Os perfis de conexão têm suporte somente para dispositivos que executam Windows e macOS.

Usar endereços diferentes de um Servidor de Administração único

Os dispositivos com o Agente de Rede instalado podem conectar-se ao Servidor de Administração da intranet da organização ou a partir da Internet. Esta situação pode necessitar que o Agente de Rede use endereços diferentes para a conexão ao Servidor de Administração: o endereço do Servidor de Administração externo para a conexão com a Internet e o endereço do Servidor de Administração interno para a conexão da rede interna.

Para fazer isso, adicione um perfil para conexão ao Servidor de Administração a partir da Internet nas propriedades da política do Agente de Rede (na seção **Configurações do aplicativo** → **Conectividade** → **Perfis de conexão** → **Perfis de conexão do Servidor de Administração**). Na janela de criação de perfil, desative a opção **Usar somente para receber atualizações** e certifique-se de que a opção **Sincronizar as configurações de conexão com as configurações do Servidor de Administração especificadas nesse perfil** esteja selecionada. Se você usa um gateway de conexão para acessar o Servidor de Administração (por exemplo, em uma configuração do Kaspersky Security Center que está descrita em No acesso à Internet: Agente de Rede como um gateway de conexão em DMZ), deverá especificar o endereço do gateway de conexão no campo correspondente do perfil de conexão.

Alternar entre Servidores de Administração dependendo da rede atual

Se a organização tiver múltiplos escritórios com diferentes Servidores de Administração e alguns dispositivos com o Agente de Rede instalado se moverem entre eles, você precisa do Agente de Rede para conectar-se ao Servidor de Administração da rede local no escritório onde o dispositivo está atualmente localizado.

Nesse caso, é preciso criar um perfil para a conexão ao Servidor de Administração nas propriedades da política do Agente de Rede de cada um dos escritórios, exceto para o escritório doméstico onde o Servidor de Administração principal estiver localizado. Especifique os endereços dos Servidores de Administração em perfis de conexão e ative ou desative a opção **Usar somente para receber atualizações**:

- Selecione a opção se você precisar que o Agente de Rede seja sincronizado com o Servidor de Administração mestre, usando o Servidor local somente para baixar as atualizações.
- Desative a opção se for necessário que o Agente de Rede seja gerenciado completamente pelo Servidor de Administração local.

Após isso, você deve definir as condições da troca para os perfis recém criados: ao menos uma condição de cada um dos escritórios, exceto para o escritório doméstico. Cada propósito de condição consiste na detecção de itens que são específicos para o ambiente de rede de um escritório. Se uma condição for verdadeira, o perfil correspondente é ativado. Se nenhuma das condições for verdadeira, o Agente de Rede alterna para o Servidor de Administração mestre.

Criando um perfil de conexão para usuários ausentes

Um perfil de conexão do Servidor de Administração está disponível somente em dispositivos que executam Windows e macOS.

Para criar um perfil para a conexão do Agente de Rede ao Servidor de Administração para usuários fora do escritório:

1. Caso queira criar um perfil de conexão para um grupo de dispositivos gerenciados, abra a política do Agente de Rede desse grupo. Para fazer isso, execute como seguintes ações:

   a. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.

   b. Clique no link do caminho atual.

   c. Na janela aberta, selecione um grupo de administração necessário.

      Depois disso, o caminho atual é alterado.

   d. Adicione a política do Agente de Rede para o grupo de dispositivos gerenciados. Caso já tenha sido criado, clique no nome da política do Agente de Rede para abrir as propriedades da política.

2. Caso queira criar um perfil de conexão para um dispositivo gerenciado específico, faça o seguinte:

   a. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

   b. Clique no nome do dispositivo gerenciado.

   c. Na janela exibida de propriedades do dispositivo gerenciado, acesse a guia **Aplicativos**.

   d. Clique no nome da política do Agente de Rede que se aplique somente ao dispositivo gerenciado selecionado.

3. Na janela de propriedades aberta, acesse **Configurações do aplicativo** → **Conectividade** → **Perfis de conexão.**

4. Na seção **Perfis de conexão do Servidor de Administração**, clique no botão **Adicionar**.

   Por padrão, a lista de perfis de conexão contém os perfis <Modo offline> e <Servidor de Administração principal>. O perfil não pode ser editado ou removido.

   O perfil <Modo offline> não especifica nenhum Servidor para conexão. Portanto, o Agente de Rede, quando alternado para esse perfil, não tentará fazer conexão com nenhum Servidor de Administração enquanto os aplicativos instalados nos dispositivos cliente forem executados sob políticas de ausência. O perfil <Modo offline> pode ser usado se os dispositivos estiverem desconectados da rede.

   O perfil <Servidor de Administração principal> especifica para a conexão o Servidor de Administração que foi selecionado durante a instalação do Agente de Rede. O perfil <Servidor de Administração principal> é aplicado quando um dispositivo for reconectado ao Servidor de Administração principal após que ele estava sendo executado em uma rede externa por algum tempo.

5. Na janela **Configurar perfil** que se abre, configure o perfil de conexão:

   - **Nome do perfil**

     No campo de entrada, é possível consultar ou alterar o nome do perfil de conexão.

   - **Endereço do Servidor de Administração**

     O endereço do Servidor de administração ao qual o dispositivo cliente deve conectar-se durante a ativação do perfil.

   - **Número da porta**

     O número da porta que é usada para conexão.

   - **Porta SSL**

     Número da porta para conexão com, uso do protocolo SSL.

   - **Usar conexão SSL**

     Se esta opção estiver ativada, a conexão é estabelecida através de uma porta segura, com o protocolo SSL.

     Por padrão, esta opção está ativada. Recomendamos não desativar a opção para que a conexão permaneça segura.

   - Selecione a opção **Usar o servidor proxy** caso queira usar um servidor proxy para se conectar com a Internet. Se essa opção estiver selecionada, os campos estarão disponíveis para inserir configurações. Especifique as seguintes configurações para a conexão ao servidor proxy:

     - **Endereço**

       Endereço do servidor proxy usado para conexão do Kaspersky Security Center à Internet.

     - **Número da porta**

Número da porta pela qual a conexão proxy do Kaspersky Security Center será estabelecida.

- **Autenticação do servidor proxy**

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

- **Nome do usuário**

  Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

- **Senha**

  A senha definida pelo usuário de cuja conta a conexão com o servidor proxy é estabelecida (este campo está disponível se a caixa de seleção **Autenticação do servidor proxy** estiver marcada).

  Para ver a senha inserida, mantenha pressionado o botão **Exibir** pelo tempo que você desejar.

- **Endereço de gateway de conexão**

  O endereço do gateway através do qual os dispositivos cliente se conectam com o Servidor de Administração.

- **Ativar modo ausente quando o Servidor de Administração não estiver disponível**

  Marque a caixa de seleção para permitir aos aplicativos instalados em um dispositivo cliente usar perfis da política para dispositivos no modo ausente, assim como políticas de ausência, no momento de qualquer tentativa de conexão, se o Servidor de Administração não estiver disponível. Se a política de ausência do escritório não estiver definida para o aplicativo, a política ativa será usada.

  Se esta opção estiver desativada, os aplicativos usarão as políticas ativas.

  Por padrão, esta caixa de seleção está desmarcada.

- **Usar somente para receber atualizações**

  Se esta opção estiver ativada, o perfil somente será usado para baixar atualizações pelos aplicativos instalados no dispositivo cliente. Para outras operações, a conexão ao Servidor de Administração será estabelecida com as configurações de conexão iniciais definidas durante a instalação do Agente de Rede.

  Por padrão, esta opção está ativada.

- **Sincronizar as configurações de conexão com as configurações do Servidor de Administração especificadas nesse perfil**

Se esta opção estiver ativada, o Agente de Rede se conecta ao Servidor de Administração utilizando as configurações especificadas nas propriedades do perfil.

Se esta opção estiver desativada, o Agente de Rede se conecta ao Servidor de Administração utilizando as configurações originais que foram especificadas durante a instalação.

Essa opção estará disponível se a opção **Usar somente para receber atualizações** estiver desabilitada.

Por padrão, esta opção está desativada.

Um perfil para conectar o Agente de Rede ao Servidor de Administração é criado para usuários fora do escritório. Quando o Agente de Rede se conectar ao Servidor de Administração usando esse perfil, os aplicativos instalados no dispositivo cliente usarão as políticas para dispositivos no modo ausente ou políticas de ausência.

Sobre a mudança do Agente de Rede para outro servidor de Administração

O Kaspersky Security Center oferece a opção de trocar o Agente de Rede em um dispositivo cliente para outros Servidores de Administração, caso as seguintes configurações da rede tenham sido alteradas:

- **Condição do endereço do servidor DHCP** —O endereço IP do servidor Dynamic Host Configuration Protocol (DHCP) da rede foi alterado.
- **Adicionar condição para o endereço do gateway de conexão padrão** – O endereço do gateway da rede principal foi alterado.
- **Condição para o domínio DNS** – O sufixo DNS da sub-rede foi alterado.
- **Condição do endereço do servidor DNS** – O endereço IP do servidor DNS da rede foi alterado.
- **Condição do endereço do servidor WINS** – O endereço IP do servidor WINS da rede foi alterado. Essa configuração está disponível apenas para dispositivos que executam o Windows.
- **Condição da capacidade de resolução de nome** – O nome DNS ou NetBIOS do dispositivo cliente foi alterado.
- **Condição para a sub-rede** – Alterações no endereço e máscara da rede.
- **Condição de acessibilidade do Domínio do Windows** – Altera o status do domínio do Windows ao qual um dispositivo cliente está conectado. Essa configuração está disponível apenas para dispositivos que executam o Windows.
- **Condição de acessibilidade do endereço de conexão SSL** – O dispositivo cliente pode ou não (dependendo da opção selecionada) estabelecer uma conexão SSL com um servidor especificado (nome:porta). Para cada servidor, é possível especificar adicionalmente um certificado SSL. Nesse caso, o agente de rede verifica o certificado do servidor, além de verificar a capacidade de uma conexão SSL. Se o certificado não for correspondente, a conexão falhará.

Esse recurso é compatível apenas com Agentes de Rede instalados em dispositivos executando o Windows ou macOS.

As configurações iniciais da conexão do Agente de Rede ao Servidor de Administração são definidas durante a instalação do Agente de Rede. Após isso, se regras de troca do Agente de Rede para outros Servidores de Administração tiverem sido criadas, o Agente de Rede responde às alterações nas configurações de rede, como segue:

- Se as configurações de rede estiverem em conformidade com uma das regras criadas, o Agente de Rede conecta-se ao Servidor de Administração especificado nessa regra. Os aplicativos instalados nos dispositivos cliente mudam para as políticas de ausência de escritório, desde que tal comportamento esteja ativado por uma regra.

- Se nenhuma das regras se aplicarem, o Agente de Rede retorna para as configurações padrão de conexão ao Servidor de Administração especificadas durante a instalação. Os aplicativos instalados nos dispositivos cliente alternam de volta para as políticas ativas.

- Se o Servidor de Administração não estiver acessível, o Agente de Rede usa as políticas de ausência de escritório.

O Agente de Rede troca para a política de ausência somente se a opção **Ativar modo ausente quando o Servidor de Administração não estiver disponível** estiver ativada nas configurações da política do Agente de Rede.

As configurações da conexão do Agente de Rede ao Servidor de Administração são salvas em um perfil de conexão. No perfil de conexão, você poderá criar regras de troca de dispositivos clientes para políticas de ausência de escritório, assim como configurar o perfil para que ele possa ser usado apenas para baixar atualizações.

Criar uma regra de troca do Agente de Rede por localização da rede

A troca do Agente de Rede por localização da rede está disponível somente em dispositivos que executam Windows e macOS.

Para criar uma regra para a troca do Agente de Rede de um Servidor de Administração para outro se as configurações de rede forem alteradas:

1. Caso queira criar uma regra para um grupo de dispositivos gerenciados, abra a política do Agente de Rede desse grupo. Para fazer isso, execute como seguintes ações:

   a. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.

   b. Clique no link do caminho atual.

   c. Na janela aberta, selecione um grupo de administração necessário.

   Depois disso, o caminho atual é alterado.

   d. Adicione a política do Agente de Rede para o grupo de dispositivos gerenciados. Caso já tenha sido criado, clique no nome da política do Agente de Rede para abrir as propriedades da política.

2. Caso queira criar uma regra para um dispositivo gerenciado específico, faça o seguinte:

   a. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

   b. Clique no nome do dispositivo gerenciado.

   c. Na janela exibida de propriedades do dispositivo gerenciado, acesse a guia **Aplicativos**.

   d. Clique no nome da política do Agente de Rede que se aplique somente ao dispositivo gerenciado selecionado.

3. Na janela de propriedades aberta, acesse **Configurações do aplicativo** → **Conectividade** → **Perfis de conexão.**

4. Na seção **Configurações do local de rede**, clique no botão **Adicionar**.

5. Em propriedades da janela aberta, configure a descrição da localização da rede e a regra de troca. Especifique as seguintes configurações de descrição da localização da rede:

   - **Descrição**

     O nome de uma descrição da localização da rede não pode ter mais do que 255 caracteres nem conter símbolos especiais, tal como ("*<>?\/:|).

   - **Usar perfil de conexão**

     Na lista suspensa, é possível especificar o perfil de conexão usado pelo Agente de Rede para conectar ao Servidor de Administração. Este perfil será usado quando as condições da descrição da localização da rede forem atendidas. O perfil de conexão contém as configurações para a conexão do Agente de Rede ao Servidor de Administração; ele também define quando os dispositivos cliente devem alternar para as políticas de ausência de escritório. O perfil é usado somente para baixar atualizações.

   - **Descrição ativada**

     Marque essa caixa de seleção para habilitar o uso da nova descrição do local de rede.

6. Selecione as condições para a regra de alternância do Agente de Rede:

   - **Condição do endereço do servidor DHCP** – O endereço IP do servidor Dynamic Host Configuration Protocol (DHCP) da rede foi alterado.
   - **Adicionar condição para o endereço do gateway de conexão padrão** – O endereço do gateway da rede principal foi alterado.
   - **Condição para o domínio DNS** – O sufixo DNS da sub-rede foi alterado.
   - **Condição do endereço do servidor DNS** – O endereço IP do servidor DNS da rede foi alterado.
   - **Condição do endereço do servidor WINS** – O endereço IP do servidor WINS da rede foi alterado. Essa configuração está disponível apenas para dispositivos que executam o Windows.
   - **Condição da capacidade de resolução de nome** – O nome DNS ou NetBIOS do dispositivo cliente foi alterado.
   - **Condição para a sub-rede** – Alterações no endereço e máscara da rede.
   - **Condição de acessibilidade do Domínio do Windows** – Altera o status do domínio do Windows ao qual um dispositivo cliente está conectado. Essa configuração está disponível apenas para dispositivos que executam o Windows.
   - **Condição de acessibilidade do endereço de conexão SSL** – O dispositivo cliente pode ou não (dependendo da opção selecionada) estabelecer uma conexão SSL com um servidor especificado (nome:porta). Para cada servidor, é possível especificar adicionalmente um certificado SSL. Nesse caso, o agente de rede verifica o certificado do servidor, além de verificar a capacidade de uma conexão SSL. Se o certificado não for correspondente, a conexão falhará.

   As condições de uma regra se combinam através do uso do operador lógico AND. Para acionar uma regra de troca através da descrição da localização da rede, todas as condições de troca da regra devem ser atendidas.

7. Na seção de condição, especifique quando o Agente de Rede deve ser alternado para outro Servidor de Administração. Para isso, clique no botão **Adicionar** e, em seguida, defina o valor da condição.

   Além disso, a opção **Corresponde a pelo menos um valor da lista** está habilitada por padrão. É possível desabilitar essa opção caso deseje que a condição seja atendida com todos os valores especificados.

8. Salve as alterações.

Uma nova regra de troca através da descrição da localização da rede é criada; sempre que as suas condições forem atendidas, o Agente de Rede usa o perfil de conexão especificado na regra para conectar-se ao Servidor de Administração.

Assistente de implementação da proteção

Para instalar os aplicativos da Kaspersky, você pode usar o assistente de Implementação da proteção. O assistente de Implementação da proteção permite a instalação remota de aplicativos por meio de pacotes de instalação especialmente criados ou diretamente de um pacote de distribuição.

O Assistente de implementação de proteção executa as seguintes ações:

- Baixa um pacote de instalação para implementação do aplicativo (se não foi criado anteriormente). O pacote de instalação está localizado em **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**. Você pode usar esse pacote de instalação para instalação do aplicativo no futuro.
- Cria e executa uma tarefa de instalação remota para dispositivos específicos ou para um grupo de administração. A tarefa de instalação remota recém-criada é armazenada na seção **Tarefas**. Você pode iniciar essa tarefa manualmente mais tarde. O tipo de tarefa é **Instalar o aplicativo remotamente**.

Caso queira instalar o agente de rede em dispositivos com o sistema operacional SUSE Linux Enterprise Server 15, instale o pacote insserv-compat primeiro para configurar o agente de rede.

Etapa 1. Iniciar o assistente de implementação da proteção

Para iniciar o assistente de implementação da proteção manualmente,

No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Assistente de Implementação de Proteção**.

O assistente de implementação da proteção é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

Etapa 2. Seleção do pacote de instalação

Selecione o pacote de instalação do aplicativo que deseja instalar.

Se o pacote de instalação do aplicativo necessário não estiver listado, clique no botão **Adicionar** e selecione o aplicativo na lista.

Etapa 3. Seleção de um método de distribuição de arquivo de chave ou código de ativação

Selecione um método para a distribuição de arquivo de chave ou do código de ativação:

- **Não adicionar chave de licença ao pacote de instalação**

  A chave será automaticamente distribuída a todos os dispositivos com os quais ela for compatível:

  - Se a distribuição automática foi ativada nas propriedades da chave.
  - Se a tarefa **Adicionar chave** foi criada.

- **Adicionar chave de licença ao pacote de instalação**

  A chave é distribuída aos dispositivos em conjunto com o pacote de instalação.

  Não recomendamos que distribua a chave usando este método, porque os direitos de acesso de Leitura são ativados para o repositório de pacotes de instalação.

Caso o pacote de instalação já inclua um arquivo de chave ou código de ativação, essa janela será exibida, mas conterá apenas as informações da chave de licença.

Etapa 4. Seleção de versão do Agente de Rede

Se tiver selecionado o pacote de instalação de um aplicativo que não o Agente de Rede, você também precisará instalar o Agente de Rede, que conecta o aplicativo ao Servidor de Administração do Kaspersky Security Center.

Selecione a versão mais recente do Agente de Rede.

Etapa 5. Seleção de dispositivos

Especifique uma lista de dispositivos nos quais o aplicativo será instalado:

- **Instalar em dispositivos gerenciados**

  Se esta opção estiver selecionada, a tarefa de instalação remota para um grupo de dispositivos será criada.

- **Selecionar dispositivos para a instalação**

  A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

  Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

Etapa 6. Especificação das configurações de tarefa de instalação remota

Na página **Configurações da tarefa de instalação remota**, especifique as configurações para a instalação remota do aplicativo.

No grupo de configurações **Forçar download do pacote de instalação**, especifique como os arquivos que são necessários para instalar um aplicativo são distribuídos nos dispositivos clientes:

- **Usando o Agente de Rede**

  Se esta opção de seleção estiver ativada, os pacotes de instalação são entregues aos dispositivos clientes pelo Agente de Rede instalado neles.

  Caso esta opção estiver desativada, os pacotes de instalação serão entregues usando as ferramentas do sistema operacional dos dispositivos clientes.

  Recomendamos que você ative esta opção se a tarefa tiver sido atribuída a dispositivos com o Agente de Rede instalado.

  Por padrão, esta opção está ativada.

- **Usando recursos do sistema operacional através de pontos de distribuição**

  Se esta opção estiver ativada, os pacotes de instalação serão transmitidos para os dispositivos clientes usando as ferramentas do sistema operacional, através dos pontos de distribuição. Você pode selecionar esta opção se houver, no mínimo, um ponto de distribuição na rede.

  Se opção **Uso do Agente de Rede** estiver ativada, os arquivos serão entregues pelas ferramentas do sistema operacional, apenas se os recursos do Agente de Rede estiverem indisponíveis.

  Por padrão, esta opção está ativada para as tarefas de instalação remotas que são criadas em um Servidor de Administração virtual.

- **Usando recursos do sistema operacional através do Servidor de Administração**

  Caso esta opção esteja ativada, os arquivos serão transmitidos para os dispositivos clientes usando as ferramentas do sistema operacional pelo Servidor de Administração. Você pode ativar esta opção se nenhum Agente de Rede estiver instalado no dispositivo cliente, mas esse está na mesma rede que o Servidor de Administração.

  Por padrão, esta opção está ativada.

Defina as configurações adicionais:

- **Não reinstalar o aplicativo se ele já estiver instalado**

  Se esta opção estiver ativada, o aplicativo selecionado não será reinstalado se já estiver instalado neste dispositivo cliente.

  Se esta opção não estiver ativada, o aplicativo será instalado de qualquer forma.

  Por padrão, esta opção está ativada.

- **Atribuir a instalação do pacote em políticas de grupo do Active Directory**

  Se esta opção estiver ativada, é instalado um pacote de instalação, usando as políticas de grupo do Active Directory.

  Essa opção fica disponível se o pacote de instalação do Agente de Rede estiver selecionado.

  Por padrão, esta opção está desativada.

Etapa 7. Gerenciamento de reinício

Especifique a ação a ser executada se o sistema operacional precisar ser reiniciado quando você instalar o aplicativo:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min.)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Reiniciar após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

  A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

  Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

  Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

  Por padrão, esta opção está desativada.

Etapa 8. Remoção de aplicativos incompatíveis antes de instalação

Esta etapa só estará presente se o aplicativo implementado for incompatível com outros aplicativos.

Selecione a opção se quiser que o Kaspersky Security Center remova automaticamente aplicativos incompatíveis com o aplicativo implementado.

A lista de aplicativos incompatíveis também é exibida.

Se você não marcar esta opção, o aplicativo será instalado apenas em dispositivos que não têm aplicativos incompatíveis.

Etapa 9. Movimentação de dispositivos para dispositivos gerenciados

Especifique se os dispositivos devem ser movidos para um grupo de administração depois da instalação do Agente de Rede.

- **Não migrar dispositivos**

  Os dispositivos permanecem nos grupos nos quais eles estão atualmente localizados. Os dispositivos que não foram colocados em nenhum grupo continuam não atribuídos.

- **Migrar dispositivos não atribuídos para o grupo**

  Os dispositivos são movidos para o grupo de administração selecionado.

A opção **Não migrar dispositivos** está marcada por padrão. Por motivos de segurança, você pode desejar mover os dispositivos manualmente.

Etapa 10. Seleção de contas para acessar dispositivos

Se necessário, adicione as contas que serão usadas para iniciar a tarefa de instalação remota:

- **Nenhuma conta necessária (Agente de Rede instalado)**

  Se essa caixa de seleção estiver selecionada, você não precisará especificar uma conta sob a qual o instalador do aplicativo será executado. A tarefa será executada sob a conta sob a qual o serviço do Servidor de Administração está sendo executado.

  Caso o Agente de Rede não tenha sido instalado em dispositivos cliente, a opção não estará disponível.

- **Conta necessária (Agente de Rede não é usado)**

Selecione esta opção se o Agente de Rede não estiver instalado nos dispositivos aos quais você atribui a tarefa de instalação remota. Neste caso, é possível especificar uma conta de usuário ou um certificado SSH para instalar o aplicativo.

- **Conta local**. Se essa opção estiver selecionada, especifique a conta de usuário sob a qual o instalador do aplicativo será executado. Clique no botão **Adicionar**, selecione **Conta local** e, então, especifique as credenciais da conta do usuário.

  É possível especificar várias contas de usuário se, por exemplo, nenhuma delas tiver todos os direitos necessários em todos os dispositivos para os quais você atribui a tarefa. Nesse caso, todas as contas adicionadas são usadas para executar a tarefa, em ordem consecutiva, de cima para baixo.

- **Certificado SSH**. Se quiser instalar um aplicativo em um dispositivo cliente baseado em Linux, poderá especificar um certificado SSH em vez de uma conta de usuário. Clique no botão **Adicionar**, selecione **Certificado SSH** e, então, especifique as chaves privada e pública do certificado.

  Para gerar uma chave privada, você pode usar o utilitário ssh-keygen. Observe que o Kaspersky Security Center é compatível com o formato PEM de chaves privadas, mas o utilitário ssh-keygen gera chaves SSH no formato OPENSSH por padrão. O formato OPENSSH não é compatível com o Kaspersky Security Center. Para criar uma chave privada no formato PEM compatível, adicione a opção -m PEM no comando ssh-keygen. Por exemplo:

  ```
  ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail do usuário>"
  ```

Etapa 11. Início da instalação

Essa página é a última etapa do assistente. Nesta etapa, a **Tarefa de instalação remota** foi criada e configurada com sucesso.

Por padrão, a opção **Executar a tarefa após a conclusão do assistente** não está selecionada. Caso esta opção seja selecionada, a **Tarefa de instalação remota** será iniciada imediatamente após a conclusão do assistente. Caso esta opção não seja marcada, a **Tarefa de instalação remota** não será iniciada. Você pode iniciar essa tarefa manualmente mais tarde.

Clique em **OK** para concluir a etapa final do assistente de implementação da proteção.

Implementação de aplicativos Kaspersky por meio do Kaspersky Security Center Web Console

Esta seção descreve a implementação de aplicativos Kaspersky em dispositivos gerenciados, usando o Kaspersky Security Center Web Console.

Cenário: implementação de aplicativos Kaspersky por meio do Kaspersky Security Center Web Console

Este cenário explica como implementar aplicativos Kaspersky por meio do Kaspersky Security Center Web Console. Você pode usar o Assistente de início rápido e o Assistente de implementação da proteção ou concluir todas as etapas necessárias manualmente.

Os seguintes aplicativos estão disponíveis para implementação usando o Kaspersky Security Center Web Console:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux

Fases

A implementação dos aplicativos da Kaspersky é feita em fases:

1. **Download do plug-in de gerenciamento para o aplicativo**

   Esta etapa faz parte do Assistente de início rápido. Se optar por não executar o assistente, baixe o plug-in do Kaspersky Endpoint Security for Windows manualmente.

   Se você planeja gerenciar dispositivos móveis corporativos, siga as instruções fornecidas no Ajuda do Kaspersky Security for Mobile para baixar e instalar os plug-ins de gerenciamento do Kaspersky Endpoint Security for Android.

2. **Baixando e criando pacotes de instalação**

   Esta etapa faz parte do Assistente de início rápido.

   O Assistente de início rápido permite baixar o pacote de instalação com o plug-in de gerenciamento. Se você não selecionou esta opção ao executar o assistente, ou se não executou o assistente, deve baixar o pacote manualmente.

   Se você não conseguir instalar os aplicativos Kaspersky pelo Kaspersky Security Center em alguns dispositivos, por exemplo, em dispositivos de funcionários remotos, poderá criar pacotes de instalação independentes para aplicativos. Caso os pacotes autônomos sejam usados para instalar os aplicativos Kaspersky, não será preciso criar e executar uma tarefa de instalação remota, nem criar e configurar tarefas para o Kaspersky Endpoint Security for Windows.

3. **Criação, configuração e execução da tarefa de instalação remota**

   No Kaspersky Endpoint Security for Windows, essa etapa faz parte do Assistente de implementação da proteção, iniciado automaticamente após a conclusão do Assistente de início rápido. Se optar por não executar o Assistente de implementação da proteção, você deverá criar e configurar essa tarefa manualmente.

   Você também pode criar manualmente várias tarefas de instalação remotas para grupos de administração ou seleções de dispositivos diferentes. Você pode implementar versões diferentes de um aplicativo nessas tarefas.

   Certifique-se de que todos os dispositivos na sua rede sejam descobertos; e execute a(s) tarefa(s) de instalação remotas.

   > Caso queira instalar o agente de rede em dispositivos com o sistema operacional SUSE Linux Enterprise Server 15, instale o pacote insserv-compat primeiro para configurar o agente de rede.

4. **Criar e configurar as tarefas para o aplicativo gerenciado**

   A tarefa *Instalar atualização* do Kaspersky Endpoint Security for Windows deve ser configurada.

   Esta etapa faz parte do Assistente de início rápido: a tarefa é criada e configurada automaticamente com as configurações padrão. Se não tiver executado o assistente, você deverá criar essa tarefa manualmente e configurá-la manualmente. Caso use o assistente de início rápido, verifique e confirme se o cronograma da tarefa atende aos seus requisitos. (Por padrão, o início agendado da tarefa é definido como **Manualmente**, mas é possível escolher outra opção.)

   Outros aplicativos Kaspersky poderão ter outras tarefas padrão. Consulte a documentação dos aplicativos correspondentes para mais detalhes.

   Certifique-se de que a programação de cada tarefa que você atenda aos seus requisitos.

5. **Instalando o Kaspersky Security for Mobile (opcional)**

   Se você planeja gerenciar dispositivos móveis corporativos, siga as instruções fornecidas no Ajuda do Kaspersky Security for Mobile para obter informações sobre a implementação do Kaspersky Endpoint Security for Android.

6. **Criar políticas**

   Crie a política para cada aplicativo manualmente ou (no caso do Kaspersky Endpoint Security for Windows) usando o Assistente de início rápido. Você pode usar as configurações padrão da política; pode também modificar as configurações padrão da política segundo as suas necessidades a qualquer momento.

7. **Verificar os resultados**

   Certifique-se de que a implementação tenha sido concluída com sucesso: você tem políticas e tarefas para cada aplicativo, e esses aplicativos são instalados nos dispositivos gerenciados.

Resultados

A conclusão do cenário produz o seguinte:

- Todas as políticas e tarefas necessárias dos aplicativos selecionados são criadas.
- As programações de tarefas são configuradas segundo as suas necessidades.
- Os aplicativos selecionados são implementados ou planejados para ser implementados nos dispositivos cliente selecionados.

Aquisição de plugins para aplicativos Kaspersky

Para implementar um aplicativo da Kaspersky, como o Kaspersky Endpoint Security for Windows, você deve baixar o plugin de gerenciamento de aplicativos.

Para baixar um plugin de gerenciamento para um aplicativo da Kaspersky:

1. No menu principal, vá para **Configurações do console** → **Plug-ins da web**.
2. Na janela que se abre, clique no botão **Adicionar**.

   A lista de plugins disponíveis é exibida.

3. Na lista de plugins disponíveis, selecione o plugin que deseja baixar (por exemplo, Kaspersky Endpoint Security 11 for Windows) clicando no seu nome.

   Uma página de descrição de plugin é exibida.

4. Na página de descrição do plugin, clique em **Instalar o plug-in**.

5. Quando a instalação for concluída, clique em **OK**.

O plugin de gerenciamento é baixado com a configuração padrão e exibido na lista de plugins de gerenciamento.

Você pode adicionar plugins e atualizar plugins baixados de um arquivo. Os plug-ins de gerenciamento e plug-ins de gerenciamento da Web podem ser baixados da página do Suporte Técnico da Kaspersky.

Para baixar ou atualizar o plugin de um arquivo:

1. No menu principal, vá para **Configurações do console** → **Plug-ins da web**.

2. Execute uma das seguintes ações:

   - Clique em **Adicionar do arquivo** para baixar um plugin de um arquivo.
   - Clique em **Atualizar a partir do arquivo** para baixar uma atualização de um plugin de um arquivo.

3. Especifique o arquivo e a assinatura do arquivo.

4. Baixe os arquivos especificados.

O plugin de gerenciamento é baixado do arquivo e exibido na lista de plugins de gerenciamento.

Download e criação de pacotes de instalação para aplicativos Kaspersky

Você poderá criar pacotes de instalação para aplicativos Kaspersky de servidores Web da Kaspersky se o Servidor de Administração tiver acesso à Internet.

Para baixar e criar o pacote de instalação para aplicativos Kaspersky:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.
   - No menu principal, vá para **Operações** → **Repositórios** → **Pacotes de instalação**.

   Você também pode visualizar as notificações sobre novos pacotes para aplicativos Kaspersky na lista de notificações na tela. Se houver notificações sobre um novo pacote, você poderá clicar no link ao lado da notificação e prosseguir para a lista de pacotes de instalação disponíveis.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Clique em **Adicionar**.

   O Assistente de novo pacote inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Selecione **Criar um pacote de instalação para um aplicativo da Kaspersky**.

   Uma lista dos pacotes de instalação disponíveis nos servidores da Web Kaspersky é exibida. A lista contém pacotes de instalação apenas para os aplicativos compatíveis com a versão atual do Kaspersky Security Center.

4. Clique no nome de um pacote de instalação, por exemplo, Kaspersky Endpoint Security for Windows (11.1.0).

   Uma janela é exibida com informações sobre o pacote de instalação.

   > Se estiver em conformidade com as leis e os regulamentos aplicáveis, você poderá baixar e usar um pacote de instalação que inclui ferramentas criptográficas que implementam criptografia forte. Para baixar o pacote de instalação do Kaspersky Endpoint Security for Windows válido para as necessidades da sua organização, consulte a legislação do país em que os dispositivos clientes da sua organização estão localizados.

5. Leia as informações e clique no botão **Baixar e criar o pacote de instalação**.

   Se um pacote de distribuição não puder ser convertido em um pacote de instalação, o botão **Baixar o pacote de distribuição** é exibido em vez da opção **Baixar e criar o pacote de instalação**.

   O download do pacote de instalação para o Servidor de Administração é iniciado. É possível fechar a janela do assistente ou prosseguir para a próxima etapa da instrução. Caso a janela do assistente seja fechada, o processo de download continuará no modo de segundo plano.

   Se você deseja acompanhar um processo de download do pacote de instalação:

   a. No menu principal, vá para **Operações → Repositórios → Pacotes de instalação → Em andamento ()**.

   b. Acompanhe o progresso da operação na coluna **Progresso do download** e na coluna **Status do download** da tabela.

   Quando o processo for concluído, o pacote de instalação será adicionado à lista na guia **Baixado**. Se o processo de download for interrompido e o status do download mudar para **Aceitar EULA**, clique no nome do pacote de instalação e prossiga para a próxima etapa da instrução.

   > Se o tamanho dos dados contidos no pacote de distribuição selecionado exceder o limite atual, uma mensagem de erro será exibida. É possível alterar o valor limite e prosseguir com a criação do pacote de instalação.

6. Para alguns aplicativos da Kaspersky, o botão **Mostrar EULA** será exibido durante o processo de download. Se ele for exibido, faça o seguinte:

   a. Clique no botão **Mostrar EULA** para ler o Contrato de Licença do Usuário Final (EULA).

   b. Leia o EULA exibido na tela e clique em **Aceitar**.

      O download continua depois que você aceita o EULA. Se clicar em **Recusar**, o download será interrompido.

7. Quando o download for concluído, clique no botão **Fechar**.

O pacote de instalação selecionado é baixado para a pasta compartilhada do Servidor de Administração, na subpasta Pacotes. Após o download, o pacote de instalação é exibido na lista de pacotes de instalação.

Alteração do limite de tamanho dos dados de pacotes de instalação personalizada

O tamanho total dos dados descompactados durante a criação de um pacote de instalação personalizada é limitado. O limite padrão é 1 GB.

Se você tentar carregar um arquivo compactado que contém dados que excedam o limite atual, uma mensagem de erro será exibida. Pode ser necessário aumentar esse valor limite ao criar pacotes de instalação a partir de pacotes de distribuição grandes.

Para alterar o valor limite para o tamanho do pacote de instalação personalizada:

1. No dispositivo do Servidor de Administração, execute o prompt de comando na conta que foi usada para instalar o Servidor de Administração.

2. Altere o diretório atual para a pasta de instalação do Kaspersky Security Center (geralmente, <Unidade>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Dependendo do tipo de instalação do Servidor de Administração, insira um dos seguintes comandos, usando direitos de administrador:

   - Instalação local normal:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número of bytes>
     ```

   - Instalação no cluster de failover do Kaspersky Security Center:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número de bytes> --stp klfoc
     ```

   - Instalação em um cluster de failover do Windows Server:

     ```
     klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v <número de bytes> --stp cluster
     ```

   Em que <número de bytes> é um número de bytes em formato hexadecimal ou decimal.

   Por exemplo, caso o limite necessário seja 2 GB, é possível especificar o valor decimal 2147483648 ou o valor hexadecimal 0x80000000. Neste caso, para uma instalação local do Servidor de Administração, você pode usar o seguinte comando:

   ```
   klscflag -fset -pv klserver -n MaxArchivePkgSize -t d -v 2147483648
   ```

O limite de tamanho dos dados de pacotes de instalação personalizada é alterado.

Download de pacotes de distribuição para aplicativos Kaspersky

No Kaspersky Security Center Web Console, você pode baixar e salvar pacotes de distribuição para aplicativos Kaspersky. Você pode usar os pacotes de distribuição para instalar os aplicativos manualmente, sem usar o Kaspersky Security Center.

Para baixar e salvar pacotes de distribuição para aplicativos Kaspersky:

1. No menu principal, vá para **Operações → Aplicativos da Kaspersky → Versões atuais do aplicativo**.

   A lista de pacotes de distribuição, plugins e correções disponíveis é exibida. O Kaspersky Security Center exibe apenas os itens compatíveis com sua versão atual.

2. Na lista, clique no nome do pacote que deseja baixar.

   A descrição do pacote é exibida.

3. Leia a descrição e clique no botão **Baixar e criar o pacote de instalação**.

   Se um pacote de distribuição não puder ser convertido em um pacote de instalação, o botão **Baixar o pacote de distribuição** é exibido em vez de **Baixar e criar o pacote de instalação**.

   O download do pacote de instalação para o Servidor de Administração é iniciado.

O pacote de instalação ou de distribuição selecionado é baixado para a pasta compartilhada do Servidor de Administração, na subpasta **Pacotes**. Após o download, o pacote de instalação é exibido na lista de pacotes de instalação.

Verificando se o Kaspersky Endpoint Security foi implantado com sucesso

Para assegurar que você tenha implementado corretamente os aplicativos Kaspersky, como o Kaspersky Endpoint Security:

1. Ao usar o Kaspersky Security Center Web Console, certifique-se de ter o seguinte:

   - Uma política para o Kaspersky Endpoint Security e/ou outros aplicativos de segurança que você usa.
   - Tarefas para o Kaspersky Endpoint Security for Windows: tarefa *verificação rápida* e tarefa *instalar atualização* (caso o Kaspersky Endpoint Security for Windows seja usado).
   - Tarefas de outros aplicativos de segurança que você usa.

2. Em um dos dispositivos gerenciados selecionados para instalação, verifique o seguinte:

   - O Kaspersky Endpoint Security ou outro aplicativo de segurança da Kaspersky está instalado.
   - No Kaspersky Endpoint Security, as configurações de Proteção Contra Ameaças ao Arquivo, Proteção Contra Ameaças da Web e Proteção Contra Ameaças ao Correio correspondem à política criada para este dispositivo.
   - O serviço Kaspersky Endpoint Security pode ser parado e iniciado manualmente.
   - As tarefas de grupo podem ser paradas e iniciadas manualmente.

Criar pacote de instalação autônomo

Você e os usuários de dispositivos na sua organização podem usar pacotes de instalação independente para instalar os aplicativos no dispositivo manualmente.

Um pacote de instalação independente (Installer.exe) é um arquivo executável que você pode armazenar em um Servidor da Web ou na pasta compartilhada, enviar por e-mail ou transferir para um dispositivo cliente usando outro método. No dispositivo cliente, o usuário pode executar o arquivo recebido localmente para instalar um aplicativo sem envolver o Kaspersky Security Center. Você pode criar pacotes de instalação independentes para aplicativos Kaspersky e de terceiros, para as plataformas Windows, macOS e Linux. Para criar um pacote de instalação independente para um aplicativo de terceiros, você deve criar um pacote de instalação personalizado.

Certifique-se de que o pacote de instalação independente não está disponível para pessoas não autorizadas.

Para criar um pacote de instalação independente:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**.
   - No menu principal, vá para **Operações → Repositórios → Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Na lista de pacotes de instalação, selecione um pacote de instalação e, acima da lista, clique no botão **Implementar**.

3. Selecione a opção **Usando um pacote autônomo**.

   O Assistente de criação de pacote de instalação independente é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

4. Verifique e confirme se a opção **Instalar o Agente de Rede junto com este aplicativo** está ativada caso deseje instalar o Agente de Rede juntamente com o aplicativo selecionado.

   A opção é exibida conforme o aplicativo para o qual você está criando um pacote de instalação independente.

   Por padrão, esta opção está ativada. Recomendamos ativar esta opção se você não tiver certeza se o Agente de Rede está instalado no dispositivo. Se o Agente de Rede já estiver instalado no dispositivo, após a instalação do pacote de instalação independente com o Agente de Rede, esse será atualizado para a versão mais recente.

   Se você desativar esta opção, o Agente de Rede não será instalado no dispositivo e esse não será gerenciado.

   Se já existir um pacote de instalação independente para o aplicativo selecionado no Servidor de Administração, o assistente informará a respeito. Nesse caso, você deve selecionar uma das seguintes ações:

   - **Criar pacote de instalação independente**. Selecione esta opção, por exemplo, se deseja criar um pacote de instalação independente para uma nova versão do aplicativo e também deseja manter um pacote de instalação independente criado para uma versão anterior do aplicativo. O novo pacote de instalação independente é colocado em outra pasta.
   - **Usar pacote de instalação independente existente**. Selecione esta opção se desejar usar um pacote de instalação independente existente. O processo de criação do pacote não será iniciado.
   - **Recriar pacote de instalação independente existente**. Selecione esta opção se desejar criar um pacote de instalação independente para o mesmo aplicativo novamente. O pacote de instalação independente é colocado na mesma pasta.

5. Na etapa **Migrar para a lista de dispositivos gerenciados**, a opção **Não migrar dispositivos** é ativada por padrão. Se você não deseja mover o dispositivo cliente para nenhum grupo de administração após a instalação do Agente de Rede, selecione a opção ativada.

   Se quiser mover os dispositivos clientes após a instalação do Agente de Rede, selecione a opção **Migrar dispositivos não atribuídos para este grupo** e especifique um grupo de administração para o qual você deseja mover o dispositivo cliente. Por padrão, o dispositivo é movido para o grupo **Dispositivos gerenciados**.

6. Quando o processo de criação do pacote de instalação independente for concluído, clique no botão **CONCLUIR**.

   O Assistente de Criação de Pacote de Instalação Independente é fechado.

O pacote de instalação independente é criado e colocado na subpasta PkgInst da pasta compartilhada do Servidor de Administração. Você pode visualizar a lista de pacotes independentes, clicando no botão **Exibir a lista de pacotes independentes** acima da lista de pacotes de instalação.

Visualizar a lista de pacotes de instalação independente

Você pode visualizar a lista de pacotes de instalação independente e as propriedades de cada pacote de instalação independente.

Para visualizar a lista de pacotes de instalação independente para todos os pacotes de instalação:

Acima da lista, clique no botão **Exibir a lista de pacotes independentes**.

Na lista de pacotes de instalação independentes, suas propriedades são exibidas da seguinte maneira:

- **Nome do pacote**. Nome do pacote de instalação independente que é formado automaticamente como o nome do aplicativo incluído no pacote e na versão do aplicativo.
- **Nome do aplicativo**. Nome do aplicativo incluído no pacote de instalação independente.
- **Versão do aplicativo**.
- **Nome do pacote de instalação do Agente de Rede**. A propriedade será exibida apenas se o Agente de Rede estiver incluído no pacote de instalação independente.
- **Versão do Agente de Rede**. A propriedade será exibida apenas se o Agente de Rede estiver incluído no pacote de instalação independente.
- **Tamanho**. Tamanho do arquivo em MB.
- **Grupo**. Nome do grupo para o qual o dispositivo cliente é movido após a instalação do Agente de Rede.
- **Criação**. Data e hora da criação do pacote de instalação independente.
- **Modificação**. Data e hora da modificação do pacote de instalação independente.
- **Caminho**. Caminho completo para a pasta em que o pacote de instalação independente está localizado.
- **Endereço da Web**. Endereço da Web do local do pacote de instalação independente.
- **Hash do arquivo**. A propriedade é usada para certificar que o pacote de instalação independente não foi alterado por terceiros e que um usuário tem o mesmo arquivo que você criou e transferiu para o usuário.

Para visualizar a lista de pacotes de instalação independente para um pacote de instalação específico:

Selecione o pacote de instalação na lista e, acima da lista, clique no botão **Exibir a lista de pacotes independentes**.

Na lista de pacotes de instalação independentes, você pode fazer o seguinte:

- Publique um pacote de instalação independente no servidor da Web, clicando no botão **Publicar**. O pacote de instalação independente publicado está disponível para download para usuários aos quais você enviou o link para o pacote de instalação independente.
- Anular publicação de um pacote de instalação independente no Servidor Web clicando no botão **Cancelar a publicação**. O pacote de instalação independente não publicado está disponível para download apenas para você e outros administradores.
- Baixe um pacote de instalação independente para o seu dispositivo clicando no botão **Baixar**.
- Envie um e-mail com o link para um pacote de instalação independente clicando no botão **Enviar por e-mail**.
- Remova um pacote de instalação independente clicando no botão **Remover**.

Criar pacotes de instalação personalizados

Você pode usar os pacotes de instalação personalizada para fazer o seguinte:

- Instalar qualquer aplicativo (como um editor de texto) em um dispositivo cliente, por exemplo, através de uma tarefa.
- Para criar um pacote de instalação independente.

Um pacote de instalação personalizada é uma pasta com um conjunto de arquivos. Uma fonte para criar um pacote de instalação personalizado é um *arquivo morto*. O arquivo de compactação contém um ou mais arquivos que devem ser incluídos no pacote de instalação personalizada. Ao criar um pacote de instalação personalizado, é possível especificar parâmetros da linha de comandos, por exemplo, para instalar o aplicativo em modo silencioso.

Caso possua uma chave de licença ativa para o recurso Gerenciamento de patches e vulnerabilidades (VAPM), será possível converter as configurações de instalação padrão para o pacote de instalação personalizado relevante e usar os valores recomendados pelos especialistas da Kaspersky. As configurações são automaticamente convertidas durante a criação do pacote de instalação personalizado apenas se o arquivo executável correspondente estiver incluído no banco de dados de aplicativos de terceiros da Kaspersky.

Para criar um pacote de instalação personalizado:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**.
   - No menu principal, vá para **Operações → Repositórios → Pacotes de instalação**.

   Uma lista dos pacotes de instalação disponíveis no Servidor de Administração é exibida.

2. Clique em **Adicionar**.

   O Assistente de novo pacote inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Selecione **Criar um pacote de instalação a partir de um arquivo**.

4. Especifique o nome do pacote e clique no botão **Procurar**.

   Uma janela padrão de **Abrir** do Windows é abre-se no navegador e permite escolher um arquivo para criar o pacote de instalação.

5. Selecione um arquivo comprimido localizado nos discos disponíveis.

   Você pode carregar um arquivo ZIP, CAB, TAR ou TAR.GZ. Não é possível criar um pacote de instalação a partir do arquivo SFX (arquivo de extração automática).

   > Caso deseje que as configurações sejam convertidas durante a instalação do pacote, certifique-se de que a caixa de seleção **Converter as configurações para os valores recomendados para aplicativos reconhecidos pelo Kaspersky Security Center após a conclusão do assistente** esteja marcada e clique em **Avançar**.

   O carregamento do arquivo para o Servidor de Administração do Kaspersky Security Center é iniciado.

   > Se você ativou o uso das configurações de instalação recomendadas, o Kaspersky Security Center 14.2 verifica se o arquivo executável está incluído no banco de dados de aplicativos de terceiros da Kaspersky. Se a verificação for bem-sucedida, você receberá uma notificação informando que o arquivo é reconhecido. As configurações são convertidas e o pacote de instalação personalizado é criado. Nenhuma outra ação será necessária. Clique no botão **Concluir** para fechar o assistente.

6. Selecione um arquivo (na lista de arquivos extraídos do arquivo de compactação escolhido) e especifique os parâmetros da linha de comando de um arquivo executável.

   Você pode especificar parâmetros da linha de comando, para instalar o aplicativo a partir do pacote de instalação em um modo silencioso. A especificação de parâmetros da linha de comando é opcional.

   O processo para criar o pacote de instalação é iniciado.

   O assistente informa quando o processo é concluído.

   Se o pacote de instalação não for criado, a mensagem apropriada será exibida.

7. Clique no botão **Concluir** para fechar o assistente.

O pacote de instalação que você criou é baixado na subpasta Packages da pasta compartilhada do Servidor de Administração. Após o download, o pacote de instalação aparece na lista de pacotes de instalação.

Na lista de pacotes de instalação disponíveis no Servidor de Administração, clicando no link com o nome de um pacote de instalação personalizado, você pode:

- Visualize as seguintes propriedades de um pacote de instalação:
  - **Nome**. Nome do pacote de instalação personalizada.
  - **Origem**. Nome do fornecedor do aplicativo.
  - **Aplicativo**. Nome do aplicativo compactado no pacote de instalação personalizada.
  - **Versão**. Versão do aplicativo.
  - **Idioma**. Idioma do aplicativo compactado no pacote de instalação personalizada.
  - **Tamanho (MB)**. Tamanho do pacote de instalação.
  - **Sistema operacional**. Tipo do sistema operacional ao qual o pacote de instalação se destina.
  - **Criação**. Data de criação do pacote de instalação.
  - **Modificação**. Data de modificação do pacote de instalação.
  - **Tipo**. Tipo do pacote de instalação.
- Altere o nome do pacote e os parâmetros da linha de comandos. Este recurso está disponível apenas para pacotes que não são criados com base nos aplicativos Kaspersky.

Se você converteu as configurações de instalação do pacote para os valores recomendados para o processo de criação do pacote personalizado, duas seções adicionais poderão aparecer na guia **Configurações** das propriedades do pacote de instalação personalizado: **Configurações** e **Procedimento de instalação**.

A seção **Configurações** contém as seguintes propriedades, mostradas em uma tabela:

- **Nome**. Esta coluna mostra o nome atribuído a um parâmetro de instalação.
- **Tipo**. Esta coluna mostra o tipo do parâmetro de instalação.
- **Valor**. Esta coluna mostra o tipo de dados definido por um parâmetro de instalação (Bool, Filepath, Numeric, Path ou String).

A seção **Procedimento de instalação** contém uma tabela que descreve as seguintes propriedades da atualização, incluídas no pacote de instalação personalizado:

- **Nome**. O nome da atualização.
- **Descrição**. A descrição da atualização.
- **Fonte**. A fonte da atualização, isto é, se foi lançada pela Microsoft ou por outro desenvolvedor terceiro.
- **Tipo**. O tipo da atualização, ou seja, se é destinada a um driver ou aplicativo.

- **Categoria**. A categoria WSUS (Windows Server Update Services) exibida para atualizações da Microsoft (atualizações críticas, atualizações de definições, drivers, pacotes de recursos, atualizações de segurança, service packs, ferramentas, pacotes cumulativos de atualizações, atualizações ou upgrades).
- **Nível de importância segundo o MSRC**. O nível de importância da atualização definido pelo Microsoft Security Response Center (MSRC).
- **Nível de importância**. O nível de importância da atualização definido pela Kaspersky.
- **Nível de importância do patch (para patches destinados aos aplicativos Kaspersky)**. O nível de importância do patch caso se destine a um aplicativo Kaspersky.
- **Artigo**. O identificador (ID) do artigo na Base de Conhecimento que descreve a atualização.
- **Boletim**. O ID do boletim de segurança que descreve a atualização.
- **Não atribuído para instalação**. Exibe se a atualização tem o status Não atribuída para instalação.
- **A ser instalada**. Exibe se a atualização tem o status A ser instalada.
- **Instalando**. Exibe se a atualização tem o status Instalando.
- **Instalada**. Exibe se a atualização tem o status Instalada.
- **Falha**. Exibe se a atualização tem o status Falha.
- **A reinicialização é necessária**. Exibe se a atualização tem o status Reinicialização necessária.
- **Registrada**. Exibe a data e a hora em que a atualização foi registrada.
- **Instalada em modo interativo**. Exibe se a atualização requer interação com o usuário durante a instalação.
- **Revogada**. Exibe a data e a hora em que a atualização foi revogada.
- **Status de aprovação da atualização**. Exibe se a atualização está aprovada para instalação.
- **Revisão**. Exibe o número da revisão atual da atualização.
- **ID da atualização**. Exibe o ID da atualização.
- **Versão do aplicativo**. Exibe o número da versão para a qual o aplicativo será atualizado.
- **Substituída**. Exibe outras atualizações que podem substituir a atualização.
- **Substituição**. Exibe outras atualizações que podem ser substituídas pela atualização.
- **É necessário aceitar os termos do Contrato de Licença**. Exibe se a atualização requer aceitação dos termos de um Contrato de Licença do Usuário Final (EULA).
- **Fornecedor**. Exibe o nome do fornecedor da atualização.
- **Família do aplicativo**. Exibe o nome da família de aplicativos à qual a atualização pertence.
- **Aplicativo**. Exibe o nome do aplicativo ao qual a atualização pertence.

- **Idioma**. Exibe o idioma da localização da atualização.
- **Não atribuído para instalação (nova versão)**. Exibe se a atualização tem o status Não atribuída para instalação (nova versão).
- **Instalação requer pré-requisitos**. Exibe se a atualização tem o status de instalação Requer pré-requisitos.
- **Modo de download**. Exibe o modo de download da atualização.
- **É um patch**. Exibe se a atualização é um patch.
- **Não instalada**. Exibe se a atualização tem o status Não instalada.

Distribuindo pacotes de instalação para Servidores de Administração secundários

O Kaspersky Security Center permite que você crie pacotes de instalação para aplicativos Kaspersky e para aplicativos de terceiros, bem como distribuir pacotes de instalação para dispositivos clientes e instalar aplicativos por meio dos pacotes. Para otimizar a carga no Servidor de Administração principal, você pode distribuir pacotes de instalação para Servidores de Administração secundários. Depois disso, os servidores secundários transmitem os pacotes para os dispositivos clientes e você pode executar a instalação remota dos aplicativos nos dispositivos clientes.

Para distribuir pacotes de instalação para Servidores de Administração secundários:

1. Verifique se os Servidores de Administração secundários estão conectados ao Servidor de Administração principal.
2. No menu principal, vá para **Dispositivos** → **Tarefas**.

   A lista de tarefas é exibida.
3. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
4. Na página **Nova tarefa**, na lista suspensa **Aplicativo**, selecione **Kaspersky Security Center**. Em seguida, na lista suspensa **Tipo de tarefa**, selecione **Distribuir pacote de instalação** e especifique o nome da tarefa.
5. Na página **Escopo da tarefa**, selecione os dispositivos aos quais a tarefa é atribuída de uma das seguintes maneiras:
   - Se desejar criar uma tarefa para todos os Servidores de Administração secundários em um grupo de administração específico, selecione este grupo e, em seguida, crie uma tarefa de grupo para ele.
   - Se desejar criar uma tarefa para Servidores de Administração secundários específicos, selecione tais Servidores e, em seguida, crie uma tarefa para eles.
6. Na página **Pacotes de instalação distribuídos**, selecione os pacotes de instalação que devem ser copiados para os Servidores de Administração secundários.
7. Especifique uma conta para executar a tarefa *Distribuir pacote de instalação* nesta conta. É possível usar a conta e manter a opção **Conta padrão** ativada. Como alternativa, é possível especificar que a tarefa seja executada em outra conta com os direitos de acesso necessários. Para isso, selecione a opção **Especificar conta** e, em seguida, insira as credenciais dessa conta.

8. Na página **Concluir a criação da tarefa**, é possível ativar a opção **Abrir detalhes da tarefa quando a criação for concluída** para abrir a janela de propriedades da tarefa e modificar as configurações padrão da tarefa. Caso contrário, será possível definir as configurações da tarefa posteriormente, no momento oportuno.

9. Clique no botão **Concluir**.

   A tarefa criada para distribuir pacotes de instalação para os Servidores de Administração secundários é exibida na lista de tarefas.

10. É possível executar a tarefa manualmente ou aguardar que ela seja inicializada de acordo com o agendamento especificado nas configurações da tarefa.

Após a conclusão da tarefa, os pacotes de instalação selecionados são copiados para os Servidores de Administração secundários especificados.

Instalação de aplicativos usando a tarefa de instalação remota

O Kaspersky Security Center permite instalar aplicativos em dispositivos remotamente, usando tarefas de instalação remotas. Essas tarefas são criadas e atribuídas aos dispositivos por um assistente dedicado. Para atribuir uma tarefa com mais rapidez e facilidade, é possível especificar dispositivos (até mil) na janela do assistente de uma das seguintes formas:

- **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**. Neste caso, a tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

- **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**. Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

- **Atribuir a tarefa a uma seleção de dispositivos**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em uma seleção anteriormente criada. É possível especificar a seleção predefinida ou uma personalizada criada por você.

- **Atribuir tarefa a um grupo de administração**. Neste caso, a tarefa é atribuída aos dispositivos incluídos em um grupo de administração anteriormente criado.

Para evitar problemas que possam ocorrer durante a instalação do aplicativo em um dispositivo cliente sem o Agente de Rede instalado, é necessário agir conforme o descrito no procedimento de implementação forçada por meio da tarefa de instalação remota do Kaspersky Security Center.

Instalar um aplicativo remotamente

Esta seção contém informações sobre como instalar um aplicativo remotamente em um grupo de administração, dispositivos com endereços IP específicos ou uma seleção de dispositivos gerenciados.

Para instalar um aplicativo nos dispositivos específicos:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.

3. No campo **Tipo de tarefa**, selecione **Instalar o aplicativo remotamente**.

4. Selecione uma das seguintes opções:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

     Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

     Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

   - **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**

     Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

     Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

   - **Atribuir a tarefa a uma seleção de dispositivos**

     A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

     Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

5. Siga as instruções do Assistente.

   O Assistente para novas tarefas cria uma tarefa para instalação remota do aplicativo selecionado no assistente em dispositivos específicos. Se você selecionou a opção **Atribuir tarefa a um grupo de administração**, a tarefa será de grupo.

6. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que especificou nas configurações da tarefa.

Quando a tarefa de instalação remota for concluída, o aplicativo selecionado será instalado nos dispositivos específicos.

Instalar um aplicativo usando as políticas de grupo do Active Directory

O Kaspersky Security Center permite instalar os aplicativos Kaspersky em dispositivo gerenciados, usando as políticas de grupo do Active Directory.

Você pode instalar aplicativos usando as políticas de grupo do Active Directory apenas dos pacotes de instalação que incluam Agente de Rede.

Para instalar um aplicativo usando as políticas de grupo do Active Directory:

1. Execute o Assistente de implementação da proteção. Siga as instruções do Assistente.
2. Na página **Configurações da tarefa de instalação remota** do Assistente de Implementação da Proteção, habilite a opção **Atribuir a instalação do pacote em políticas de grupo do Active Directory**.
3. Na página **Selecionar contas para acessar os dispositivos**, selecione a opção **Conta necessária (Agente de Rede não é usado)**.
4. Adicionar a conta com privilégios de administrador no dispositivo onde o Kaspersky Security Center é instalado ou na conta incluída no grupo de domínio Proprietários do criador de política de grupo.
5. Conceda as permissões para a conta selecionada:
   a. Acesse **Painel de Controle** → **Ferramentas Administrativas** e abra **Gerenciamento de Política de Grupo**.
   b. Clique no nó com o domínio desejado.
   c. Clique na seção **Delegação**.
   d. Na lista suspensa de **Permissão**, selecione **Vincular GPOs**.
   e. Clique em **Adicionar**.
   f. Na janela aberta **Selecionar usuário, computador ou grupo**, selecione a conta desejada.
   g. Clique em **OK** para fechar a janela **Selecionar usuário, computador ou grupo**.
   h. Na lista **Grupos e usuários**, selecione a conta recém-adicionada, depois clique em **Avançado** → **Avançado**.
   i. Na lista **Entradas de permissão**, clique duas vezes na conta recém-adicionada.
   j. Conceda as seguintes permissões:
      - **Criar objetos de grupo**
      - **Excluir objetos de grupo**
      - **Criar objetos de contêiner de política de grupo**
      - **Excluir objetos de contêiner de política de grupo**
   k. Clique em **OK** para salvar as alterações.
6. Defina outras configurações seguindo as instruções do assistente.
7. Execute manualmente a tarefa de instalação remota criada ou aguarde pelo seu início programado.

Isto inicia a seguinte sequência de instalação remota:

1. Quando a tarefa estiver em execução, os seguintes objetos são criados em cada domínio que inclui os quaisquer dispositivos cliente do conjunto especificado:

   - Objeto da política de grupo (GPO) sob o nome **Kaspersky_AK{GUID}**.

   - Um grupo de segurança que corresponde à GPO. Esse grupo de segurança inclui dispositivos cliente abrangidos pela tarefa. O conteúdo do grupo de segurança define o escopo da GPO.

2. O Kaspersky Security Center instala os aplicativos Kaspersky selecionados nos dispositivos cliente diretamente do KLSHARE, que é a pasta de rede compartilhada no aplicativo. Na pasta de instalação do Kaspersky Security Center, será criada uma subpasta auxiliar que contém o arquivo .msi para o aplicativo a ser instalado.

3. Quando novos dispositivos são adicionados ao escopo da tarefa, são adicionados ao grupo de segurança após o início da próxima tarefa. Se a opção **Executar tarefas ignoradas** estiver selecionada no agendamento da tarefa, os dispositivos são adicionados imediatamente ao grupo de segurança.

4. Quando dispositivos são excluídos do escopo da tarefa, são excluídos também do grupo de segurança após o início da próxima tarefa.

5. Quando uma tarefa for excluída do Active Directory, a GPO, o link para o GPO e o grupo de segurança correspondente serão excluídos também.

Se quiser aplicar outro esquema de instalação usando o Active Directory, você pode definir as configurações necessárias manualmente. Por exemplo, isso poderá ser necessário nos seguintes casos:

- Quando o administrador da proteção de antivírus não tem direitos para efetuar alterações ao Active Directory de determinados domínios;

- Quando o pacote de instalação original tiver que ser armazenado em um recurso de rede separado;

- Quando é necessário vincular uma GPO a unidades específicas do Active Directory.

Estão disponíveis as opções que se seguem para usar um esquema de instalação alternativo através do Active Directory:

- Se a instalação tiver que ser realizada diretamente da pasta compartilhada do Kaspersky Security Center, nas propriedades da GPO do Active Directory especifique o arquivo .msi localizado na subpasta de execução da pasta do pacote de instalação para obter o aplicativo desejado.

- Se o pacote de instalação tiver de ser localizado em outro recurso de rede, é necessário copiar a totalidade do conteúdo da pasta exec, já que além do arquivo com a extensão, a pasta contém arquivos de configuração gerados quando o pacote foi criado. Para instalar a chave de licença com o aplicativo, copie também o arquivo de chave para essa pasta.

Instalando aplicativos nos Servidores de Administração secundários

Para instalar um aplicativo em Servidores de Administração secundários:

1. Estabeleça uma conexão ao Servidor de Administração que controla os Servidores de Administração secundários relevantes.

2. Certifique-se de que o pacote de instalação corresponde ao aplicativo sendo instalado em cada um dos Servidores de Administração secundários selecionados. Se você não encontrar o pacote de instalação em nenhum dos Servidores secundários, distribua-o. Para este efeito, crie uma tarefa com o tipo de tarefa **Distribuir pacote de instalação**.

3. Crie uma tarefa para uma instalação de aplicativo remoto em Servidores de Administração secundários. Selecione o tipo de tarefa **Instalar o aplicativo no Servidor de Administração secundário remotamente**.

   O Assistente para novas tarefas cria uma tarefa para instalação remota do aplicativo selecionado no assistente em Servidores de Administração secundários específicos.

4. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que especificou nas configurações da tarefa.

Quando a tarefa de instalação remota for concluída, o aplicativo selecionado será instalado nos Servidores de Administração secundários.

Especificando configurações para instalação remota em dispositivos Unix

Ao instalar um aplicativo em um dispositivo Unix usando uma tarefa de instalação remota, você pode especificar configurações específicas do Unix para a tarefa. Essas configurações estão disponíveis nas propriedades da tarefa depois da tarefa ser criada.

Para especificar configurações específicas do Unix para uma tarefa de instalação remota:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Clique no nome da tarefa de instalação remota para a qual deseja especificar as configurações específicas do Unix.

   A janela de propriedades da tarefa é aberta.

3. Acesse **Configurações do aplicativo** → **Configurações Unix específicas**.

4. Especificar as seguintes configurações:

   - **Defina uma senha para a conta raiz (apenas para implementação via SSH)**

     Se o comando `sudo` não puder ser usado no dispositivo de destino sem especificar a senha, selecione esta opção e, em seguida, especifique a senha para a conta raiz. Kaspersky Security Center transmite a senha de forma criptografada para o dispositivo de destino, descriptografa a senha e inicia o procedimento de instalação em nome da conta raiz com a senha especificada.

     Kaspersky Security Center não usa a conta ou a senha especificada para criar uma conexão SSH.

   - **Especifique o caminho para uma pasta temporária com permissões de execução no dispositivo de destino (apenas para implementação via SSH)**

     Se o diretório/tmp no dispositivo de destino não tiver permissão de execução, selecione esta opção e, a seguir, especifique o caminho para o diretório com a permissão de execução. O Kaspersky Security Center usa o diretório especificado como um diretório temporário para acessar pelo SSH. O aplicativo coloca o pacote de instalação no diretório e executa o procedimento de instalação.

5. Clique no botão **Salvar**.

   As configurações de tarefa especificadas são salvas.

Início e interrupção de aplicativos da Kaspersky

É possível usar a tarefa *Iniciar ou interromper aplicativo* para iniciar e interromper os aplicativos da Kaspersky em dispositivos gerenciados.

Para criar a tarefa Iniciar ou interromper aplicativo:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na lista suspensa **Aplicativo**, selecione o aplicativo ao qual se deseja criar uma tarefa.

   Os aplicativos da Kaspersky serão exibidos na lista caso você tenha anteriormente adicionado os plug-ins de gerenciamento da web para esses aplicativos.
4. Na lista **Tipo de tarefa**, selecione a tarefa **Ativação do aplicativo**.
5. No campo **Nome da tarefa**, especifique o nome da nova tarefa.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).
6. Selecione os dispositivos aos quais a tarefa será atribuída.

7. Na janela **Aplicativos**, faça o seguinte:

   - Marque as caixas de seleção ao lado dos nomes dos aplicativos para os quais se deseja criar a tarefa.
   - Selecione a opção **Iniciar aplicativo** ou **Parar aplicativo**.

8. Caso queira modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na etapa **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.

10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

11. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades e, em seguida, salve-as.

A tarefa é criada e configurada.

Caso queira executar a tarefa, basta selecioná-la na lista de tarefas e, então, clicar no botão **Iniciar**.

Gerenciamento de Dispositivos Móveis

O gerenciamento da proteção de dispositivos móveis através do Kaspersky Security Center é executado usando o recurso Gerenciamento de Dispositivos Móveis, o qual requer uma licença dedicada. Se você pretende gerenciar dispositivos móveis de propriedade dos funcionários da sua organização, ative o Gerenciamento de Dispositivos Móveis.

O Gerenciamento de Dispositivos Móveis permite gerenciar os dispositivos Android dos funcionários. A proteção é fornecida pelo aplicativo móvel Kaspersky Endpoint Security for Android instalado nos dispositivos. Este aplicativo móvel garante a proteção de dispositivos móveis contra ameaças da web, vírus e outros programas que representam ameaças. Para gerenciamento centralizado por meio Kaspersky Security Center Web Console, você deve instalar os seguintes plugins de gerenciamento da web no dispositivo onde o Kaspersky Security Center Web Console está instalado:

- Plugin do Kaspersky Security for Mobile
- Plugin do Kaspersky Endpoint Security for Android.

Para obter informações sobre a implementação de proteção e gerenciamento de dispositivos móveis, consulte a Ajuda do Kaspersky Security for Mobile.

Modificar as configurações do Gerenciamento de Dispositivos Móveis no Kaspersky Security Center Web Console

Para modificar as configurações de Gerenciamento de Dispositivos Móveis:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Portas adicionais**.

3. Modifique as configurações relevantes:

   - **Abrir porta para dispositivos móveis**

     Caso este botão de alternância esteja ativado, a porta para dispositivos móveis será aberta no Servidor de Administração.

     Você pode usar a porta para dispositivos móveis somente se o componente Gerenciamento de Dispositivos Móveis estiver instalado.

     Caso o botão de alternância esteja desativado, a porta para dispositivos móveis no Servidor de Administração não será usada.

     Por padrão, o botão de alternância está desativado.

   - **Porta para sincronização de dispositivos móveis**

     Número da porta SSL usada para conexão de dispositivos móveis ao Servidor de Administração. O número da porta padrão é 13292.

     É usado o sistema decimal para registros.

   - **Porta para ativação de dispositivos móveis**

     A porta para conexão do Kaspersky Endpoint Security for Android para os servidores de ativação da Kaspersky.

     O número da porta padrão é 17100.

4. Clique no botão **Salvar**.

Os dispositivos móveis poderão agora ser conectados ao Servidor de Administração.

Substituição de aplicativos de segurança de terceiros

A Instalação de aplicativos de segurança da Kaspersky através do Kaspersky Security Center pode necessitar a remoção de software de terceiros incompatível com o aplicativo sendo instalado. O Kaspersky Security Center fornece vários modos de remover os aplicativos de terceiros.

Remoção de aplicativos incompatíveis usando o instalador

Esta opção está disponível no Console de Administração com base no Console de Gerenciamento Microsoft.

O método do instalador de remoção de aplicativos incompatíveis tem suporte em vários tipos de instalação. Antes da instalação do aplicativo de segurança, todos os aplicativos incompatíveis são removidos automaticamente se a janela de propriedades do pacote de instalação deste aplicativo de segurança (seção **Aplicativos incompatíveis**) tiver a opção **Desinstalar automaticamente aplicativos incompatíveis** selecionada.

Remoção de aplicativos incompatíveis ao configurar a instalação remota de um aplicativo

Você pode ativar a opção **Desinstalar automaticamente aplicativos incompatíveis** ao configurar a instalação remota de um aplicativo de segurança. No Console de Administração com base no Console de Gerenciamento Microsoft (MMC), esta opção está disponível no Assistente de instalação remota. No Kaspersky Security Center Web Console, você pode encontrar essa opção no Assistente de implementação da proteção. Quando esta opção está ativada, o Kaspersky Security Center remove aplicativos incompatíveis antes de instalar um aplicativo de segurança em um dispositivo gerenciado.

Instruções de como proceder:

- Console de Administração: Remoção de aplicativos com o uso do Assistente de Instalação Remota
- Kaspersky Security Center Web Console: Remover aplicativos incompatíveis antes da instalação

Remover aplicativos incompatíveis através de uma tarefa dedicada

Para remover aplicativos incompatíveis, use a tarefa **Desinstalar o aplicativo remotamente**. Esta tarefa deve ser executada nos dispositivos antes da execução da tarefa de instalação do aplicativo de segurança. Por exemplo, na tarefa de instalação, você pode selecionar o tipo de agendamento **Na conclusão de outra tarefa** onde a outra tarefa for **Desinstalar o aplicativo remotamente**.

Este método da desinstalação é útil quando o instalador do aplicativo de segurança não puder remover apropriadamente um aplicativo incompatível.

Instruções do Console de Administração: Criando uma tarefa.

Localizar dispositivos na rede

Esta seção descreve a pesquisa e a descoberta de dispositivos em rede.

O Kaspersky Security Center permite encontrar dispositivos com base em critérios especificados. Você pode salvar os resultados da pesquisa em um arquivo de texto.

O recurso de pesquisa e localização lhe permite localizar os seguintes dispositivos:

- Os dispositivos gerenciados nos grupos de administração do Servidor de Administração do Kaspersky Security Center e seus Servidores de Administração secundários.
- Dispositivos não atribuídos gerenciados por Servidor de Administração do Kaspersky Security Center e seus Servidores de Administração secundários.

Cenário: Localizar dispositivos na rede

Você deve executar a localização de dispositivos antes da instalação dos aplicativos de segurança. O Servidor de Administração recebe informações sobre dispositivos descobertos e permite o gerenciamento dos dispositivos por meio de políticas. Sondagens de rede regulares são necessárias para atualizar a lista de dispositivos disponíveis na rede.

Antes de iniciar a sondagem da rede, verifique e confirme se o protocolo SMB está ativado. Caso contrário, o Kaspersky Security Center não poderá descobrir dispositivos na rede submetida a sondagem. Para ativar o protocolo SMB, siga as instruções para o seu sistema operacional.

A descoberta de dispositivos em rede ocorre nos seguintes estágios:

1. **Descobrir dispositivos**

   O Assistente de início rápido lhe guia através da descoberta de dispositivos inicial e ajuda a localizar os dispositivos na rede, tal como computadores, tablets e celulares. Você também pode realizar a localização de dispositivos manualmente.

2. **Configurar sondagens agendadas**

   Decida qual(is) tipo(s) de sondagem deseja usar regularmente. Ative os tipos desejados e configure o agendamento de sondagem. É possível se referir às recomendações para frequência de sondagem de rede.

3. **Configuração de regras para adicionar dispositivos descobertos aos grupos de administração (opcionais)**

   Se novos dispositivos aparecerem na sua rede, eles serão descobertos durante as sondagens regulares e automaticamente incluídos no grupo **Dispositivos não atribuídos**. É possível configurar regras de movimento de dispositivos para alocar automaticamente os dispositivos para o grupo **Dispositivos gerenciados**. Também é possível configurar regras de retenção.

   Caso a etapa 3 seja ignorada, os dispositivos recém-descobertos serão alocados para o grupo **Dispositivos não atribuídos**. Se quiser, você poderá mover esses dispositivos para o grupo **Dispositivos gerenciados** manualmente. Caso os dispositivos sejam movidos manualmente para o grupo **Dispositivos gerenciados**, é possível analisar as informações sobre cada dispositivo e decidir se deseja movê-lo para um grupo de administração e, neste caso, para qual grupo exatamente.

Resultados

A conclusão do cenário produz o seguinte:

- O Servidor de Administração do Kaspersky Security Center descobre os dispositivos que estão na rede e fornece informações sobre eles.
- As sondagens futuras são realizadas segundo o agendamento especificado.
- Os dispositivos recém-descobertos são organizados de acordo com as regras configuradas. (Ou, se nenhuma regra estiver configurada, os dispositivos permanecerão no grupo **Dispositivos não atribuídos**).

Localização dos dispositivos

Esta seção descreve os tipos de descoberta de dispositivos disponíveis no Kaspersky Security Center e fornece informações sobre o uso de cada tipo.

O Servidor de Administração recebe informações sobre a estrutura da rede e os dispositivos nessa rede por meio de sondagem regular. As informações são registradas no banco de dados do Servidor de Administração. O Servidor de Administração pode usar os seguintes tipos de sondagem:

- **Sondagem da rede do Windows**. O Servidor de Administração pode executar dois tipos de sondagem de rede do Windows: rápida e completa. Durante uma sondagem rápida, o Servidor de Administração somente recupera a informação da lista dos nomes de NetBIOS dos dispositivos em todos os domínios da rede e grupos de trabalho. Durante a sondagem completa, são solicitadas mais informações de cada dispositivo cliente, como nome do sistema operacional, endereço IP, nome DNS e nome NetBIOS. Por padrão, as sondagens rápida e completa estão ativadas. A sondagem de rede do Windows pode não conseguir descobrir dispositivos, por exemplo, se as portas UDP 137, UDP 138, TCP 139 estiverem fechadas no roteador ou forem fechadas pelo firewall.
- **Sondagem do Active Directory**. O Servidor de Administração recupera informações sobre a estrutura da unidade do Active Directory e sobre os nomes DNS dos dispositivos dos grupos do Active Directory. Por padrão, esse tipo de sondagem está ativado. Recomendamos usar a sondagem do Active Directory, caso o Active Directory seja usado; caso contrário, o Servidor de Administração não descobrirá nenhum dispositivo. Se você usar o Active Directory, mas alguns dos dispositivos em rede não forem listados como membros, esses dispositivos não poderão ser descobertos pela sondagem do Active Directory.
- **Sondagem de intervalos de IP**. O Servidor de Administração fará a sondagem dos conjuntos de IPs especificados usando pacotes ICMP ou o protocolo NBNS e compilará um conjunto de dados completo nos dispositivos dentro dos conjuntos de IPs. Por padrão, esse tipo de sondagem está desativado. Não se recomenda usar esse tipo de sondagem se você usar a sondagem da rede do Windows e/ou a sondagem do Active Directory.
- **Sondagem zeroconf**. Um ponto de distribuição que sonda a rede IPv6 usando rede zero configuração (também referida como *Zeroconf*). Por padrão, esse tipo de sondagem está desativado. Você pode usar a sondagem do Zeroconf se o ponto de distribuição executar Linux.

Se você tiver configurado e ativado as regras para migrar dispositivos, os dispositivos recentemente descobertos estarão automaticamente incluídos no grupo **Dispositivos gerenciados**. Se nenhuma regra de movimento tiver sido ativada, os dispositivos recentemente descobertos serão automaticamente incluídos no grupo **Dispositivos não atribuídos**.

Você pode modificar as configurações de descoberta de dispositivo para cada tipo. Por exemplo, é possível modificar o agendamento de amostragem ou definir se deve amostrar toda a floresta do Active Directory ou apenas um domínio específico.

Antes de iniciar a sondagem da rede, verifique e confirme se o protocolo SMB está ativado. Caso contrário, o Kaspersky Security Center não poderá descobrir dispositivos na rede submetida a sondagem. Para ativar o protocolo SMB, siga as instruções para o seu sistema operacional.

Sondagem da rede do Windows

Sobre a sondagem de rede do Windows

Durante uma sondagem rápida, o Servidor de Administração somente recupera a informação da lista dos nomes de NetBIOS dos dispositivos em todos os domínios da rede e grupos de trabalho. Durante uma sondagem completa, as seguintes informações são solicitadas de cada dispositivo cliente:

- Nome de sistema operacional
- Endereço IP
- Nome DNS
- Nome NetBIOS

As sondagens rápida e completa requerem o seguinte:

- Portas UDP 137/138, TCP 139, UDP 445, TCP 445 devem estar disponíveis na rede.
- O protocolo SMB está ativado.
- O serviço Microsoft Computer Browser deve ser usado, e o navegador principal do computador deve estar ativado no Servidor de Administração.
- O serviço Microsoft Computer Browser deve ser usado, e o navegador principal do computador deve estar ativado nos dispositivos cliente:
  - Em pelo menos um dispositivo, se o número de dispositivos em rede não exceder 32.
  - Em pelo menos um dispositivo para cada 32 dispositivos em rede.

A sondagem completa poderá ser executada apenas se a sondagem rápida tiver sido executada pelo menos uma vez.

Visualização e alteração das configurações para a sondagem da rede Windows

Para modificar as propriedades da sondagem da rede do Windows:

1. No menu principal, vá para **Descoberta e implementação** → **Descoberta** → **Domínios do Windows**.
2. Clique no botão **Propriedades**.

   A janela Propriedades do domínio do Windows é exibida.
3. Ative ou desative a sondagem de rede do Windows usando o botão de alternância **Ativar sondagem da rede Windows**.
4. Configure o agendamento da amostragem. Por padrão, a amostragem rápida é executada a cada 15 minutos, e a amostragem completa, a cada 60 minutos.

   Opções de agendamento da sondagem:

   - **A cada N dias**

     A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

     Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

   - **A cada N minutos**

     A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

   - **Por dias da semana**

     A sondagem é executada regularmente, nos dias da semana e na hora especificados.

   - **Todos os meses em dias especificados das semanas selecionadas**

     A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

   - **Executar tarefas ignoradas**

     Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

     Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

     Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

     Por padrão, esta opção está desativada.
5. Clique no botão **Salvar**.

As propriedades são salvas e aplicadas a todos os domínios e grupos de trabalho do Windows descobertos.

Execução da amostragem manualmente

Para executar a amostragem imediatamente,

Clique em **Iniciar sondagem rápida** ou **Iniciar sondagem completa**.

Quando a amostragem é completa, você pode exibir a lista de dispositivos descobertos na página **Domínios do Windows** marcando a caixa de seleção ao lado de um nome de domínio e clicando no botão **Dispositivos**.

Sondagem do Active Directory

Use a sondagem do Active Directory se você usar o Active Directory; caso contrário, recomenda-se usar outros tipos de sondagem. Se você usar o Active Directory, mas alguns dos dispositivos em rede não forem listados como membros, esses dispositivos não poderão ser descobertos usando a sondagem do Active Directory.

O Kaspersky Security Center envia uma solicitação ao controlador de domínio e recebe a estrutura de dispositivos do Active Directory. A sondagem do Active Directory é executada de hora em hora.

Antes de iniciar a sondagem da rede, verifique e confirme se o protocolo SMB está ativado. Caso contrário, o Kaspersky Security Center não poderá descobrir dispositivos na rede submetida a sondagem. Para ativar o protocolo SMB, siga as instruções para o seu sistema operacional.

Visualização e modificação de configurações para sondagem do Active Directory

Para visualizar e modificar as configurações para sondagem do Active Directory:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Active Directory**.
2. Clique no botão **Propriedades**.

   A janela Propriedades do Active Directory é aberta.

3. Na janela de propriedades do Active Directory, é possível definir as seguintes configurações:

   a. Ative ou desative a sondagem do Active Directory usando o botão de alternância.

   b. Alterar o agendamento da sondagem.

      O período padrão é de uma hora. Os dados recebidos na próxima sondagem substituem completamente os dados antigos.

   c. Defina configurações avançadas para selecionar o escopo de sondagem:

      - Domínio do Active Directory ao qual o Kaspersky Security Center pertence
      - A floresta de domínio à qual o Kaspersky Security Center pertence
      - Lista especificada de domínios do Active Directory

      Para adicionar um domínio ao escopo de amostragem, selecione uma opção de domínio, clique no botão **Adicionar** e especifique o endereço do controlador de domínio e o nome e a senha da conta para acessá-lo.

4. Para aplicar as novas configurações, clique no botão **Salvar**.

As novas configurações são aplicadas à sondagem do Active Directory.

Execução da amostragem manualmente

Para executar a amostragem imediatamente,

clique em **Iniciar sondagem**.

Visualização dos resultados da sondagem do Active Directory

Para visualizar os resultados da sondagem do Active Directory:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Active Directory**.

   A lista de unidades organizacionais descobertas é exibida.

2. Se quiser, selecione uma unidade organizacional e clique no botão **Dispositivos**.

   A lista de dispositivos na unidade organizacional é exibida.

Você pode pesquisar a lista e filtrar os resultados.

Sondagem do conjunto de IPs

Inicialmente, o Kaspersky Security Center adquire conjuntos de IPs para amostragem a partir das configurações de rede do dispositivo no qual está instalado. Se o endereço de dispositivo for 192.168.0.1 e a máscara de sub-rede for 255.255.255.0, o Kaspersky Security Center incluirá a rede 192.168.0.0/24 na lista do endereço de amostragem automaticamente. O Kaspersky Security Center faz a amostragem de todos os endereços de 192.168.0.1 a 192.168.0.254.

Não se recomenda usar a amostragem de conjuntos de IPs se você usar a amostragem de rede do Windows e/ou a amostragem do Active Directory.

O Kaspersky Security Center pode pesquisar intervalos de IP por pesquisa de DNS reverso ou usando o protocolo NBNS:

- **Pesquisa de DNS reverso**

  O Kaspersky Security Center tenta executar a resolução de nome inversa para cada endereço IP do intervalo especificado para um nome de DNS usando as solicitações de DNS padrão. Se essa operação tiver sucesso, o servidor enviará uma `ICMP ECHO REQUEST` (da mesma forma que o comando ping) ao nome recebido. Se o dispositivo responder, as informações sobre ele serão adicionadas ao banco de dados do Kaspersky Security Center. A resolução de nome inversa é necessária para excluir os dispositivos de rede que podem ter um endereço IP, mas não são computadores, por exemplo, impressoras em rede ou roteadores.

  Esse método de sondagem depende de um serviço de DNS local corretamente configurado. Ele deve ter uma zona de pesquisa inversa. Nas redes em que o Active Directory é usado, tal zona é mantida automaticamente. Mas nessas redes, a amostragem de subrede IP não fornece mais informações do que a amostragem do Active Directory. Além disso, os administradores de pequenas redes muitas vezes não configuram a zona de pesquisa inversa porque não ela é necessária para o funcionamento de muitos serviços de rede. Por esses motivos, a sondagem de sub-rede de IP é desativada por padrão.

- **Protocolo NBNS**

  Se a resolução de nome reverso não for possível em sua rede por algum motivo, o Kaspersky Security Center usa o protocolo NBNS para pesquisar os conjuntos de IPs. Se uma solicitação para um endereço IP retornar um nome NetBIOS, as informações sobre este dispositivo serão adicionadas ao banco de dados do Kaspersky Security Center.

Antes de iniciar a sondagem da rede, verifique e confirme se o protocolo SMB está ativado. Caso contrário, o Kaspersky Security Center não poderá descobrir dispositivos na rede submetida a sondagem. Para ativar o protocolo SMB, siga as instruções para o seu sistema operacional.

Visualização e modificação de configurações para amostragem de faixas IP

Para visualizar e modificar as propriedades para amostragem de faixas IP:

1. No menu principal, vá para **Descoberta e implementação** → **Descoberta** → **Intervalos de IPs**.
2. Clique no botão **Propriedades**.

   A janela de propriedades da Sondagem de IPs se abre.
3. Ative ou desative a Sondagem de IPs usando o botão de alternar **Permitir a sondagem**.

4. Configure o agendamento da amostragem. Por padrão, a amostragem de IP é executada a cada 420 minutos (sete horas).

   Ao especificar o intervalo de amostragem, assegure-se de que essa configuração não exceda o valor do parâmetro de duração do endereço IP. Se um endereço IP não for verificado por sondagem durante a duração do endereço IP, esse endereço IP será automaticamente removido dos resultados da sondagem. Por padrão, a duração dos resultados da sondagem é de 24 horas, pois os endereços IP dinâmicos (atribuídos com o uso de Dynamic Host Configuration Protocol (DHCP)) mudam a cada 24 horas.

   Opções de agendamento da sondagem:

   - **A cada N dias**

     A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

     Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

   - **A cada N minutos**

     A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

   - **Por dias da semana**

     A sondagem é executada regularmente, nos dias da semana e na hora especificados.

   - **Todos os meses em dias especificados das semanas selecionadas**

     A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

   - **Executar tarefas ignoradas**

     Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

     Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

     Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

     Por padrão, esta opção está desativada.

5. Clique no botão **Salvar**.

As propriedades são salvas e aplicadas a todos os conjuntos de IPs.

Execução da amostragem manualmente

Para executar a amostragem imediatamente,

clique em **Iniciar sondagem**.

Adição e modificação de um conjunto de IPs

Inicialmente, o Kaspersky Security Center adquire conjuntos de IPs para amostragem a partir das configurações de rede do dispositivo no qual está instalado. Se o endereço de dispositivo for 192.168.0.1 e a máscara de sub-rede for 255.255.255.0, o Kaspersky Security Center incluirá a rede 192.168.0.0/24 na lista do endereço de amostragem automaticamente. O Kaspersky Security Center faz a amostragem de todos os endereços de 192.168.0.1 a 192.168.0.254. Você pode modificar os conjuntos de IPs definidos automaticamente ou adicionar conjuntos de IPs personalizados.

Você pode criar um intervalo apenas para endereços IPv4. Se você ativar a sondagem Zeroconf, o Kaspersky Security Center sondará toda a rede.

Para adicionar um novo conjunto de IPs:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Intervalos de IPs**.
2. Para adicionar um novo conjunto de IPs, clique no botão **Adicionar**.
3. Na janela que for aberta, especifique as seguintes configurações:
   - **Nome do intervalo IP**

     Um nome do conjunto de IPs. Você pode especificar o próprio conjunto de IPs como o nome, por exemplo, "192.168.0.0/24".

   - **Intervalo de IP ou endereço e máscara de sub-rede**

     Defina o conjunto de IPs especificando os endereços IP inicial e final ou o endereço de sub-rede e a máscara de sub-rede. Você também pode selecionar um dos conjuntos de IPs já existentes clicando no botão **Procurar**.

   - **Duração do endereço IP (horas)**

     Ao especificar esse parâmetro, verifique se ele excede o conjunto de intervalos de sondagem no agendamento de sondagem. Se um endereço IP não for verificado por sondagem durante a duração do endereço IP, esse endereço IP será automaticamente removido dos resultados da sondagem. Por padrão, a duração dos resultados da sondagem é de 24 horas, pois os endereços IP dinâmicos (atribuídos com o uso de Dynamic Host Configuration Protocol (DHCP)) mudam a cada 24 horas.
4. Selecione **Ativar sondagem de intervalos IP** se quiser fazer a amostragem da sub-rede ou do intervalo que adicionou. Caso contrário, a sub-rede ou o intervalo que você adicionou não serão amostrados.
5. Clique no botão **Salvar**.

O novo conjunto de IPs é adicionado à lista de conjuntos de IPs.

Você pode executar a amostragem de cada conjunto de IPs separadamente usando o botão **Iniciar sondagem**. Quando a sondagem é concluída, será possível visualizar a lista de dispositivos descobertos usando o botão **Dispositivos**. Por padrão, a duração dos resultados da sondagem é de 24 horas e é igual à configuração de duração do endereço IP.

Para adicionar uma sub-rede a um conjunto de IPs existente:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Intervalos de IPs**.
2. Clique no nome do conjunto de IPs ao qual deseja adicionar uma sub-rede.
3. Na janela que se abre, clique no botão **Adicionar**.
4. Especifique uma sub-rede usando o seu endereço e máscara ou usando o primeiro e o último endereço IP no conjunto de IPs. Ou adicione uma sub-rede existente clicando no botão **Procurar**.
5. Clique no botão **Salvar**.

   A nova sub-rede é adicionada ao conjunto de IPs.
6. Clique no botão **Salvar**.

As novas configurações do conjunto de IPs são salvas.

Você pode adicionar quantas sub-redes precisar. Não é permitido que os conjuntos de IPs se sobreponham, mas as sub-redes não nomeadas dentro de um conjunto de IPs não têm tais restrições. Você pode ativar e desativar a amostragem independentemente para cada conjunto de IPs.

Sondagem Zeroconf

Este tipo de pesquisa é compatível apenas com pontos de distribuição baseados em Linux.

Um ponto de distribuição pode pesquisar redes que possuem dispositivos com endereços IPv6. Nesse caso, os intervalos IP não são especificados e o ponto de distribuição controla toda a rede usando a rede zero configuração (referida como *Zeroconf*). Para começar a usar o Zeroconf, você deve instalar o utilitário avahi-browse no ponto de distribuição.

Para ativar a sondagem de rede IPv6:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Intervalos de IPs**.
2. Clique no botão **Propriedades**.
3. Na janela que se abre, alterne o botão **Usar Zeroconf para sondar redes IPv6**.

Em seguida, o ponto de distribuição começa a sondar a rede. Nesse caso, os intervalos IP especificados são ignorados.

Configuração de regras de retenção para dispositivos não atribuídos

Após a conclusão da sondagem de rede do Windows, os dispositivos encontrados são colocados em subgrupos do grupo de administração de Dispositivos não atribuídos. Este grupo de administração pode ser encontrado em **Descoberta e implementação → Descoberta → Domínios do Windows**. A pasta **Domínios do Windows** é o grupo principal. Ele contém grupos denominados segundo os domínios e grupos de trabalho correspondentes encontrados durante a sondagem. O grupo principal também pode conter o grupo de administração de dispositivos móveis. Você pode configurar as regras de retenção dos dispositivos não atribuídos do grupo principal e de cada um dos grupos secundários. As regras de retenção não dependem das configurações de descoberta de dispositivos e funcionam mesmo se a descoberta de dispositivos estiver desativada.

As regras de retenção de dispositivo não afetam os dispositivos que têm uma ou mais unidades criptografadas com criptografia completa do disco. Esses dispositivos não são excluídos automaticamente. Somente é possível excluí-los manualmente. Caso necessite excluir um dispositivo com uma unidade criptografada, primeiro descriptografe a unidade e, em seguida, exclua o dispositivo.

Para configurar as regras de retenção para dispositivos não atribuídos:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Domínios do Windows**.
2. Execute uma das seguintes ações:
   - Para definir configurações do grupo principal, clique no botão **Propriedades**.

     A janela Propriedades do domínio do Windows é exibida.
   - Para definir configurações de um grupo secundário, clique no nome do grupo.

     A janela Propriedades do grupo secundário é aberta.
3. Defina as seguintes configurações:
   - **Remover o dispositivo do grupo se estiver inativo por mais de (dias)**

     Se esta opção estiver selecionada, você poderá especificar o intervalo de tempo após o qual o dispositivo será automaticamente removido do grupo. Por padrão, esta opção também é distribuída aos grupos secundários. O intervalo de tempo predefinido é de 7 dias.

     Por padrão, esta opção está ativada.
   - **Herdar do grupo principal**

     Se esta opção estiver ativada, o período de retenção para os dispositivos no grupo atual é herdado do grupo principal e não pode ser alterado.

     Esta opção está disponível somente para grupos secundários.

     Por padrão, esta opção está ativada.
   - **Forçar herança em grupos secundários**

     Os valores de configuração serão distribuídos aos grupos secundários, mas essas configurações são bloqueadas nas propriedades dos grupos secundários.

     Por padrão, esta opção está desativada.
4. Clique no botão **Aceitar**.

As suas alterações serão salvas e aplicadas.

Aplicativos Kaspersky: licenciamento e ativação

Esta seção descreve os recursos do Kaspersky Security Center relacionados ao trabalho com chaves de licença de aplicativos gerenciados da Kaspersky.

O Kaspersky Security Center lhe permite realizar a distribuição centralizada de chaves de licença para os aplicativos Kaspersky em dispositivos clientes, monitorar seu uso e renovar licenças.

Ao adicionar uma chave de licença usando o Kaspersky Security Center, as configurações da chave de licença são salvas no Servidor de Administração. Com base nestas informações, o aplicativo gera um relatório sobre o uso das chaves de licença e notifica o administrador sobre a expiração das licenças e sobre a violação das restrições de licença que estão definidas nas propriedades das chaves de licença. Você pode configurar as notificações do uso de chaves de licença dentro das configurações do Servidor de Administração.

Licenciamento de aplicativos gerenciados

Os aplicativos Kaspersky instalados em dispositivos gerenciados devem ser licenciados com a aplicação de um arquivo de chave ou um código de ativação à cada um dos aplicativos. Um arquivo de licença ou um código de ativação pode ser implementado nas seguintes formas:

- Implementação automática
- O pacote de instalação de um aplicativo gerenciado
- A tarefa de adicionar uma *chave de licença* para um aplicativo gerenciado
- Ativação manual de um aplicativo gerenciado

É possível adicionar uma nova chave de licença ativa ou reserva por qualquer um dos métodos listados acima. Um aplicativo da Kaspersky usa uma chave ativa no momento e armazena uma chave reserva para aplicar após a expiração da chave ativa. O aplicativo ao qual a chave de licença é adicionada define se a chave é ativa ou reserva. A definição da chave não depende do método usado para adicionar uma nova chave de licença.

Implementação automática

Se você usar aplicativos gerenciados diferentes e precisa implementar um arquivo de chave ou código de ativação específico para dispositivos, opte por outras formas de implementar aquele código de ativação ou arquivo de chave.

O Kaspersky Security Center lhe permite implementar automaticamente as chaves de licença disponíveis nos dispositivos. Por exemplo, três chaves de licença são armazenadas no repositório do Servidor de Administração. Se você selecionou a caixa de seleção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados** para todas as três chaves de licença. Um aplicativo de segurança da Kaspersky – por exemplo, Kaspersky Endpoint Security for Windows – é instalado nos dispositivos da organização. Um novo dispositivo é descoberto, no qual uma chave de licença deve ser implementada. O aplicativo determina, por exemplo, que duas das chaves de licença do repositório podem ser implementadas ao dispositivo: a chave de licença denominada *Key_1* e chave de licença denominada *Key_2*. Uma destas chaves de licença é implementada no dispositivo. Neste caso, não pode ser previsto qual das duas chaves de licença será implementada no dispositivo, porque a implementação automática de chaves de licença não é fornecida para nenhuma atividade do administrador.

Quando uma chave de licença é implementada, os dispositivos são recontados para aquela chave de licença. Você deve assegurar-se de que o número de dispositivos nos quais a chave de licença foi implementada não excede o limite da licença. Se o número de dispositivos exceder o limite de licença, todos os dispositivos que não foram cobertos pela licença serão terão o status *Crítico* atribuído.

Antes da implementação, o arquivo de chave ou o código de ativação deve ser adicionado ao repositório do Servidor de Administração.

Instruções de como proceder:

- Console de Administração:
  - Adição de uma chave de licença ao repositório do Servidor de Administração
  - Distribuição automática de uma chave de licença

  ou
- Kaspersky Security Center Web Console:
  - Adição de uma chave de licença ao repositório do Servidor de Administração
  - Distribuição automática de uma chave de licença

Observe que uma chave de licença distribuída automaticamente pode não ser exibida no repositório do Servidor de Administração virtual nos seguintes casos:

- A chave de licença não é válida para o aplicativo.
- O Servidor de Administração virtual não tem dispositivos gerenciados.
- A chave de licença já foi usada para dispositivos gerenciados por outro Servidor de Administração virtual e o limite no número de dispositivos foi atingido.

Adicionando um arquivo de chave ou código de ativação ao pacote de instalação de um aplicativo gerenciado

Por motivos de segurança, esta opção não é recomendada. Um arquivo de licença ou um código de ativação adicionado a um pacote de instalação pode se tornar comprometido.

Se você instalar um aplicativo gerenciado usando um pacote de instalação, poderá especificar um código de ativação ou um arquivo de chave neste pacote de instalação ou na política do aplicativo. A chave de licença será implementada nos dispositivos gerenciados no momento da próxima sincronização do dispositivo com o Servidor de Administração.

Instruções de como proceder:

- Console de Administração:
  - Criação de um pacote de instalação
  - Instalar aplicativos em dispositivos cliente

  ou
- Kaspersky Security Center Web Console: Adicionando uma chave de licença a um pacote de instalação

Implementação através da tarefa de adicionar uma chave de licença para um aplicativo gerenciado

Se você optar por usar a tarefa de *Adicionar chave de licença* para um aplicativo gerenciado, poderá selecionar a chave de licença que deve ser implementada nos dispositivos e selecionar os dispositivos de qualquer forma conveniente – por exemplo, selecionando um grupo de administração ou uma seleção de dispositivos.

Antes da implementação, o arquivo de chave ou o código de ativação deve ser adicionado ao repositório do Servidor de Administração.

Instruções de como proceder:

- Console de Administração:
  - Adição de uma chave de licença ao repositório do Servidor de Administração
  - Implementando uma chave de licença para dispositivos clientes

  ou
- Kaspersky Security Center Web Console:
  - Adição de uma chave de licença ao repositório do Servidor de Administração
  - Implementando uma chave de licença para dispositivos clientes

Adicionar um código de ativação ou um arquivo de chave manualmente nos dispositivos

Você pode ativar o aplicativo da Kaspersky instalado localmente usando as ferramentas fornecidas na interface do aplicativo. Consulte a documentação do aplicativo instalado.

Adição de uma chave de licença ao repositório do Servidor de Administração

Adicionar uma chave de licença ao repositório do Servidor de Administração:

1. No menu principal, vá para **Operações** → **Licenciamento** → **Licenças da Kaspersky**.
2. Clique no botão **Adicionar**.
3. Selecione o que você quer adicionar:
   - **Adicionar arquivo de chave**

     Clique no botão **Selecionar arquivo de chave** e navegue até o arquivo .key que deseja adicionar.
   - **Insira o código de ativação**

     Especifique o código de ativação no campo de texto e clique no botão **Enviar**.
4. Clique no botão **Fechar**.

A chave de licença ou várias chaves de licença são adicionadas ao repositório do Servidor de Administração.

Implementando uma chave de licença para dispositivos clientes

O Kaspersky Security Center Web Console permite distribuir uma chave de licença para dispositivos clientes automaticamente ou por meio da tarefa de **Ativação do aplicativo**. É possível usar a tarefa para distribuir chaves para um grupo específico de dispositivos. Durante a distribuição de uma chave de licença por meio da tarefa, o limite do licenciamento em relação ao número de dispositivos não é levado em consideração. Use a distribuição automática de chaves para interromper a distribuição de uma chave de licença automaticamente quando o limite do licenciamento for atingido.

Caso a distribuição automática de uma chave de licença seja ativada, não crie uma tarefa de **Ativação do aplicativo** para distribuir essa chave aos dispositivos clientes. Caso contrário, a carga no Servidor de Administração aumentará devido à sincronização frequente.

Antes da implementação, adicione uma chave de licença ao repositório do Servidor de Administração.

*Para distribuir uma chave de licença para dispositivos clientes por meio da tarefa de **Ativação do aplicativo**:*

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O **Assistente para novas tarefas** inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na lista suspensa **Aplicativo**, selecione o aplicativo ao qual você deseja adicionar uma chave de licença.
4. Na lista **Tipo de tarefa**, selecione a tarefa **Ativação do aplicativo**.

5. No campo **Nome da tarefa**, especifique o nome da nova tarefa.

6. Selecione os dispositivos aos quais a tarefa será atribuída.

7. Na etapa **Selecionando uma chave de licença** do assistente, clique no link **Adicionar chave** para adicionar a chave.

8. No painel de adição de chave, adicione a chave de licença usando uma das seguintes opções:

   É necessário adicionar a chave de licença somente se ela não tiver sido adicionada ao repositório do Servidor de Administração antes da criação da tarefa de **Ativação do aplicativo**.

   - Selecione a opção **Insira o código de ativação** para inserir um código de ativação e, então, faça o seguinte:

     a. Especifique o código de ativação e, então, clique no botão **Enviar**.

     As informações sobre a chave de licença são exibidas no painel de adição de chave.

     b. Clique no botão **Salvar**.

     Se você quiser distribuir automaticamente a chave de licença para dispositivos gerenciados, ative a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

     O painel de adição de chave é fechado.

   - Selecione a opção **Adicionar arquivo de chave** para adicionar um arquivo de chave e, em seguida:

     a. Clique no botão **Selecionar arquivo de chave**.

     b. Na janela exibida, selecione um arquivo de chave e, então, clique no botão **Abrir**.

     As informações sobre a chave de licença são exibidas no painel de adição de chave de licença.

     c. Clique no botão **Salvar**.

     Se você quiser distribuir automaticamente a chave de licença para dispositivos gerenciados, ative a opção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.

     O painel de adição de chave é fechado.

9. Selecione a chave de licença na tabela de chaves.

10. Na etapa **Informações da licença** do assistente, desmarque a caixa de seleção padrão **Usar como chave reserva** caso queira substituir a chave de licença ativa.

    Por exemplo, isso é necessário quando a organização muda e a chave de outra organização é necessária no dispositivo; ou se a chave for emitida novamente e uma nova licença expirar antes da licença atual. Para evitar erros, é necessário desmarcar a caixa de seleção **Usar como chave reserva**.

    Caso queira mais informações sobre os problemas que podem ocorrer ao adicionar uma chave de licença ao Kaspersky Security Center e como resolvê-los, consulte a base de conhecimento do Kaspersky Security Center.

11. Na etapa **Concluir a criação da tarefa** do assistente, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** para modificar as configurações padrão da tarefa.

    Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois.

12. Clique no botão **Concluir**.

    O assistente cria a tarefa. Se você ativou a opção **Abrir detalhes da tarefa quando a criação for concluída**, a janela de propriedades da tarefa abre automaticamente. Nesta janela, você pode especificar as configurações gerais da tarefa e, se necessário, alterar as configurações especificadas durante a criação da tarefa.

    > Você também pode abrir a respectiva janela de propriedades clicando no nome da tarefa criada na lista de tarefas.

    A tarefa é criada, configurada e exibida na lista de tarefas.

13. Para executar a tarefa, selecione-a na lista de tarefas e, então, clique no botão **Iniciar**.

    Você também pode definir um agendamento de início de tarefa na guia **Agendamento** da janela de propriedades da tarefa.

    Para obter uma descrição detalhada das configurações de início agendado, consulte as configurações gerais da tarefa.

Depois que a tarefa for concluída, a chave de licença será implementada nos dispositivos selecionados.

Distribuição automática de uma chave de licença

O Kaspersky Security Center permite a distribuição automática de chaves de licença para os dispositivos gerenciados, se elas estiverem localizadas no repositório de chaves de licença do Servidor de Administração.

Para distribuir automaticamente uma chave de licença para os dispositivos gerenciados:

1. No menu principal, vá para **Operações** → **Licenciamento** → **Licenças da Kaspersky**.
2. Clique em o nome da chave de licença que você pretende distribuir automaticamente para os dispositivos.
3. Na janela de propriedades da chave de licença que abrir, selecione a caixa de seleção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados**.
4. Clique no botão **Salvar**.

   A chave de licença é distribuída automaticamente para todos os dispositivos compatíveis.

A distribuição de chaves de licença é realizada através do Agente de Rede. Não é criada nenhuma tarefa de distribuição de chaves de licença para o aplicativo.

Durante a distribuição automática de uma chave de licença, o limite de licenciamento no número de dispositivos é levado em conta. O limite de licenciamento é definido nas propriedades da chave de licença. Se o limite de licenciamento for alcançado, a distribuição desta chave de licença nos dispositivos termina automaticamente.

Observe que uma chave de licença distribuída automaticamente pode não ser exibida no repositório do Servidor de Administração virtual nos seguintes casos:

- A chave de licença não é válida para o aplicativo.
- O Servidor de Administração virtual não tem dispositivos gerenciados.
- A chave de licença já foi usada para dispositivos gerenciados por outro Servidor de Administração virtual e o limite no número de dispositivos foi atingido.

O Servidor de Administração virtual distribui automaticamente chaves de licença de seu repositório e do repositório do Servidor de Administração. Recomendamos que você:

- Use a tarefa *Adicionar chave de licença* para selecionar a chave de licença que deve ser implementada nos dispositivos.
- Evite desativar a opção **Permitir a implementação automática das chaves de licença deste Servidor de Administração virtual em seus dispositivos** nas configurações do Servidor de Administração virtual. Caso contrário, o Servidor de Administração virtual não distribuirá chaves de licença aos dispositivos, incluindo as chaves de licença do repositório do Servidor de Administração.

Se a caixa de seleção **Distribuir automaticamente a chave de licença aos dispositivos gerenciados** for marcada na janela de propriedades da chave de licença, uma chave de licença é distribuída em sua rede imediatamente. Caso essa opção não seja selecionada, será possível usar uma tarefa para distribuir uma chave de licença posteriormente.

A distribuição automática de chaves de licença configuradas no Servidor de Administração principal não se estende a dispositivos gerenciados por Servidores de Administração secundários não virtuais.

Visualizando de informações sobre chaves de licença em uso

Para exibir a lista das chaves de licença adicionadas ao repositório do Servidor de Administração:

No menu principal, vá para **Operações → Licenciamento → Licenças da Kaspersky**.

A lista exibida contém os arquivo de chave e os códigos de ativação adicionados ao repositório do Servidor de Administração.

Para exibir as informações detalhadas sobre uma chave de licença:

1. No menu principal, vá para **Operações → Licenciamento → Licenças da Kaspersky**.
2. Clique no nome da chave de licença necessária.

Na janela de propriedades da chave de licença que se abre, você pode visualizar:

- Na guia **Geral**: as informações principais sobre a chave de licença
- Na guia **Dispositivos**: a lista de dispositivos clientes em que a chave de licença foi usada para a ativação do aplicativo da Kaspersky instalado

Para exibir quais chaves de licença são implementadas em um dispositivo cliente específico:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo necessário.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Aplicativos**.
4. Clique no nome do aplicativo do qual deseja exibir as informações sobre a chave de licença.
5. Na janela de propriedades do aplicativo que se abre, clique na guia **Geral** e abra a seção **Licença**.

As informações principais sobre as chaves de licença adicional ativas são exibidas.

Para definir configurações atualizadas das chaves de licença do Servidor de Administração virtual, o Servidor de Administração envia uma solicitação para os servidores de ativação da Kaspersky ao menos uma vez por dia. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos.

Remover uma chave de licença do repositório

Quando você remove a chave de licença ativa de um recurso adicional do Servidor de Administração, por exemplo Gerenciamento de patches e vulnerabilidades ou Gerenciamento de Dispositivos Móveis, o recurso correspondente fica indisponível. Se uma chave reserva de licença tiver sido adicionada, a chave reserva de licença se tornará automaticamente a chave de licença ativa após a remoção da chave de licença ativa anterior.

Ao remover a chave de licença ativa implementada em um dispositivo gerenciado, o aplicativo continuará funcionando no dispositivo gerenciado.

Para remover um arquivo de chave ou um código de ativação do repositório do Servidor de Administração:

1. Verifique se o Servidor de Administração não usa um arquivo de chave ou um código de ativação que se desejar remover. Se o Servidor de Administração estiver usando, não será possível remover a chave. Para realizar a verificação:
   a. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

      A janela Propriedades do Servidor de Administração é aberta.

   b. Na guia **Geral**, selecione a seção **Chaves de licença**.

   c. Caso o arquivo de chave ou o código de ativação necessário seja exibido na seção aberta, clique no botão **Remover chave de licença ativa** e, em seguida, confirme a operação. Depois disso, o Servidor de Administração não usa a chave de licença removida, mas a chave permanece no repositório do Servidor de Administração. Caso o arquivo de chave ou o código de ativação necessário não seja exibido, o Servidor de Administração não o utilizará.
2. No menu principal, vá para **Operações** → **Licenciamento** → **Licenças da Kaspersky**.
3. Selecione o arquivo de chave ou o código de ativação necessário e clique no botão **Excluir**.

O arquivo de chave ou o código de ativação selecionado são removidos do repositório.

Você pode adicionar novamente uma chave de licença removida ou adicionar uma nova chave de licença.

Revogando o consentimento com um Contrato de Licença do Usuário Final

Se você decidir parar de proteger alguns de seus dispositivos clientes, poderá revogar o Contrato de Licença do Usuário Final (EULA) para qualquer aplicativo da Kaspersky gerenciado. É necessário desinstalar o aplicativo selecionado antes de revogar seu EULA.

Os EULAs aceitos em um Servidor de Administração virtual podem ser revogados no Servidor de Administração virtual ou no Servidor de Administração principal. Os EULAs aceitos em um Servidor de Administração principal podem ser revogados somente no Servidor de Administração principal.

Para revogar o EULA dos aplicativos gerenciados da Kaspersky:

1. Abra a janela de propriedades do Servidor de Administração e na guia **Geral**, selecione a seção **Contratos de Licença do Usuário Final**.

   É exibida uma lista de EULAs, aceitos ao criar pacotes de instalação, durante a instalação contínua de atualizações ou mediante implementação do Kaspersky Security for Mobile.

2. Na lista, selecione o EULA que deseja revogar.

   Você pode visualizar as seguintes propriedades da EULA:

   - Data em que o EULA foi aceito
   - Nome do usuário que aceitou o EULA

3. Clique na data de aceite de qualquer EULA para abrir sua janela de propriedades que exibe os seguintes dados:

   - Nome do usuário que aceitou o EULA
   - Data em que o EULA foi aceito
   - Identificador exclusivo (UID) do EULA
   - Texto completo do EULA
   - Lista de objetos (pacotes de instalação, atualizações contínuas, aplicativos móveis) vinculados ao EULA e seus respectivos nomes e tipos

4. Na parte inferior da janela de propriedades do EULA, clique no botão **Revogar Contrato de Licença**.

   Se existirem objetos (pacotes de instalação e suas respectivas tarefas) que impeçam a revogação do EULA, a notificação correspondente será exibida. Não é possível continuar com a revogação até que esses objetos sejam excluídos.

   Na janela que se abre, você é informado que deve primeiro desinstalar o aplicativo da Kaspersky que corresponde ao EULA.

5. Clique no botão para confirmar a revogação.

A EULA foi revogada. Ele não é mais exibido na lista de Contratos de licença na seção **Contratos de Licença do Usuário Final**. A janela de propriedades do EULA se fecha; o aplicativo não estará mais instalado.

Renovando licenças para aplicativos da Kaspersky

Você pode renovar uma licença de um aplicativo da Kaspersky que expirou ou está prestes a expirar (em menos de 30 dias).

Para renovar uma licença expirada ou uma licença prestes a expirar:

1. Execute alguma das seguintes ações:

   - No menu principal, vá para **Operações → Licenciamento → Licenças da Kaspersky**.
   - No menu principal, vá para **Monitoramento e relatórios → Painel**, e depois clique no link **Ver licenças expiradas** ao lado de uma notificação.

   A janela **Licenças da Kaspersky** é aberta, permitindo visualiza e renovar licenças.

2. Clique no link **Renovar licença** ao lado da licença necessária.

   Ao clicar no link de renovação da licença, você concorda em transferir à Kaspersky as seguintes informações sobre o Kaspersky Security Center: a versão, a localização de uso, a ID de licença do software (ou seja, a ID da licença sendo renovada), se a licença foi comprada via empresa parceira ou não.

3. Na janela aberta do serviço de renovação de licença, siga as instruções para renovar uma licença.

   A licença foi renovada.

No Kaspersky Security Center Web Console, são exibidas notificações quando uma licença está prestes a expirar, de acordo com a seguinte programação:

- 30 dias antes do vencimento
- 7 dias antes do vencimento
- 3 dias antes do vencimento
- 24 horas antes do vencimento
- Quando uma licença expirou

Usando o Kaspersky Marketplace para escolher as soluções comerciais Kaspersky de sua preferência

Marketplace é uma seção no menu principal que permite visualizar toda a gama de soluções comerciais Kaspersky. Selecione as que você precisa e prossiga com a compra no site da Kaspersky. Você pode usar filtros para visualizar apenas as soluções que se adaptam à sua organização e aos requisitos do seu sistema de segurança da informação. A selecionar uma solução, o Kaspersky Security Center redireciona seu acesso para a página da web relacionada no site da Kaspersky para saber mais sobre essa solução. Cada página da web permite efetuar compra ou contém instruções sobre o processo de compra.

Na seção **Marketplace**, você pode filtrar as soluções Kaspersky usando os seguintes critérios:

- Número de dispositivos (endpoints, servidores e outros tipos de ativos) que você deseja proteger:
  - 50–250
  - 250–1000
  - Mais de 1000
- Nível de experiência da equipe de segurança da informação da sua organização:
  - **Foundations**

    Este nível é típico para empresas que possuem apenas uma equipe de TI. O número máximo possível de ameaças é bloqueado automaticamente.
  - **Optimum**

    Esse nível é típico para empresas que têm uma função de segurança de TI específica na equipe de TI. Nesse nível, as empresas precisam de soluções que lhes permitam enfrentar as ameaças genéricas e também as que desviam dos mecanismos preventivos existentes.
  - **Expert**

    Este nível é típico para empresas com ambientes de TI complexos e distribuídos. A equipe de segurança de TI é experiente ou a empresa possui uma equipe de SOC (Security Operations Center). As soluções necessárias permitem que as empresas enfrentem ameaças complexas e ataques direcionados.
- Tipos de ativos que você deseja proteger:
  - **Endpoints**: estações de trabalho de funcionários, máquinas físicas e virtuais, sistemas integrados
  - **Servidores**: servidores físicos e virtuais
  - **Nuvem**: ambientes de nuvem pública, privada ou híbrida; serviços na nuvem
  - **Rede**: rede local, infraestrutura de TI
  - **Serviço**: serviços relacionados à segurança fornecidos pela Kaspersky

Para encontrar e adquirir uma solução empresarial Kaspersky:

1. No menu principal, vá para **Marketplace**.

   Por padrão, a seção exibe todas as soluções comerciais Kaspersky disponíveis.

2. Para visualizar apenas as soluções adequadas à sua organização, selecione os valores necessários nos filtros.

3. Clique na solução que deseja adquirir ou sobre a qual deseja saber mais.

   Você será redirecionado para a página da solução. Você pode seguir as instruções na tela para prosseguir com a compra.

Configuração da proteção da rede

Esta seção contém informações sobre a configuração manual de políticas e tarefas, funções de usuário, criação de uma estrutura de grupo de administração e hierarquia de tarefas.

Cenário: Configurar a proteção da rede

O Assistente de início rápido cria políticas e tarefas com as configurações padrão. Essas configurações podem ficar abaixo do ideal ou até mesmo não serem permitidas pela organização. Portanto, recomendamos que você ajuste essas políticas e tarefas e crie outras, se necessárias para a sua rede.

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

- Servidor de Administração do Kaspersky Security Center instalado com êxito
- Kaspersky Security Center Web Console instalado com êxito (opcional)
- Cenário principal de instalação do Kaspersky Security Center concluído
- Concluiu o Assistente de início rápido ou criou manualmente as seguintes políticas e tarefas no grupo de administração **Dispositivos gerenciados**:
  - Política do Kaspersky Endpoint Security
  - Tarefa de grupo para atualizar o Kaspersky Endpoint Security
  - Política de Agente de Rede
  - Tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*

A configuração da proteção de rede continua em fases:

1. **Configuração e propagação de políticas e perfis da política de aplicativos Kaspersky**

Para configurar e propagar as configurações dos aplicativos Kaspersky instalados nos dispositivos gerenciados, você pode usar duas abordagens de gerenciamento de segurança diferentes: centrado no dispositivo ou centrado no usuário. Essas duas abordagens também podem ser combinadas. Para implementar o gerenciamento de segurança centrado no dispositivo, você pode usar ferramentas fornecidas no Console de Administração baseado no Console de Gerenciamento Microsoft ou Kaspersky Security Center Web Console. O gerenciamento de segurança centrado no usuário pode ser implementado por meio do Kaspersky Security Center Web Console somente.

2. **Configuração de tarefas de gerenciamento remoto de aplicativos Kaspersky**

   Verifique as tarefas criadas com o Assistente de início rápido e faça o ajuste fino delas, se necessário.

   Instruções de como proceder:

   - Console de Administração:
     - Configurar a tarefa de grupo para atualizar o Kaspersky Endpoint Security
     - Agendar a tarefa Encontrar vulnerabilidades e atualizações necessárias
   - Kaspersky Security Center Web Console:
     - Configurar a tarefa de grupo para atualizar o Kaspersky Endpoint Security
     - As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias

   Se necessário, crie tarefas adicionais para gerenciar os aplicativos Kaspersky instalados nos dispositivos cliente.

3. **Avaliação e limitação da carga de eventos no banco de dados**

   As informações sobre eventos que ocorrem durante a operação de aplicativos gerenciados são transferidas de um dispositivo cliente e registradas no banco de dados do Servidor de Administração. Para reduzir a carga do Servidor de Administração, avalie e limite o número máximo de eventos que podem ser armazenados no banco de dados.

   Instruções de como proceder:

   - Console de Administração: Configuração do número máximo de eventos
   - Kaspersky Security Center Web Console: Configurar o número máximo de eventos

Resultados

Quando você concluir esse cenário, sua rede estará protegida pela configuração de aplicativos, tarefas e eventos da Kaspersky recebidos pelo Servidor de Administração:

- Os aplicativos Kaspersky são configurados de acordo com as políticas e perfis de política.
- Os aplicativos são gerenciados através de um conjunto de tarefas.
- O número máximo de eventos que podem ser armazenados no banco de dados está definido.

Quando a configuração da proteção de rede for concluída, você poderá prosseguir para configurar atualizações regulares para bancos de dados e aplicativos Kaspersky.

Para obter detalhes sobre como configurar respostas automáticas a ameaças detectadas pelo Kaspersky Sandbox, consulte a Ajuda Online do Kaspersky Sandbox 2.0.

Sobre as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário

Você pode gerenciar configurações de segurança do ponto de vista de recursos de dispositivo e do ponto de vista de funções de usuário. A primeira abordagem é chamada de *gerenciamento de segurança centrado no dispositivo*, e a segunda, *gerenciamento de segurança centrado no usuário*. Para aplicar configurações diferentes a dispositivos diferentes, é possível usar um dos tipos de gerenciamento ou ambos em conjunto. Para implementar o gerenciamento de segurança centrado no dispositivo, você pode usar ferramentas fornecidas no Console de Administração baseado no Console de Gerenciamento Microsoft ou Kaspersky Security Center Web Console. O gerenciamento de segurança centrado no usuário pode ser implementado por meio do Kaspersky Security Center Web Console somente.

O gerenciamento de segurança centralizado no dispositivo permite aplicar diferentes configurações de aplicativos de segurança aos dispositivos gerenciados, dependendo dos recursos específicos do dispositivo. Por exemplo, você pode aplicar configurações diferentes aos dispositivos alocados em diferentes grupos de administração. Você também pode diferenciar os dispositivos usando esses dispositivos no Active Directory ou suas especificações de hardware.

O gerenciamento de segurança centralizado no usuário permite aplicar diferentes configurações do aplicativo de segurança à diferentes funções do usuário. Você pode criar várias funções de usuário, atribuir uma função de usuário apropriada á cada usuário e definir configurações de aplicativos diferentes para os dispositivos pertencentes a usuários com funções diferentes. Por exemplo, convém aplicar configurações do aplicativo diferentes nos dispositivos de contadores e especialistas em recursos humanos (RH). Como resultado, quando o gerenciamento de segurança centrado no usuário é implementado, cada departamento, o departamento de contas e o departamento de RH, têm a sua própria configuração para os aplicativos Kaspersky. Uma configuração define qual configuração do aplicativo pode ser modificada pelos usuários e que são impostas e bloqueadas pelo administrador.

gerenciamento de segurança centrado no usuário, você pode aplicar configurações de aplicativo específicas a usuários individuais. Isso pode ser necessário quando um funcionário tem uma função única na empresa ou quando você quer controlar incidentes de segurança relacionados a dispositivos de uma pessoa específica. Dependendo da função desse funcionário na empresa, você pode expandir ou limitar os direitos dessa pessoa para alterar as configurações do aplicativo. Por exemplo, é possível expandir os direitos de um administrador do sistema que gerencia dispositivos clientes em um escritório local.

Você também pode combinar as abordagens de gerenciamento de segurança centrada no dispositivo e centrada no usuário. Por exemplo, você pode configurar uma política de aplicativo específica para cada grupo de administração e, adicionalmente, criar perfis de política para uma ou várias funções dos usuários da sua empresa. Nesse caso, as políticas e os perfis de política são aplicados na seguinte ordem:

1. As políticas criadas para o gerenciamento de segurança centrado no dispositivo são aplicadas.
2. Elas são modificadas pelos perfis de política segundo as prioridades de perfil de política.
3. As políticas são modificadas pelos perfis de política associados às funções de usuário.

Configuração e propagação de políticas: abordagem centrada no dispositivo

Quando você concluir este cenário, os aplicativos serão configurados em todos os dispositivos gerenciados em conformidade com as políticas de aplicativo e perfis da política definidos por você.

Pré-requisitos

Antes de iniciar, assegure-se de que você tenha instalado o Servidor de Administração do Kaspersky Security Center e o Kaspersky Security Center Web Console (opcional). Se tiver instalado o Kaspersky Security Center Web Console, você também poderá considerar o gerenciamento de segurança centrado no usuário como uma alternativa ou opção adicional à abordagem centrada no dispositivo.

Fases

O cenário de gerenciamento centrado no dispositivo dos aplicativos Kaspersky consiste nas seguintes etapas:

1. **Configurar os políticas de aplicativo**

   Defina as configurações para aplicativos da Kaspersky instalados nos dispositivos gerenciados por meio da criação de uma política para cada aplicativo. Esse conjunto de políticas será propagado para os dispositivos clientes.

   Quando você configura a proteção da sua rede no Assistente de início rápido, o Kaspersky Security Center cria a política padrão para os seguintes aplicativos:

   - Kaspersky Endpoint Security for Windows – para dispositivos clientes baseados em Windows
   - Kaspersky Endpoint Security for Linux – para dispositivos clientes baseados em Linux

   Se tiver concluído o processo de configuração usando este assistente, você não precisará criar uma nova política para este aplicativo. Siga para a configuração manual da política do Kaspersky Endpoint Security.

   Se você tiver uma estrutura hierárquica de vários Servidores de Administração e/ou grupos de administração, os Servidores de Administração secundários e os grupos de administração secundários herdarão as políticas do Servidor de Administração principal por padrão. Você pode forçar a herança pelos grupos secundários e Servidores de Administração secundários para proibir qualquer modificação das configurações definidas na política de fluxo acima. Se você quiser que somente uma parte das configurações seja herdada por imposição, poderá bloqueá-las na política de fluxo acima. O restante das configurações desbloqueadas ficarão disponíveis para modificação nas políticas de fluxo abaixo. A hierarquia de políticas criada permite que você gerencie dispositivos nos grupos de administração com mais eficiência.

   Instruções de como proceder:

   - Console de Administração: Criar uma política
   - Kaspersky Security Center Web Console: Criar uma política

2. **Criar os perfis da política (opcional)**

Se você quiser que os dispositivos em um único grupo de administração seja executado sob diferentes configurações de política, crie perfis de políticas para esses dispositivos. Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos de destino em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo gerenciado.

Usando condições de ativação do perfil, você pode aplicar diferentes perfis de políticas, por exemplo, nos dispositivos localizados em uma unidade ou grupo de segurança específico do Active Directory, ter configuração de hardware específica ou marcada com tags específicas. Use tags para filtrar dispositivos que atendem a critérios específicos. Por exemplo, você pode criar um identificador denominado *Windows*, marcar todos os dispositivos executando o sistema operacional Windows com esse identificador e especificar esse identificador como uma condição de ativação para um perfil da política. Como resultado, os aplicativos Kaspersky instalados em todos os dispositivos executando o Windows serão gerenciados por seu próprio perfil da política.

Instruções de como proceder:

- Console de Administração:
  - Criar um perfil da política
  - Criar uma regra de ativação do perfil da política
- Kaspersky Security Center Web Console:
  - Criar um perfil da política
  - Criar uma regra de ativação do perfil da política

3. **Propagar políticas e perfil da política para os dispositivos gerenciados**

   Por padrão, o Servidor de Administração sincroniza automaticamente com os dispositivos gerenciados a cada 15 minutos. Você pode ignorar a sincronização automática e executar a sincronização manualmente usando o comando Forçar a sincronização. Além disso, a sincronização é forçada depois que você cria ou altera a política ou um perfil da política. Durante a sincronização, as políticas novas ou alteradas e os perfis da política são propagados para os dispositivos gerenciados.

   Se usar o Kaspersky Security Center Web Console, você poderá verificar se as políticas e os perfil da política foram entregues a um dispositivo. O Kaspersky Security Center especifica a data e hora de entrega nas propriedades do dispositivo.

   Instruções de como proceder:

   - Console de Administração: Sincronização forçada
   - Kaspersky Security Center Web Console: Sincronização forçada

Resultados

Quando o cenário centrado no dispositivo for concluído, os aplicativos Kaspersky serão configurados segundo as configurações especificadas e propagadas por meio da hierarquia de políticas.

As políticas e perfis da política de aplicativo configuradas serão aplicadas automaticamente aos novos dispositivos adicionados aos grupos de administração.

Configuração e propagação de políticas: abordagem centrada no usuário

Esta seção descreve o cenário da abordagem centrada no usuário para configuração centralizada de aplicativos da Kaspersky instalados nos dispositivos gerenciados. Quando você concluir este cenário, os aplicativos serão configurados em todos os dispositivos gerenciados em conformidade com as políticas de aplicativo e perfis da política definidos por você.

Este cenário pode ser implementado por meio do Kaspersky Security Center Web Console versão 13 ou posterior.

Pré-requisitos

Antes de iniciar, certifique-se de que você instalou com êxito o Servidor de Administração do Kaspersky Security Center e o Kaspersky Security Center Web Console e que concluiu o cenário de instalação principal. Você pode também considerar o gerenciamento de segurança centrado no dispositivo como uma alternativa ou opção adicional à abordagem centrada no usuário. Saiba mais sobre duas abordagens de gerenciamento.

Processar

O cenário de gerenciamento centrado no usuário dos aplicativos da Kaspersky consiste nas seguintes etapas:

1. **Configurar os políticas de aplicativo**

   Defina as configurações para aplicativos da Kaspersky instalados nos dispositivos gerenciados por meio da criação de uma política para cada aplicativo. Esse conjunto de políticas será propagado para os dispositivos cliente.

   Quando você configura a proteção da sua rede no Assistente de início rápido, o Kaspersky Security Center cria a política padrão do Kaspersky Endpoint Security. Se tiver concluído o processo de configuração usando este assistente, você não precisará criar uma nova política para este aplicativo. Prossiga para a configuração manual da política do Kaspersky Endpoint Security.

   Se você tiver uma estrutura hierárquica de vários Servidores de Administração e/ou grupos de administração, os Servidores de Administração secundários e os grupos de administração secundários herdarão as políticas do Servidor de Administração principal por padrão. Você pode forçar a herança pelos grupos secundários e Servidores de Administração secundários para proibir qualquer modificação das configurações definidas na política de fluxo acima. Se você quiser que somente uma parte das configurações seja herdada por imposição, poderá bloqueá-las na política de fluxo acima. O restante das configurações desbloqueadas ficarão disponíveis para modificação nas políticas de fluxo abaixo. A hierarquia de políticas criada permite que você gerencie dispositivos nos grupos de administração com mais eficiência.

   Instruções: Criação de uma política

2. **Especificar proprietários dos dispositivos**

   Atribua os dispositivos gerenciados aos usuários correspondentes.

   Instruções: Atribuição de um usuário como proprietário do dispositivo

3. **Definir funções do usuário típicas para a sua empresa**

Pense sobre diferentes tipos de trabalhos que os funcionários da sua empresa normalmente executam. Você deve dividir todos de acordo com as funções. Por exemplo, você pode dividi-los por departamentos, profissões ou cargos. Depois disso, você precisará criar uma função do usuário para cada grupo. Tenha em mente que cada função do usuário terá seu próprio perfil da política contendo configurações do aplicativo específicas para essa função.

4. **Criar funções de usuário**

   Crie e configure uma função do usuário para cada grupo de funcionários que você definiu na etapa anterior ou use as funções do usuário predefinidas. As funções do usuário conterão o conjunto de direitos de acesso aos recursos do aplicativo.

   Instruções: Criação de uma função de usuário

5. **Especificar o escopo de cada função de usuário**

   Para cada uma das funções de usuário criadas, defina usuários e/ou grupos de segurança e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

   Instruções: Edição do escopo de uma função de usuário

6. **Criar os perfis da política**

   Crie um perfil da política para cada função de usuário em sua empresa. Os perfis da política definem quais configurações serão aplicadas aos aplicativos instalados em dispositivos de usuários dependendo da função de cada usuário.

   Instruções: Criação de um perfil da política

7. **Associar perfis da política com as funções do usuário**

   Associe os perfis de política criados com as funções do usuário. Depois disso: o perfil da política fica ativo para um usuário com a função especificada. As configurações definidas no perfil da política serão aplicadas aos aplicativos da Kaspersky instalados nos dispositivos do usuário.

   Instruções: Associar perfis da política a funções

8. **Propagar políticas e perfil da política para os dispositivos gerenciados**

   Por padrão, o Servidor de Administração sincroniza automaticamente com os dispositivos gerenciados a cada 15 minutos. Durante a sincronização, as políticas novas ou alteradas e os perfis da política são propagados para os dispositivos gerenciados. Você pode ignorar a auto sincronização e executar a sincronização manualmente usando o comando Forçar a sincronização. Quando a sincronização estiver concluída, as políticas e os perfis da política serão entregues e aplicados aos aplicativos Kaspersky instalados.

   Você pode verificar se as políticas e os perfis da política foram entregues a um dispositivo. O Kaspersky Security Center especifica a data e hora de entrega nas propriedades do dispositivo.

   Instruções: Sincronização forçada

Resultados

Quando o cenário centrado no usuário for concluído, os aplicativos da Kaspersky serão configurados segundo as configurações especificadas e propagadas por meio da hierarquia de políticas e perfis de política.

Para um novo usuário, você terá de criar uma nova conta, atribuir o usuário com uma das funções de usuário criadas e atribuir os dispositivos ao usuário. As políticas e perfis da política de aplicativo configuradas serão automaticamente aplicadas aos novos dispositivos adicionados aos dispositivos de esse usuário.

Configurações de política do Agente de Rede

Para configurar uma política do Agente de Rede:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política do Agente de Rede.

   A janela de propriedades da política do Agente de Rede se abre.

Veja a tabela de comparação detalhando como as configurações abaixo se aplicam, dependendo do tipo de sistema operacional usado.

Geral

Nesta guia, você pode modificar o status da política e especificar a herança das configurações da política:

- No bloco **Status da política**, você pode selecionar um dos modos de política:
  - Ativo

    Se esta opção estiver selecionada, a política é habilitada.

    Por padrão, esta opção está selecionada.

  - Inativo

    Se esta opção estiver selecionada, a política é habilitada, mas continua armazenada na pasta **Políticas**. Se necessário, a política pode ser habilitada.

- No grupo de configurações **Herança de configurações**, você pode configurar a herança de política:
  - Herdar configurações da política principal

    Se esta opção estiver ativada, os valores das configurações de política são herdados da política de grupo de nível superior e, portanto são bloqueados.

    Por padrão, esta opção está ativada.

  - Forçar herança de configurações nas políticas secundárias

    Se esta opção estiver ativada, após a aplicação das alterações da política, as seguintes ações serão realizadas:

    - Os valores das configurações da política serão propagados às políticas de subgrupos de administração, ou seja, às políticas secundárias.
    - No bloco **Herança de configurações** da seção **Geral** na janela Propriedades de cada política secundária, a opção **Herdar configurações da política principal** será automaticamente ativada.

    Se a opção estiver ativada, as configurações das políticas secundárias são bloqueadas.

    Por padrão, esta opção está desativada.

Configuração de eventos

Nessa guia, é possível configurar o registro e a notificação de eventos. Os eventos são distribuídos conforme o nível de importância nas seguintes seções na guia **Configuração de eventos**:

- **Falha funcional**
- **Advertência**
- **Informações**

Em cada seção, a lista de tipos de eventos exibe os tipos de eventos e o prazo padrão de armazenamento de eventos no Servidor de Administração (em dias). Após clicar no tipo de evento, é possível especificar as configurações do registro de eventos e as notificações sobre eventos selecionados na lista. Por padrão, as configurações de notificação comuns especificadas para todo o Servidor de Administração são usadas para todos os tipos de evento. Contudo, você pode alterar configurações específicas dos tipos de evento necessários.

Por exemplo, na seção **Advertência**, é possível configurar o tipo de evento **Ocorreu um incidente**. Os eventos podem acontecer, por exemplo, quando o espaço livre em disco de um ponto de distribuição for inferior a 2 GB (pelo menos 4 GB são necessários para instalar aplicativos e baixar atualizações remotamente). Para configurar o evento **Ocorreu um incidente**, clique nele e especifique onde armazenar os eventos ocorridos e como notificá-los.

Caso o agente de rede tenha detectado um incidente, é possível gerenciá-lo usando as configurações de um dispositivo gerenciado.

Configurações do aplicativo

Configurações

Na seção **Configurações**, você pode configurar a política do Agente de Rede:

- **Distribuir os arquivos somente através dos pontos de distribuição**

  Se essa opção for ativada, os Agentes de Rede em dispositivos gerenciados recuperam atualizações apenas de pontos de distribuição.

  Se esta opção estiver desativada, os Agentes de Rede em dispositivos gerenciados recuperam atualizações de pontos de distribuição ou do Servidor de Administração.

  Observe que os aplicativos de segurança em dispositivos gerenciados recuperam atualizações da fonte definida na tarefa de atualização para cada aplicativo de segurança. Se você ativar a opção **Distribuir os arquivos somente através dos pontos de distribuição**, certifique-se de que o Kaspersky Security Center está definido como uma fonte de atualização nas tarefas de atualização.

  Por padrão, esta opção está desativada.

- **Tamanho máximo da fila de eventos, em MB**

  Neste campo, você pode especificar o espaço máximo na unidade que uma fila de eventos pode ocupar.

  O valor predefinido é 2 megabytes (MB).

- **O aplicativo tem permissão para recuperar os dados estendidos da política no dispositivo**

  O Agente de Rede instalado em um dispositivo gerenciado transfere informações sobre a política do aplicativo de segurança aplicada ao aplicativo de segurança (por exemplo, Kaspersky Endpoint Security for Windows). Você pode visualizar as informações transferidas na interface do aplicativo de segurança.

  O Agente de Rede transfere as seguintes informações:

  - Hora da entrega da política para o dispositivo gerenciado.
  - Nome da política ativa no momento da entrega da política ao dispositivo gerenciado.
  - Nome da política de ausência temporária no momento da entrega da política ao dispositivo gerenciado (indisponível para o Agente de Rede para Linux).
  - Nome e caminho completo para o grupo de administração que continha o dispositivo gerenciado no momento da entrega da política para o dispositivo gerenciado.
  - Lista de perfis de política ativos com seus nomes e prioridades no momento da entrega da política ao dispositivo gerenciado.

  Você pode usar as informações para garantir que a política correta seja aplicada ao dispositivo e para fins de solução de problemas. Por padrão, esta opção está desativada.

- **Proteger serviço do Agente de Rede contra remoção ou interrupção não autorizada e impedir alterações nas configurações**

  Quando esta opção estiver ativado, após o Agente de Rede ter sido instalado em um dispositivo gerenciado, o componente não poderá ser removido ou reconfigurado sem os privilégios necessários. O serviço Agente de Rede não pode ser interrompido. Essa opção não tem efeito nos controladores de domínio.

  Ative esta opção para proteger o Agente de Rede em estações de trabalho operadas com direitos de administrador local.

  Por padrão, esta opção está desativada.

- **Usar senha de desinstalação**

  Caso esta opção esteja marcada, ao clicar no botão **Modificar**, será possível especificar a senha para o utilitário klmover e desinstalar remotamente o Agente de Rede.

  Por padrão, esta opção está desativada.

Repositórios

Na seção **Repositórios**, você pode selecionar os tipos de objetos cujos detalhes serão enviados do Agente de Rede para o Servidor de Administração. Se a modificação de algumas configurações nesta seção estiver bloqueada pela política do Agente de Rede, você não pode modificá-las.

- **Detalhes dos aplicativos instalados**

  Se esta opção estiver ativada, as informações sobre os aplicativos instalados nos dispositivos clientes serão enviadas ao Servidor de Administração.

  Por padrão, esta opção está ativada.

- **Incluir informações sobre patches**

  As informações sobre os patches para os aplicativos instalados nos dispositivos cliente são enviadas ao Servidor de Administração. A ativação desta opção pode aumentar a carga no Servidor de Administração e DBMS, assim como causar volume aumentado do banco de dados.

  Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

- **Detalhes das atualizações do Windows Update**

  Se esta opção estiver marcada, as informações sobre as atualizações do Microsoft Windows Update que devem ser instaladas nos dispositivos clientes serão enviadas ao Servidor de Administração.

  Algumas vezes, mesmo se a opção estiver desativada, as atualizações são exibidas nas propriedades do dispositivo na seção **Atualizações disponíveis**. Pode acontecer se, por exemplo, os dispositivos da organização tiveram vulnerabilidades que poderiam ser corrigidas por estas atualizações.

  Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

  As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

- Detalhes das vulnerabilidades de software e das atualizações correspondentes

  Se essa opção estiver ativada, as informações sobre vulnerabilidades no software de terceiros (incluindo software da Microsoft), detectadas em dispositivos gerenciados e sobre atualizações de software para corrigir vulnerabilidades de terceiros (não incluindo o software da Microsoft) são enviadas ao Servidor de Administração.

  Selecionando esta opção (**Detalhes das vulnerabilidades de software e das atualizações correspondentes)** aumenta a carga da rede, a carga do disco do Servidor de Administração e o consumo de recurso pelo Agente de Rede.

  Por padrão, esta opção está ativada. Ela está disponível apenas para Windows.

  Para gerenciar atualizações de software da Microsoft, use a opção **Detalhes das atualizações do Windows Update**.

- Detalhes do registro de hardware

  O Agente de Rede instalado em um dispositivo envia informações sobre o hardware do dispositivo para o Servidor de Administração. Você pode exibir os detalhes do hardware nas propriedades do dispositivo.

  Verifique e confirme se o utilitário lshw está instalado nos dispositivos Linux a partir dos quais deseja buscar detalhes de hardware. Os detalhes de hardware obtidos de máquinas virtuais podem estar incompletos, dependendo do hipervisor usado.

Atualizações e vulnerabilidades de software

Na seção **Atualizações e vulnerabilidades de software**, é possível configurar a pesquisa e a distribuição de atualizações do Windows, assim como ativar a verificação de arquivos executáveis quanto a vulnerabilidades:

- **Usar Servidor de Administração como servidor WSUS**

  Se esta opção estiver ativada, as atualizações do Windows não serão baixadas no Servidor de Administração. O Servidor de Administração fornece atualizações baixadas para os serviços Windows Update em dispositivos cliente no modo centralizado através de Agentes de Rede.

  Se esta opção estiver ativada, o Servidor de Administração não é usado para baixar as atualizações do Windows. Neste caso, os dispositivos cliente recebem por si só as atualizações do Windows.

  Por padrão, esta opção está desativada.

- Você pode limitar as atualizações Windows que os usuários podem instalar em seus dispositivos manualmente usando o Windows Update.

  Em dispositivos que executam o Windows 10, se o Windows Update já tiver encontrado atualizações para o dispositivo, a nova opção selecionada em **Permitir aos usuários gerenciar a instalação de atualizações do Windows Update** será aplicada apenas depois que as atualizações encontradas forem instaladas.

  Selecione um item na lista suspensa:

  - **Permitir que os usuários instalem todas as atualizações do Windows Update**

    Os usuários podem instalar todas as atualizações do Microsoft Windows Update que são aplicáveis aos seus dispositivos.

    Selecione esta opção se você não quiser interferir na instalação das atualizações.

    Quando o usuário instala atualizações do Microsoft Windows Update manualmente, as atualizações podem ser baixadas de servidores da Microsoft e não do Servidor de Administração. Isso é possível se o Servidor de Administração ainda não tiver baixado as atualizações. Baixar atualizações dos servidores da Microsoft resulta em tráfego extra.

  - **Permitir que os usuários instalem apenas atualizações do Windows Update aprovadas**

    Os usuários podem instalar todas as atualizações do Microsoft Windows Update que são aplicáveis aos seus dispositivos e que você aprovou.

    Por exemplo, pode ser necessário verificar primeiro a instalação das atualizações em um ambiente de teste, assegurar-se de que elas não interferem na operação dos dispositivos e, só então, permitir a instalação dessas atualizações aprovadas nos dispositivos cliente.

    Quando o usuário instala atualizações do Microsoft Windows Update manualmente, as atualizações podem ser baixadas de servidores da Microsoft e não do Servidor de Administração. Isso é possível se o Servidor de Administração ainda não tiver baixado as atualizações. Baixar atualizações dos servidores da Microsoft resulta em tráfego extra.

- **Não permitir que os usuários instalem atualizações do Windows Update**

  Os usuários não podem instalar atualizações do Microsoft Windows Update em seus dispositivos manualmente. Todas das atualizações aplicáveis são instaladas conforme configuradas por você.

  Selecione esta opção se você deseja gerenciar a instalação das atualizações centralmente.

  Por exemplo, pode ser necessário otimizar o agendamento da atualização para que a rede não fique sobrecarregada. Você pode agendar atualizações fora do horário para que não interfiram na produtividade dos usuários.

- No grupo de configurações **Modo de pesquisa do Windows Update**, você pode selecionar um modo de pesquisa de atualizações:

  - **Ativo**

    Se essa opção estiver selecionada, o Servidor de Administração com suporte do Agente de Rede inicia uma solicitação ao Windows Update Agent no dispositivo cliente por uma fonte de atualização: Servidores do Windows Update ou WSUS. A seguir, o Agente de Rede passa as informações recebidas do Windows Update Agent para o Servidor de Administração.

    A opção entra em vigor somente se **Conectar com o servidor de atualizações para atualizar dados** A opção da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* está selecionada.

    Por padrão, esta opção está selecionada.

  - **Passivo**

    Se você selecionar esta opção, o Agente de Rede passa informações ao Servidor de Administração periodicamente sobre atualizações obtidas na última sincronização do Windows Update Agent com a fonte de atualização. Se não for efetuada uma sincronização do Windows Update Agent com uma fonte de atualização, as informações sobre as atualizações no Servidor de Administração se tornam desatualizadas.

    Selecione esta opção se desejar obter atualizações do cache de memória da fonte de atualização.

  - **Desativado**

    Se esta opção for selecionada, o Servidor de Administração não solicita qualquer informação sobre atualizações.

    Selecione esta opção se, por exemplo, quiser testar as atualizações no seu dispositivo local primeiro.

- **Verificar a vulnerabilidade dos arquivos executáveis ao executá-los**

  Se essa caixa de seleção estiver selecionada, as vulnerabilidades serão verificadas quando os arquivos executáveis forem executados.

  Por padrão, esta opção está ativada.

Gerenciamento de reinício

Na seção **Gerenciamento de reinício**, é possível especificar a ação a ser executada se o sistema operacional de um dispositivo gerenciado precisar ser reiniciado para uso correto, instalação ou desinstalação de um aplicativo:

- **Não reiniciar o sistema operacional**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o sistema operacional automaticamente se necessário**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min.)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Forçar reinicialização após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  - **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

Windows Desktop Sharing

Na seção **Windows Desktop Sharing**, será possível ativar e configurar a auditoria das ações do administrador executadas em um dispositivo remoto quando o acesso à área de trabalho for compartilhado:

- **Ativar auditoria**

  Se a opção estiver marcada, a auditoria das ações do administrador no dispositivo remoto será ativada. Os registros de ações do administrador no dispositivo remoto são registrados:

  - No log de eventos no dispositivo remoto
  - Em um arquivo com a extensão syslog localizado na pasta de instalação do Agente de Rede no dispositivo remoto
  - No banco de dados de eventos do Kaspersky Security Center

  A auditoria das ações do administrador está disponível quando as seguintes condições são observadas:

  - A licença de Gerenciamento de patches e vulnerabilidades está em uso
  - O administrador tem o direito de iniciar o acesso compartilhado à área de trabalho do dispositivo remoto

  Se esta opção estiver desmarcada, a auditoria das ações do administrador no dispositivo remoto será desativada.

  Por padrão, esta opção está desativada.

- **Máscaras de arquivos para monitorar quando lidos**

  A lista contém máscaras de arquivos. Quando a auditoria é ativada, o aplicativo monitora a leitura do administrador de arquivos que correspondem às máscaras e salva informações sobre os arquivos lidos. A lista está disponível se a caixa de seleção **Ativar auditoria** for marcada. Você pode editar máscaras de arquivos e adicionar novas máscaras à lista. Cada nova máscara de arquivo deve ser especificada na lista em uma nova linha.

  Por padrão, são especificadas as seguintes máscaras de arquivos: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

- **Máscaras de arquivos para monitorar quando modificados**

  A lista contém máscaras de arquivos no dispositivo remoto. Quando a auditoria é ativada, o aplicativo monitora alterações efetuadas pelo administrador em arquivos que correspondem a máscaras e salva informações sobre essas modificações. A lista está disponível se a caixa de seleção **Ativar auditoria** for marcada. Você pode editar máscaras de arquivos e adicionar novas máscaras à lista. Cada nova máscara de arquivo deve ser especificada na lista em uma nova linha.

  Por padrão, são especificadas as seguintes máscaras de arquivos: *.txt, *.rtf, *.doc, *.xls, *.docx, *.xlsx, *.odt, *.pdf.

Gerenciar patches e atualizações

Na seção **Gerenciar patches e atualizações**, você poderá configurar o download e a distribuição das atualizações, assim como a instalação dos patches nos dispositivos gerenciados:

- **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**

  Se esta opção estiver ativada, os patches da Kaspersky com o status de aprovação *Indefinido* são automaticamente instaladas nos dispositivos gerenciados imediatamente após terem sido baixadas dos servidores de atualização.

  Se esta opção estiver desativada, as correções da Kaspersky que foram baixadas e identificadas com o status *Indefinido* somente serão instaladas após você alterar o status para *Aprovado*.

  Por padrão, esta opção está ativada.

- **Fazer antecipadamente o download das atualizações e dos bancos de dados de antivírus via Servidor de Administração (recomendado)**

  Se esta opção está ativada, o modelo offline do download da atualização é usado. Quando o Servidor de Administração recebe atualizações, ele notifica o Agente de Rede (nos dispositivos em que ele esteja instalado) sobre as atualizações que serão necessárias para os aplicativos gerenciados. Quando o Agentes de Rede recebe informações sobre essas atualizações, ele baixa dos arquivos relevantes do Servidor de Administração com antecedência. Na primeira conexão com o Agente de Rede, o Servidor de Administração inicia um download de atualizações. Após o Agente de Rede ter baixado todas as atualizações em um dispositivo cliente, as atualizações se tornam disponíveis para os aplicativos naquele dispositivo.

  Quando um aplicativo gerenciado em um dispositivo cliente tentar acessar o Agente de Rede quanto a atualizações, o Agente de Rede verifica se ele tem todas as atualizações necessárias. Se as atualizações forem recebidas do Servidor de Administração até 25 horas antes de terem sido solicitadas pelo aplicativo gerenciado, o Agente de Rede não se conectará ao Servidor de Administração, mas fornecerá ao aplicativo gerenciado as atualizações do cache local. A conexão com o Servidor de Administração pode não ser estabelecida quando o Agente de Rede fornecer atualizações aos aplicativos em dispositivos cliente, mas a conexão não é necessária para a atualização.

  Se esta opção está desativada, o modelo offline do download da atualização é usado. As atualizações são distribuídas de acordo com o agendamento da tarefa de download da atualização.

  Por padrão, esta opção está ativada.

Conectividade

A seção **Conectividade** inclui três subseções:

- **Rede**
- **Perfis de conexão**
- **Agendador de conexão**

Na subseção **Rede**, você pode configurar a conexão ao Servidor de Administração, ativar o uso de uma porta UDP e especificar o número da porta UDP.

- No grupo de configurações **Conectar-se ao Servidor de Administração**, você poderá configurar a conexão ao Servidor de Administração e especificar o intervalo de tempo para a sincronização entre os dispositivos cliente e o Servidor de Administração:

  - Intervalo de sincronização (min.)

    O Agente de Rede sincroniza o dispositivo gerenciado com o Servidor de Administração. Recomendamos definir o intervalo de sincronização (também conhecido como heartbeat) para 15 minutos a cada 10.000 dispositivos gerenciados.

    Se o intervalo de sincronização estiver definido para menos de 15 minutos, a sincronização será realizada a cada 15 minutos. Se o intervalo de sincronização estiver definido como 15 minutos ou mais, a sincronização será realizada no intervalo de sincronização especificado.

  - Compactar o tráfego de rede

    Se esta opção estiver ativada, a velocidade de transferência de dados pelo Agente de Rede é aumentada através da redução da quantidade de informação a ser transferida e consequente carga inferior sobre o Servidor de Administração.

    A carga na CPU do computador cliente pode aumentar.

    Por padrão, esta caixa de seleção é marcada.

  - Abrir portas do Agente de Rede no firewall do Microsoft Windows

    Se esta opção estiver habilitada, as portas necessárias para o Agente de Rede e o Servidor de Administração serão adicionadas à lista de exclusão do Firewall do Microsoft Windows.

    Por padrão, esta opção está ativada.

  - Usar conexão SSL

    Se esta opção estiver ativada, a conexão com o Servidor de Administração é estabelecida através de uma porta segura via SSL.

    Por padrão, esta opção está ativada.

  - Use o gateway de conexão no ponto de distribuição (se disponível) sob as configurações de conexão padrão

    Se esta opção estiver marcada, o gateway de conexão no ponto de distribuição é usado sob as configurações especificadas nas propriedades do grupo de administração.

    Por padrão, esta opção está ativada.

- Usar porta UDP

Caso deseje que o Agente de Rede seja conectado com o Servidor de Administração por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de **Porta UDP**. Por padrão, esta opção está ativada. A porta UDP padrão para estabelecer conexão com o Servidor de Administração é 15000.

- **Número da porta UDP**

  Neste campo, é possível inserir o número da porta UDP. O número da porta padrão é 15000.

  É usado o sistema decimal para registros.

  Se um dispositivo cliente estiver executando o Windows XP Service Pack 2, o firewall integrado bloqueará a porta UDP 15000. Essa porta deve ser aberta manualmente.

- **Usar ponto de distribuição para forçar conexão com o Servidor de Administração**

  Selecione esta opção se você selecionou a opção **Usar este ponto de distribuição como um servidor push** na janela de configurações do ponto de distribuição. Do contrário, o ponto de distribuição não atuará como um servidor push.

Na subseção **Perfis de conexão**, é possível especificar as configurações da localização da rede e ativar o modo ausente quando o Servidor de Administração não estiver disponível:

- **Configurações do local de rede**

  As configurações da localização da rede definem as características da rede à qual o dispositivo cliente está conectado e especifica as regras para o Agente de Rede alternando de um perfil de conexão do Servidor de Administração a outro quando aquelas características da rede forem alteradas.

- **Perfis de conexão do Servidor de Administração**

  Nesta seção, é possível visualizar e adicionar perfis para a conexão do Agente de Rede com o Servidor de Administração. Nesta seção, você também pode criar regras para alternar o Agente de Rede para diferentes Servidores de Administração quando os seguintes eventos ocorrem:

  - Quando o dispositivo cliente se conectar a outra rede local
  - Quando um dispositivo perde a conexão com a rede local da organização
  - Quando o endereço do gateway de conexão for alterado ou o endereço do servidor DNS for modificado

  Os perfis de conexão têm suporte somente para dispositivos que executam Windows e macOS.

- **Ativar modo ausente quando o Servidor de Administração não estiver disponível**

  Se esta opção estiver marcada, no caso da conexão com este perfil, os aplicativos instalados no dispositivo cliente irão usar as políticas de ausência de escritório, assim como as políticas de ausência de escritório. Se a política de ausência não estiver definida para o aplicativo, a política ativa será usada.

  Se esta opção estiver desativada, os aplicativos usarão as políticas ativas.

  Por padrão, esta opção está desativada.

Na subseção **Agendador de conexão**, você pode especificar os intervalos de tempo durante os quais o Agente de Rede envia dados para o Servidor de Administração:

- **Conectar quando necessário**

  Se esta opção estiver selecionada, a conexão é estabelecida quando o Agente de Rede tem de enviar dados para o Servidor de Administração.

  Por padrão, esta opção está selecionada.

- **Conectar-se nos intervalos de tempo especificados**

  Se esta opção estiver selecionada, o Agente de Rede se conecta ao Servidor de Administração numa hora específica. Você pode adicionar vários períodos de tempo de conexão.

Sondagem da rede por pontos de distribuição

Na seção **Sondagem da rede por pontos de distribuição**, você pode configurar a amostragem automática da rede. Você pode usar as seguintes opções para ativar a sondagem e definir a frequência:

- **Rede Windows**

  Se a esta opção estiver ativada, o Servidor de Administração automaticamente efetua a sondagem da rede de acordo com o agendamento configurado ao clicar nos links **Definir agendamento da sondagem rápida** e **Definir agendamento da sondagem completa**.

  Caso essa opção esteja desativada, o Servidor de Administração sonda a rede com o intervalo especificado no campo **Frequência de sondagens da rede (min.)**.

  O intervalo de descoberta de dispositivos para versões do Agente de Rede anteriores a 10.2 pode ser configurado nos campos **Frequência de sondagens de domínios Windows (min.)** (para a sondagem rápida de rede do Windows) e **Frequência de sondagens da rede (min.)** (para a sondagem completa de rede do Windows).

  Por padrão, esta opção está desativada.

- **Zeroconf**

  Se esta opção for ativada, o ponto de distribuição sondará automaticamente a rede com dispositivos IPv6 usando a rede zero configuração (também referida como *Zeroconf*). Nesse caso, a sondagem de intervalo de IP ativada é ignorada, porque o ponto de distribuição sonda toda a rede.

  Para começar a usar o Zeroconf, as seguintes condições devem ser atendidas:

  - O ponto de distribuição deve executar Linux.
  - Você deve instalar o utilitário avahi-browse no ponto de distribuição.

  Se essa opção estiver desativada, o ponto de distribuição não faz a sondagem com dispositivos IPv6y.

  Por padrão, esta opção está desativada.

- Intervalos de IPs

  Caso a opção esteja ativada, o ponto de distribuição automaticamente realiza a sondagem dos intervalos de IP de acordo com o agendamento configurado ao clicar no link **Definir agendamento da sondagem**.

  Se essa opção estiver desmarcada, o ponto de distribuição não faz a sondagem dos intervalos de IP.

  A frequência de sondagem de conjuntos de IPs para versões do Agente de Rede anteriores a 10.2 pode ser configurada no campo **Intervalo de sondagem (min.)**. O campo está disponível se a opção estiver ativada.

  Por padrão, esta opção está desativada.

- Active Directory

  Se a opção estiver habilitada, o ponto de distribuição sondará automaticamente o Active Directory de acordo com o agendamento que você configurou clicando no link **Definir agendamento da sondagem**.

  Se esta opção estiver desativada, o Servidor de Administração não faz a sondagem do Active Directory.

  A frequência de sondagem do Active Directory para versões do Agente de Rede anteriores a 10.2 pode ser configurada no campo **Intervalo de sondagem (min.)**. O campo está disponível caso a opção esteja ativada.

  Por padrão, esta opção está desativada.

Configurações de rede para pontos de distribuição

Na seção **Configurações de rede para pontos de distribuição**, você pode especificar as configurações de acesso à Internet:

- **Usar o servidor proxy**
- **Endereço**
- **Número da porta**
- Ignorar servidor proxy para endereços locais

  Se esta opção estiver ativada, nenhum servidor proxy será usado para se conectar aos dispositivos na rede local.

  Por padrão, esta opção está desativada.

- Autenticação do servidor proxy

  Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

  Por padrão, esta caixa de seleção está desmarcada.

- **Nome do usuário**
- **Senha**

KSN Proxy (pontos de distribuição)

Na seção **KSN Proxy (pontos de distribuição)**, você pode configurar o aplicativo para usar o ponto de distribuição para encaminhar solicitações da Kaspersky Security Network (KSN) por meio dos dispositivos gerenciados:

- **Ativar Proxy KSN no lado do ponto de distribuição**

  O serviço Proxy da KSN é executado no dispositivo que é usado como um ponto de distribuição. Use este recurso para redistribuir e otimizar o tráfego na rede.

  O ponto de distribuição envia as estatísticas da KSN, que são listadas na Declaração da Kaspersky Security Network, à Kaspersky. Por padrão, a Declaração da KSN está localizada em %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

  Por padrão, esta opção está desativada. A ativação desta opção somente terá efeito se as opções **Usar Servidor de Administração como um servidor proxy** e **Concordo em usar a Kaspersky Security Network** estiverem ativadas na janela de propriedades do Servidor de Administração.

  É possível atribuir um nó de um cluster ativo-passivo a um ponto de distribuição e habilitar o servidor proxy da KSN nesse nó.

- **Encaminhar solicitações da KSN para o Servidor de Administração**

  O ponto de distribuição encaminha solicitações do KSN dos dispositivos gerenciados para o Servidor de Administração.

  Por padrão, esta opção está ativada.

- **Acessar a KSN Cloud/KSN Privada diretamente pela internet**

  O ponto de distribuição encaminha solicitações à KSN dos dispositivos gerenciados para a KSN Cloud ou KSN Privada. As solicitações KSN geradas no próprio ponto de distribuição também são enviadas diretamente à KSN Cloud ou à KSN Privada.

  Os pontos de distribuição com o Agente de Rede versão 11 (ou anterior) instalado não podem acessar diretamente a KSN Privada. Se você deseja reconfigurar os pontos de distribuição para enviar solicitações à KSN à KSN Privada, ative a opção **Encaminhar solicitações da KSN para o Servidor de Administração** para cada ponto de distribuição.

  Os pontos de distribuição com o Agente de Rede versão 12 (ou posterior) instalado podem acessar diretamente a KSN Privada.

- **Porta**

  O número da porta TCP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. O número da porta padrão é 13111.

- **Porta UDP**

  Caso deseje que o Agente de Rede seja conectado com o Servidor de Administração por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de **Porta UDP**. Por padrão, esta opção está ativada. A porta UDP padrão para estabelecer conexão com o Servidor de Administração é 15000.

Atualizações (pontos de distribuição)

Na seção **Atualizações (pontos de distribuição)**, é possível ativar o recurso de download de arquivos diff, para que os pontos de distribuição recebam atualizações na forma de arquivos diff dos servidores de atualização da Kaspersky.

Histórico de revisões

Nessa guia, é possível visualizar a lista de revisões de política e reverter alterações feitas na política, se necessário.

Configuração manual da política do Kaspersky Endpoint Security

Esta seção fornece recomendações sobre como configurar a política do Kaspersky Endpoint Security. É possível executar a configuração na janela de propriedades da política. Ao editar uma configuração, clique no ícone de cadeado à direita do grupo relevante de configurações para aplicar os valores especificados a uma estação de trabalho.

Configurar a Kaspersky Security Network

A Kaspersky Security Network (KSN) é a infraestrutura de serviços em nuvem que tem informações sobre a reputação de arquivos, recursos da Web e software. A Kaspersky Security Network permite que o Kaspersky Endpoint Security for Windows responda mais rapidamente a diferentes tipos de ameaças, melhore o desempenho dos componentes de proteção e reduza a probabilidade de falsos positivos. Para obter mais informações sobre a Kaspersky Security Network, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

Para especificar as configurações recomendadas de KSN:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.
3. Nas propriedades da política, acesse **Configurações do aplicativo** → **Proteção Avançada Contra Ameaças** → **Kaspersky Security Network**.
4. Certifique-se de que a opção **Kaspersky Security Network** esteja ativada. Use esse recurso para redistribuir e otimizar o tráfego na rede.
5. Ativar o uso de servidores KSN se o serviço de proxy da KSN não estiver disponível. Os servidores KSN podem estar localizados no lado da Kaspersky (quando a KSN Global é usada) ou no lado de terceiros (quando a KSN Privada é usada).
6. Clique em **OK**.

As configurações de KSN recomendadas são especificadas.

Verificação da lista das redes protegidas por Firewall

Verifique se o Firewall do Kaspersky Endpoint Security for Windows protege todas as redes. Por padrão, o Firewall protege as redes com os seguintes tipos de conexão:

- **Rede pública**. Aplicativos de segurança, firewalls ou filtros não protegem dispositivos nessa rede.
- **Rede local**. O acesso a arquivos e impressoras é restrito para dispositivos nesta rede.
- **Rede confiável**. Os dispositivos dessa rede são protegidos contra ataques e acesso não autorizado a arquivos e dados.

Se você configurou uma rede personalizada, certifique-se de ela esteja protegida por Firewall. Para isso, verifique a lista de redes nas propriedades da política do Kaspersky Endpoint Security for Windows. A lista pode não conter todas as redes.

Para obter mais informações sobre o Firewall, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

Para verificar a lista de redes:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.
3. Nas propriedades de política, acesse **Configurações do aplicativo** → **Proteção Essencial Contra Ameaças** → **Firewall**.
4. Em **Redes disponíveis**, clique no link **Configurações de rede**.

   A janela de **Conexões de rede** é aberta. Esta janela exibe a lista de redes.
5. Caso a lista tenha uma rede ausente, basta adicioná-la.

Desativar a verificação de unidades de rede

Quando o Kaspersky Endpoint Security for Windows verifica as unidades de rede, isso pode sobrecarregá-las significativamente. É mais conveniente executar a verificação indireta em servidores de arquivos.

É possível desabilitar a verificação das unidades de rede nas propriedades de política do Kaspersky Endpoint Security for Windows. Para a descrição das propriedades da política, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

Para desativar a verificação de unidades de rede:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.
3. Nas propriedades de política, acesse **Configurações do aplicativo** → **Proteção Essencial Contra Ameaças** → **Proteção Contra Ameaças ao Arquivo**.

4. Em **Escopo de proteção**, desative a opção **Todas as unidades de rede**.

5. Clique em **OK**.

A verificação de unidades de rede está desativada.

Excluir detalhes de software da memória do Servidor de Administração

Recomendamos que o Servidor de Administração não salve as informações sobre módulos de software que sejam iniciados nos dispositivos de rede. Como resultado, a memória do Servidor de Administração não ficará sobrecarregada.

É possível desabilitar o salvamento dessas informações nas propriedades de política do Kaspersky Endpoint Security for Windows.

Para desativar a gravação de informações sobre os módulos de software instalados:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.

2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.

3. Nas propriedades de política, acesse **Configurações do aplicativo** → **Configurações gerais** → **Relatórios e armazenamento**.

4. Em **Transferência de dados para o Servidor de Administração**, desmarque a caixa de seleção **Sobre os aplicativos iniciados** se ainda estiver marcada na política de nível superior.

   Quando esta caixa de seleção for marcada, o banco de dados do Servidor de Administração salvará as informações sobre todas as versões de todos os módulos do software nos dispositivos em rede. Estas informações podem necessitar de uma quantidade significativa do espaço disponível em disco para o banco de dados do Kaspersky Security Center (dúzias de gigabytes).

As informações sobre módulos de software instalados não são mais salvas no banco de dados do Servidor de Administração.

Configurar o acesso à interface do Kaspersky Endpoint Security for Windows em estações de trabalho

Caso a proteção contra ameaças na rede da organização precise ser gerenciada no modo centralizado por meio do Kaspersky Security Center, especifique as configurações da interface nas propriedades da política do Kaspersky Endpoint Security for Windows, conforme descrito abaixo. Como resultado, você impedirá o acesso não autorizado ao Kaspersky Endpoint Security for Windows em estações de trabalho e a alteração das configurações do Kaspersky Endpoint Security for Windows.

Para a descrição das propriedades da política, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

Para especificar as configurações de interface recomendadas:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.
3. Nas propriedades de política, acesse **Configurações do aplicativo** → **Configurações gerais** → **Interface**.
4. Em **Interação com o usuário**, selecione a opção **Não exibir interface do usuário**. Isso desativa a exibição da interface do usuário do Kaspersky Endpoint Security for Windows nas estações de trabalho, para que seus usuários não possam alterar as configurações do Kaspersky Endpoint Security for Windows.
5. Em **Proteção por senha**, ative o botão de alternância. Isso reduz o risco de alterações não autorizadas ou não intencionais em configurações do Kaspersky Endpoint Security for Windows nas estações de trabalho.

As configurações recomendadas da interface do Kaspersky Endpoint Security for Windows são especificadas.

Salvar eventos de política importantes no banco de dados do Servidor de Administração

Para evitar a sobrecarga do banco de dados do Servidor de Administração, recomendamos que você salve apenas os eventos importantes no banco de dados.

Para configurar o registro de eventos importantes no banco de dados do Servidor de Administração:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique na política do Kaspersky Endpoint Security for Windows.

   A janela de propriedades da política selecionada é aberta.
3. Nas propriedades da política, abra a guia **Configuração de eventos**.

4. Na seção **Crítico**, clique em **Adicionar evento** e marque as caixas de seleção ao lado dos seguintes eventos apenas:

   - *O Contrato de Licença do Usuário Final foi violado*
   - *A execução automática do aplicativo está desativada*
   - *Erro de ativação*
   - *Ameaça ativa detectada. A Desinfecção avançada deve ser iniciada*
   - *Não é possível desinfectar*
   - *Detectado link perigoso aberto anteriormente*
   - *Processo encerrado*
   - *Atividade de rede bloqueada*
   - *Ataque de rede detectado*
   - *Proibida a inicialização do aplicativo*
   - *Acesso negado (bases locais)*
   - *Acesso negado (KSN)*
   - *Erro de atualização local*
   - *Não é possível iniciar duas tarefas simultaneamente*
   - *Erro de interação com o Kaspersky Security Center*
   - *Nem todos os componentes foram atualizados*
   - *Erro na aplicação das regras de criptografia/descriptografia do arquivo*
   - *Erro ao ativar o modo portátil*
   - *Erro ao desativar o modo portátil*
   - *Não foi possível carregar o módulo de criptografia*
   - *A política não pode ser aplicada*
   - *Erro ao alterar componentes do aplicativo*

5. Clique em **OK**.

6. Na seção **Falha funcional**, clique em **Adicionar evento** e selecione a caixa de seleção ao lado do evento *Configurações de tarefa inválidas. Configurações não aplicadas*.

7. Clique em **OK**.

8. Na seção **Advertência**, clique em **Adicionar evento** e marque as caixas de seleção ao lado dos seguintes eventos apenas:

    - *A Autodefesa está desativada*
    - *Componentes de proteção desativados*
    - *Chave de reserva inválido*
    - *Foi detectado um software legítimo que pode ser usado por intrusos para danificar seu computador ou dados pessoais (bancos locais)*
    - *Foi detectado um software legítimo que pode ser usado por intrusos para danificar seu computador ou dados pessoais (KSN)*
    - *Objeto excluído*
    - *Objeto desinfectado*
    - *O usuário optou por cancelar a política de criptografia*
    - *O arquivo foi restaurado da quarentena no servidor da Kaspersky Anti Targeted Attack Platform pelo administrador*
    - *O arquivo foi enviado para a quarentena no servidor da Kaspersky Anti Targeted Attack Platform pelo administrador*
    - *Mensagem de bloqueio de inicialização do aplicativo para o administrador*
    - *Mensagem de bloqueio de acesso ao dispositivo para o administrador*
    - *Mensagem de bloqueio de acesso à página da Web para o administrador*

9. Clique em **OK**.

10. Na seção **Informações**, clique em **Adicionar evento** e marque as caixas de seleção ao lado dos seguintes eventos apenas:

    - *Foi criada uma cópia de backup do objeto*
    - *Proibida a inicialização do aplicativo em modo de teste*

11. Clique em **OK**.

O registro de eventos importantes no banco de dados do Servidor de Administração é configurado.

Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security

A opção de agendamento ideal e recomendada para o Kaspersky Endpoint Security é **Quando novas atualizações são baixadas no repositório** quando a caixa de seleção **Usar retardo aleatório automaticamente para início da tarefa** estiver marcada.

Concedendo acesso offline ao dispositivo externo bloqueado pelo Controle de Dispositivos

No componente Controle de Dispositivos da política do Kaspersky Endpoint Security for Windows, você pode gerenciar o acesso do usuário a dispositivos externos instalados ou conectados ao dispositivo cliente (por exemplo, discos rígidos, câmeras ou módulos Wi-Fi). Isso permite proteger o dispositivo cliente contra infecções quando esses dispositivos externos são conectados e impedir a perda ou vazamento de dados.

Se você precisar conceder acesso temporário ao dispositivo externo bloqueado pelo Controle de Dispositivos, mas não for possível adicionar o dispositivo à lista de dispositivos confiáveis, você poderá conceder acesso offline temporário ao dispositivo externo. Acesso off-line significa que o dispositivo cliente não tem nenhum acesso à rede.

É possível conceder acesso offline ao dispositivo externo bloqueado pelo Controle de Dispositivos somente se a opção **Permitir solicitações de acesso temporário** estiver ativada nas configurações da política do Kaspersky Endpoint Security for Windows, na seção **Configurações do aplicativo → Controles de segurança → Controle de dispositivos**.

A concessão de acesso offline ao dispositivo externo bloqueado pelo Controle de Dispositivos inclui as seguintes fases:

1. Na janela de diálogo Kaspersky Endpoint Security for Windows, o usuário do dispositivo que deseja acessar o dispositivo externo bloqueado gera um arquivo de solicitação de acesso e o envia ao administrador do Kaspersky Security Center.

2. Ao obter essa solicitação, o administrador do Kaspersky Security Center cria um arquivo de chave de acesso e o envia ao usuário do dispositivo.

3. Na janela de diálogo Kaspersky Endpoint Security for Windows, o usuário do dispositivo ativa o arquivo da chave de acesso e obtém acesso temporário ao dispositivo externo.

Para conceder acesso temporário ao dispositivo externo bloqueado pelo Controle de Dispositivos:

1. No menu principal, vá para **Dispositivos → Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Nesta lista, selecione o dispositivo do usuário que solicita acesso ao dispositivo externo bloqueado pelo Controle de Dispositivos.

   Você pode selecionar apenas um dispositivo.

3. Acima da lista de dispositivos gerenciados, clique no botão de elipse (...) e, em seguida, clique no botão **Permitir acesso ao dispositivo em modo offline**.

4. Na janela **Configurações do aplicativo** que se abre, na seção **Controle de Dispositivos**, clique no botão **Procurar**.

5. Selecione o arquivo de solicitação de acesso que você recebeu do usuário e clique no botão **Abrir**. O arquivo deve ter o formato AKEY.

   Os detalhes do dispositivo bloqueado para o qual o usuário solicitou acesso são exibidos.

6. Especifique o valor da configuração de **Duração do acesso**.

   Essa configuração define o período durante o qual você concede ao usuário acesso ao dispositivo bloqueado. O valor padrão é o valor especificado pelo usuário ao criar o arquivo de acesso à solicitação.

7. Especifique o período durante o qual a chave de acesso pode ser ativada no dispositivo.

   Essa configuração define o período durante o qual o usuário pode ativar o acesso ao dispositivo bloqueado usando a tecla de acesso fornecida.

8. Clique no botão **Salvar**.

   Isso abre a janela padrão **Salvar chave de acesso** do Microsoft Windows.

9. Selecione a pasta de destino na qual deseja salvar o arquivo que contém a chave de acesso do dispositivo bloqueado.

10. Clique no botão **Salvar**.

Como resultado, quando você envia ao usuário o arquivo da chave de acesso e o ativa na janela de diálogo do Kaspersky Endpoint Security for Windows, o usuário tem acesso temporário ao dispositivo bloqueado durante o período específico.

Remover aplicativos ou atualizações de software remotamente

Para remover aplicativos ou atualizações de software remotamente de dispositivos selecionados:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Desinstalar aplicativo remotamente**.

4. Especifique o nome da tarefa que está criando.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).

5. Dispositivos aos quais a tarefa será atribuída.

6. Selecione o tipo de software que deseja remover e, em seguida, selecione os aplicativos, atualizações ou patches específicos que deseja remover:

   - **Desinstalar o aplicativo gerenciado**

     Uma lista de aplicativos da Kaspersky é exibida. Selecione o aplicativo que deseja remover.

   - **Desinstalar aplicativo incompatível**

     Uma lista de aplicativos incompatíveis com os aplicativos de segurança da Kaspersky ou do Kaspersky Security Center é exibida. Marque as caixas de seleção ao lado dos aplicativos que deseja remover.

   - **Desinstalar aplicativo do registro de aplicativos**

Por padrão, os Agentes de Rede enviam ao Servidor de Administração informações sobre os aplicativos instalados nos dispositivos gerenciados. A lista de aplicativos instalados é armazenada no registro de aplicativos.

Para selecionar um aplicativo no registro de aplicativos:

a. Clique no campo **Aplicativo a ser desinstalado** e selecione o aplicativo que deseja remover.

Se você selecionar o Agente de Rede do Kaspersky Security Center, ao executar a tarefa, o status *Concluído com êxito* mostra que o processo de remoção foi iniciado. Se o Agente de Rede do Kaspersky Security Center for removido, o status não será alterado. Se a tarefa falhar, o status será alterado para *Falha*.

b. Especifique as opções de desinstalação:

- Modo de desinstalação

Selecione como deseja remover o aplicativo:

- **Definir o comando de desinstalação automaticamente**

  Se o aplicativo tiver um comando de desinstalação definido pelo fornecedor do aplicativo, o Kaspersky Security Center usa esse comando. Recomendamos que você selecione esta opção.

- **Especificar o comando de desinstalação**

  Selecione esta opção se desejar especificar seu próprio comando para a desinstalação do aplicativo.

  Recomendamos que você primeiro tente remover o aplicativo usando a opção **Definir o comando de desinstalação automaticamente**. Se a desinstalação por meio do comando definido automaticamente falhar, use seu próprio comando.

  Digite um comando de instalação no campo e especifique a seguinte opção:

  Use este comando para desinstalação apenas se o comando padrão não tiver sido autodetectado

  O Kaspersky Security Center verifica se o aplicativo selecionado tem ou não um comando de desinstalação definido pelo fornecedor do aplicativo. Se o comando for encontrado, o Kaspersky Security Center o usará em vez do comando especificado no campo **Comando para desinstalação de aplicativos**.

  Recomendamos que você ative esta opção.

- Efetuar reinício após a desinstalação bem-sucedida do aplicativo

Se o aplicativo exigir que o sistema operacional seja reiniciado no dispositivo gerenciado após a desinstalação bem-sucedida, o sistema operacional será reiniciado automaticamente.

- **Desinstalar a atualização, patch ou o aplicativo de terceiro especificado**

  Uma lista de atualizações, patches e aplicativos de terceiros é exibida. Selecione o item que deseja remover.

  A lista exibida é uma lista geral de aplicativos e atualizações e não corresponde aos aplicativos e atualizações instalados nos dispositivos gerenciados. Antes de selecionar um item, recomendamos que você verifique se o aplicativo ou a atualização está instalada nos dispositivos definidos no escopo da tarefa. Você pode visualizar a lista de dispositivos nos quais o aplicativo ou a atualização está instalada por meio da janela de propriedades.

  Para visualizar a lista de dispositivos:

  a. Clique no nome do aplicativo ou da atualização.

     A janela de propriedades é exibida.

  b. Abra a seção **Dispositivos**.

     Você também pode visualizar a lista de aplicativos e atualizações instalados na janela de propriedades do dispositivo.

7. Especifique como os dispositivos clientes farão o download do utilitário de desinstalação:

- **Usando o Agente de Rede**

  Os arquivos são entregues aos dispositivos clientes pelo Agente de Rede instalado nesses dispositivos.

  Se esta opção estiver desativada, os arquivos serão entregues usando ferramentas do Microsoft Windows.

  Recomendamos que você ative esta opção se a tarefa tiver sido atribuída a dispositivos com o Agente de Rede instalado.

- **Usando recursos do sistema operacional através do Servidor de Administração**

  Os arquivos são transmitidos para dispositivos clientes usando as ferramentas do sistema operacional do Servidor de Administração. Você pode ativar esta opção se nenhum Agente de Rede estiver instalado no dispositivo cliente, mas o dispositivo cliente está na mesma rede que o Servidor de Administração.

- **Usando recursos do sistema operacional através de pontos de distribuição**

  Os arquivos são transmitidos para dispositivos clientes usando ferramentas do sistema operacional por meio de pontos de distribuição. Você pode ativar esta opção se houver, no mínimo, um ponto de distribuição na rede.

  Se a opção **Usando o Agente de Rede** estiver marcada, os arquivos serão entregues por meio das ferramentas do sistema operacional somente se os recursos do Agente de Rede estiverem indisponíveis.

- **Número máximo de downloads concomitantes**

  O número máximo permitido de dispositivos clientes para os quais o Servidor de Administração pode transmitir os arquivos simultaneamente. Quanto maior esse número, mais rápido o aplicativo será desinstalado, mas a carga no Servidor de Administração será maior.

- **Número máximo de tentativas de desinstalação**

Se, ao executar a tarefa *Desinstalar aplicativo remotamente*, o Kaspersky Security Center falhar em desinstalar um aplicativo em um dispositivo gerenciado dentro do número de execuções do instalador especificado pelo parâmetro, o Kaspersky Security Center interromperá a entrega do pacote de desinstalação a este dispositivo gerenciado e não iniciará mais o instalador no dispositivo.

O parâmetro **Número máximo de tentativas de desinstalação** permite salvar os recursos do dispositivo gerenciado, assim como reduzir o tráfego (desinstalação, execução do arquivo MSI e mensagens de erro).

As tentativas recorrentes de início de tarefas podem indicar um problema no dispositivo e que impede a desinstalação. O administrador deve resolver o problema dentro do número especificado de tentativas de desinstalação e, em seguida, reiniciar a tarefa (manualmente ou por programação).

Se a desinstalação não for realizada eventualmente, o problema será considerado não solucionável e quaisquer tarefas adicionais serão consideradas como custosas em temos de consumo desnecessário de recursos e tráfego.

Quando a tarefa é criada, o contador de tentativas fica definido como `0`. Cada execução do instalador retorna um erro no dispositivo e incrementa a leitura do contador.

Se o número de tentativas especificado no parâmetro tiver sido excedido e o dispositivo estiver pronto para a desinstalação do aplicativo, você poderá aumentar o valor do parâmetro **Número máximo de tentativas de desinstalação** e iniciar a tarefa para desinstalar o aplicativo. Alternativamente, você pode criar uma nova tarefa *Desinstalar aplicativo remotamente*.

- Verificar o tipo do sistema operacional antes de baixar

  Antes de transmitir os arquivos para dispositivos clientes, o Kaspersky Security Center verifica se as configurações do pacote de instalação são aplicáveis ao sistema operacional do dispositivo cliente. Caso as configurações não sejam aplicáveis, o Kaspersky Security Center não transmitirá os arquivos e não tentará instalar o aplicativo. Por exemplo, para instalar algum aplicativo em dispositivos de um grupo de administração que inclui dispositivos que executam vários sistemas operacionais, é possível atribuir a tarefa de instalação ao grupo de administração e então ativar essa opção para ignorar os dispositivos que executem um sistema operacional diferente do requerido.

- Usar senha de desinstalação

  Esse parâmetro será exibido se, na etapa anterior, a opção **Desinstalar aplicativo gerenciado** foi selecionada e, em seguida, o Agente de Rede do Kaspersky Security Center foi especificado no campo **Aplicativo a ser desinstalado**.

  Caso tenha definido anteriormente a senha para a desinstalação remota do Agente de Rede nas configurações de política do Agente de Rede, marque a caixa de seleção **Usar senha de desinstalação** e insira a senha de desinstalação no campo **Senha**. Caso não tenha definido a senha para a desinstalação remota do Agente de Rede, não marque a caixa de seleção.

8. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

9. Se necessário, adicione as contas que serão usadas para iniciar a tarefa de desinstalação remota:

- **Nenhuma conta necessária (Agente de Rede instalado)**

  Se essa caixa de seleção estiver selecionada, você não precisará especificar uma conta sob a qual o instalador do aplicativo será executado. A tarefa será executada sob a conta sob a qual o serviço do Servidor de Administração está sendo executado.

  Caso o Agente de Rede não tenha sido instalado em dispositivos cliente, a opção não estará disponível.

- **Conta necessária (Agente de Rede não é usado)**

  Selecione esta opção se o Agente de Rede não estiver instalado nos dispositivos aos quais você atribui a tarefa de *Desinstalar aplicativo remotamente*. Nesse caso, é possível especificar uma conta de usuário ou um certificado SSH para desinstalar o aplicativo.

  - **Conta local**. Se essa opção estiver selecionada, especifique a conta de usuário sob a qual o instalador do aplicativo será executado. Clique no botão **Adicionar**, selecione **Conta local** e, então, especifique as credenciais da conta do usuário.

    É possível especificar várias contas de usuário se, por exemplo, nenhuma delas tiver todos os direitos necessários em todos os dispositivos para os quais você atribui a tarefa. Nesse caso, todas as contas adicionadas são usadas para executar a tarefa, em ordem consecutiva, de cima para baixo.

  - **Certificado SSH**. Se quiser desinstalar um aplicativo de um dispositivo cliente baseado em Linux, é possível especificar um certificado SSH em vez de uma conta de usuário. Clique no botão **Adicionar**, selecione **Certificado SSH** e, então, especifique as chaves privada e pública do certificado.

    Para gerar uma chave privada, você pode usar o utilitário ssh-keygen. Observe que o Kaspersky Security Center é compatível com o formato PEM de chaves privadas, mas o utilitário ssh-keygen gera chaves SSH no formato OPENSSH por padrão. O formato OPENSSH não é compatível com o Kaspersky Security Center. Para criar uma chave privada no formato PEM compatível, adicione a opção -m PEM no comando ssh-keygen.

    Por exemplo:

    ```
    ssh-keygen -m PEM -t rsa -b 4096 -C "<e-mail do usuário>"
    ```

10. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    A tarefa é criada e exibida na lista de tarefas.

12. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

13. Na janela Propriedades da tarefa, especifique as configurações gerais da tarefa.

14. Clique no botão **Salvar**.

15. Execute a tarefa manualmente ou aguarde que ela seja inicializada de acordo com a programação que você especificou nas configurações da tarefa.

    Após a conclusão da tarefa de desinstalação remota, o aplicativo selecionado será removido dos dispositivos clientes selecionados.

Problemas na desinstalação remota

Às vezes, a desinstalação remota de aplicativos de terceiros pode terminar com a seguinte advertência: "A desinstalação remota foi concluída neste dispositivo com avisos: o aplicativo para remoção não está instalado". Esse problema ocorre quando o aplicativo em questão já foi desinstalado ou foi instalado apenas para um usuário individual. Os aplicativos instalados para um usuário individual (também chamados de aplicativos por usuário) ficam invisíveis e não podem ser desinstalados remotamente se o usuário não estiver conectado.

Esse comportamento se diferencia de aplicativos destinados ao uso por vários usuários no mesmo dispositivo (também chamados de aplicativos por dispositivo). Os aplicativos por dispositivo ficam visíveis e acessíveis a todos os usuários do dispositivo.

Portanto, os aplicativos por usuário devem ser desinstalados somente quando o usuário estiver conectado.

Fonte de informação sobre os aplicativos instalados

O Agente de Rede recupera informações sobre software instalado em dispositivos Windows das seguintes chaves de registro:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para todos os usuários.

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para todos os usuários.

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para o usuário atual.

- HKEY_USER<...>\Software\Microsoft\Windows\CurrentVersion\Uninstall

  Contém informações sobre aplicativos instalados para usuários específicos.

Reverter um objeto para uma revisão anterior

Você poderá reverter as alterações feitas à um objeto, se necessário. Por exemplo, você poderá ter que reverter as configurações de uma política ao seu estado em uma data específica.

Para reverter as alterações feitas à um objeto:

1. Na janela de propriedades do objeto, abra a guia **Histórico de revisões**.
2. Na lista de revisões do objeto, selecione a revisão para a qual você precisa reverter as modificações.
3. Clique no botão **Reverter**.
4. Clique em **OK** para confirmar a operação.

   O objeto é agora revertido à revisão selecionada. A lista de revisões de objeto exibe um registro da ação que foi executada. A descrição da revisão exibe as informações sobre o número da revisão à qual você reverteu o objeto.

A operação de reversão está disponível apenas para objetos de política e tarefa.

Tarefas

Esta seção descreve as tarefas utilizadas pelo Kaspersky Security Center.

Sobre as tarefas

O Kaspersky Security Center gerencia os aplicativos de segurança da Kaspersky instalados nos dispositivos cliente criando e executando *tarefas*. As tarefas são necessárias para a instalação, inicialização e interrupção de aplicativos, verificação de arquivos, atualização de bancos de dados e módulos de software e para a realização de outras ações em aplicativos.

As tarefas de um aplicativo específico podem ser criadas usando o Kaspersky Security Center Web Console apenas se o plugin de gerenciamento desse aplicativo estiver instalado no Kaspersky Security Center Web Console Server.

As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

As tarefas executadas no Servidor de Administração incluem o seguinte:

- Distribuição automática de relatórios
- Download de atualizações para o repositório
- Backup de dados do Servidor de Administração
- Manutenção do banco de dados

Os seguintes tipos de tarefas são executados nos dispositivos:

- *Tarefas locais* – Tarefas que são executadas em um dispositivo específico

  As tarefas locais podem ser modificadas pelo administrador usando as ferramentas do Console de Administração ou pelo usuário de um dispositivo remoto (por exemplo, através da interface do aplicativo de segurança). Se uma tarefa local tiver sido modificada simultaneamente pelo administrador e pelo usuário de um dispositivo gerenciado, as modificações feitas pelo administrador entrarão em vigor porque elas têm uma maior prioridade.

- *Tarefas de grupo* – Tarefas que são executadas em todos os dispositivos de um grupo específico

  Salvo de especificado de outra maneira nas propriedades de tarefa, uma tarefa de grupo também afeta todos os subgrupos do grupo selecionado. Uma tarefa de grupo também afeta (opcionalmente) os dispositivos que foram conectados aos Servidores de Administração secundários e virtuais implementados no grupo ou em algum dos seus subgrupos.

- *Tarefas globais* – Tarefas que são realizadas em um conjunto de dispositivos, independentemente se os mesmos estão incluídos em qualquer grupo

Para cada aplicativo, você pode criar qualquer número de tarefas de grupo, tarefas globais ou tarefas locais.

Você pode efetuar alterações nas configurações de tarefas, exibir o andamento das tarefas, copiar, exportar, importar e excluir tarefas.

Uma tarefa é iniciada em um dispositivo cliente somente se um aplicativo para o qual a tarefa foi criada estiver sendo executado.

Os resultados da execução das tarefas no log de eventos do sistema operacional em cada dispositivo, no log de eventos do sistema operacional: do Servidor de Administração e no banco de dados do Servidor de Administração.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Sobre o escopo de tarefa

O *escopo de uma tarefa* é o conjunto de dispositivos nos quais a tarefa é executada. Os tipos de escopo são os seguintes:

- Para uma *tarefa local*, o escopo é o próprio dispositivo.
- Para uma tarefa do *Servidor de Administração*, o escopo é o Servidor de Administração.
- Para uma *tarefa de grupo*, o escopo é a lista de dispositivos incluídos no grupo.

Ao criar uma *tarefa global*, você pode usar os seguintes métodos para especificar o escopo:

- Especificar determinados dispositivos manualmente.

  Você pode usar um endereço IP (ou uma faixa IP), nome NetBIOS ou nome DNS como o endereço do dispositivo.

- Importar uma lista de dispositivos de um arquivo TXT com os endereços dos dispositivos a serem adicionados (cada endereço deve ser colocado em uma linha individual).

  Se você importar uma lista de dispositivos a partir de um arquivo ou cria uma lista manualmente, e se os dispositivos cliente estão identificados pelos seus nomes, a lista deve conter somente os dispositivos cuja informação já foi adicionada ao banco de dados do Servidor de Administração. Além disso, as informações devem ter sido inseridas quando os dispositivos foram conectados ou durante a descoberta de dispositivos.

- Especificar uma seleção de dispositivos.

  Ao longo do tempo, o escopo de uma tarefa se modifica quando o conjunto de dispositivos incluídos na seleção são modificados. Uma seleção de dispositivos pode ser feita com base nos atributos do dispositivo, incluindo o software instalado em um dispositivo, e com base em tags atribuídas aos dispositivos. A seleção de dispositivos é o modo mais flexível para especificar o escopo de uma tarefa.

  As tarefas para seleções de dispositivos sempre são executadas de acordo com um agendamento pelo Servidor de Administração. Estas tarefas não podem ser executadas em dispositivos que não tenham uma conexão com o Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas diretamente nos dispositivos e, por isso, não dependem da conexão do dispositivo com o Servidor de Administração.

As tarefas para Seleções de dispositivos não são executadas na hora local de um dispositivo; em vez disso, elas serão executadas na hora local do Servidor de Administração. As tarefas cujo escopo é especificado por outros métodos são executadas na hora local de um dispositivo.

Criar uma tarefa

Para criar uma tarefa:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as instruções.
3. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
4. Clique no botão **Concluir**.

A tarefa é criada e exibida na lista de tarefas.

Para criar uma nova tarefa atribuída aos dispositivos selecionados:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, marque as caixas de seleção ao lado dos dispositivos para executar a tarefa para eles. Você pode usar as funções de pesquisa e filtro para encontrar os dispositivos que está procurando.

3. Clique no botão **Executar a tarefa** e selecione **Adicionar uma nova tarefa**.

   O Assistente para novas tarefas inicia.

   Na primeira etapa do assistente, você pode remover os dispositivos selecionados para incluir no escopo da tarefa. Siga as instruções do assistente.

4. Clique no botão **Concluir**.

A tarefa é criada para os dispositivos selecionados.

Como iniciar uma tarefa manualmente

O aplicativo inicia as tarefas de acordo com as configurações de agendamento especificadas nas propriedades de cada tarefa. Você pode iniciar uma tarefa manualmente a qualquer momento por meio da lista de tarefas. Você também pode selecionar dispositivos na lista **Dispositivos gerenciados** e, em seguida, iniciar uma tarefa existente para eles.

Para iniciar uma tarefa manualmente:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Na lista de tarefas, selecione a caixa de seleção ao lado da tarefa que deseja iniciar.

3. Clique no botão **Iniciar**.

A tarefa é iniciada. Você pode verificar o status da tarefa na coluna **Status** ou clicando no botão **Resultado**.

Visualizando a lista de tarefas

Você pode ver a lista de tarefas criadas no Kaspersky Security Center.

Para visualizar a lista de tarefas,

No menu principal, vá para **Dispositivos** → **Tarefas**.

A lista de tarefas é exibida. As tarefas são agrupadas pelos nomes dos aplicativos aos quais estão relacionados. Por exemplo, a tarefa *Desinstalar aplicativo remotamente* está relacionada ao Servidor de Administração e a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ao Agente de Rede.

Para visualizar as propriedades de uma tarefa,

Clique no nome da tarefa.

A janela de propriedades da tarefa é exibida com várias guias nomeadas. Por exemplo, **Tipo de tarefa** é exibido na guia **Geral** e o agendamento de tarefas - na guia **Agendamento**.

Configurações de tarefa gerais

Esta seção contém as configurações que podem ser definidas e especificadas para a maioria das tarefas. A lista de configurações disponíveis depende da tarefa que se está configurando.

Configurações especificadas durante a criação de tarefa

Você pode especificar as seguintes configurações ao criar uma tarefa. Algumas dessas configurações também podem ser modificadas nas propriedades da tarefa criada.

- Configurações para reiniciar o sistema operacional:
  - **Não reiniciar o dispositivo**

    Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

  - **Reiniciar o dispositivo**

    Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

  - **Perguntar ao usuário o que fazer**

    O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

    Por padrão, esta opção está selecionada.

  - **Repetir aviso a cada (min.)**

    Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

    Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

    Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

  - **Reiniciar após (min.)**

    Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

    Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  - **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

- Configurações de agendamento de tarefas:
  - **Configuração Início agendado:**
    - A cada N horas

      A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

      Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

    - A cada N dias

      A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

      Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

    - A cada N semanas

      A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

      Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

    - A cada N minutos

      A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

      Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

    - Diariamente (não é compatível com horário de verão)

A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

Por padrão, a tarefa inicia diariamente na hora atual do sistema.

- **Semanalmente**

  A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Manualmente**

  A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

  Por padrão, esta opção está selecionada.

- **Todos os meses em dias especificados das semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **Quando novas atualizações são baixadas no repositório**

  A tarefa é executada após as atualizações serem baixadas no repositório. Por exemplo, pode ser necessário usar esse agendamento para a tarefa Encontrar as vulnerabilidades e atualizações necessárias.

- **No surto de vírus**

A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

- Antivírus para estações de trabalho e servidores de arquivo
- Antivírus para defesa de perímetro
- Antivírus para sistemas de correio

Por padrão, todos os tipos de aplicativos estão selecionados.

Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

  Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

  Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

  Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

  Por padrão, esta opção está desativada.

- **Usar retardo aleatório automaticamente para início da tarefa**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

- Dispositivos aos quais a tarefa será atribuída:
  - **Selecionar os dispositivos na rede detectados pelo Servidor de Administração**

    A tarefa é atribuída a dispositivos específicos. Os dispositivos específicos podem incluir dispositivos em grupos de administração, assim como dispositivos não atribuídos.

    Por exemplo, pode ser necessário usar esta opção em uma tarefa de instalação do Agente de Rede em dispositivos não atribuídos.

  - **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**

    Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

    Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

  - **Atribuir a tarefa a uma seleção de dispositivos**

    A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

    Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

  - **Atribuir tarefa a um grupo de administração**

    A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

    Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

    Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

- Configurações de conta:
  - **Conta padrão**

    A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

    Por padrão, esta opção está selecionada.

  - **Especificar uma conta**

    Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

  - **Conta**

Conta sob a qual a tarefa é executada.

- **Senha**

  Senha da conta sob a qual a tarefa será executada.

Configurações especificadas após a criação da tarefa

Você pode especificar as seguintes configurações após criar uma tarefa.

- Configurações de tarefa de grupo:
  - **Distribuir para subgrupos**

    Essa opção só está disponível nas configurações das tarefas de grupo.

    Quando essa opção está habilitada, o escopo da tarefa inclui:

    - O grupo de administração selecionado ao criar a tarefa.
    - Os grupos de administração subordinados ao grupo de administração selecionado em qualquer nível abaixo da hierarquia do grupo.

    Quando essa opção está desabilitada, o escopo da tarefa inclui apenas o grupo de administração selecionado ao criar a tarefa.

    Por padrão, esta opção está ativada.

  - **Distribuir em Servidores de Administração secundários e virtuais**

    Quando essa opção está habilitada, a tarefa efetiva no Servidor de Administração principal também é aplicada nos Servidores de Administração secundários (incluindo os virtuais). Caso já exista uma tarefa do mesmo tipo no Servidor de Administração secundário, ambas as tarefas serão aplicadas no Servidor de Administração secundário (a existente e a herdada do Servidor de Administração principal).

    Essa opção só está disponível quando a opção **Distribuir para subgrupos** está habilitada.

    Por padrão, esta opção está desativada.

- Configurações de agendamento avançado:
  - **Ligar dispositivos usando a função Wake-On-LAN antes de iniciar a tarefa (min.)**

    O sistema operacional do dispositivo selecionado inicia na hora especificada, antes do início da tarefa. O período de tempo padrão é de cinco minutos.

    Ative esta opção se você quiser que a tarefa seja executada em todos os dispositivos clientes do escopo da tarefa, inclusive nos dispositivos que são desligados quando a tarefa está prestes a ser iniciada.

    Se você quiser que o dispositivo seja desativado automaticamente após a conclusão da tarefa, ative a opção **Desligar os dispositivos após concluir a tarefa**. Esta opção pode ser encontrada na mesma janela.

    Por padrão, esta opção está desativada.

  - **Desligar os dispositivos após concluir a tarefa**

Por exemplo, pode ser necessário ativar esta opção para uma tarefa que instala atualizações nos dispositivos clientes todas as sextas-feiras após o horário comercial e, em seguida, desliga esses dispositivos durante o fim de semana.

Por padrão, esta opção está desativada.

- **Parar a tarefa se ela for executada por mais que (min.)**

  Após o final do período especificado, a tarefa é interrompida automaticamente, quer tenha sido concluída ou não.

  Ative esta opção se você quiser interromper (ou parar) tarefas que levam muito tempo para serem executadas.

  Por padrão, esta opção está desativada. O tempo predefinido de execução da tarefa é de 120 minutos.

- Configurações de notificação:
  - Bloco **Armazenar histórico de tarefas**:
    - Armazenar no banco de dados do Servidor de Administração por (dias)

      Os eventos de aplicativo relacionados à execução da tarefa em todos os dispositivos clientes do escopo da tarefa são armazenados no Servidor de Administração durante o número de dias especificado. Quando esse período termina, as informações são excluídas do Servidor de Administração.

      Por padrão, esta opção está ativada.

    - Armazenar no log de eventos do SO no dispositivo

      Os eventos de aplicativo relacionados à execução da tarefa são armazenados localmente no Log de Eventos do Windows de cada dispositivo cliente.

      Por padrão, esta opção está desativada.

    - Armazenar no log de eventos do SO no Servidor de Administração

      Os eventos de aplicativo relacionados à execução da tarefa em todos os dispositivos cliente do escopo da tarefa são armazenados centralmente no Log de Eventos do Windows do sistema operacional (SO) do Servidor de Administração.

      Por padrão, esta opção está desativada.

    - Salvar todos os eventos

      Se esta opção estiver selecionada, todos os eventos relacionados à tarefa serão salvos nos logs de eventos.

    - Salvar eventos relacionados ao progresso da tarefa

      Se esta opção estiver selecionada, apenas os eventos relacionados à execução da tarefa serão salvos nos logs de eventos.

    - Salvar apenas os resultados da execução da tarefa

      Se esta opção estiver selecionada, apenas os eventos relacionados aos resultados da tarefa serão salvos nos logs de eventos.

  - Notify administrator of task execution results

    Você pode selecionar os métodos pelos quais os administradores recebem notificações sobre os resultados de execução da tarefa: por e-mail, por SMS e pela execução de um arquivo executável. Para configurar a notificação, clique em link **Configurações**.

    Por padrão, todos os métodos de notificação estão desativados.

  - Notificar somente erros

Se esta opção estiver ativada, os administradores serão notificados apenas quando uma execução de tarefa for concluída com um erro.

Se esta opção estiver desativada, os administradores serão notificados após cada conclusão de execução de tarefa.

Por padrão, esta opção está ativada.

- Configurações de segurança.
- Configurações do escopo da tarefa.

  Dependendo de como o escopo da tarefa é determinado, as seguintes configurações estão presentes:

  - Dispositivos

    Se o escopo de uma tarefa for determinado por um grupo de administração, você pode exibir visualizar esse grupo. Nenhuma alteração está disponível nesse ponto. No entanto, você pode definir **Exclusões do escopo da tarefa**.

    Se o escopo de uma tarefa for determinado por uma lista de dispositivos, você pode alterar essa lista adicionando e removendo dispositivos.

  - Seleção de dispositivos

    Você pode alterar a seleção de dispositivos aos quais a tarefa é aplicada.

  - Exclusões do escopo da tarefa

    Você pode especificar grupos de dispositivos aos quais a tarefa não é aplicada. Os grupos a serem excluídos podem somente ser subgrupos do grupo de administração ao qual a tarefa é aplicada.

- **Histórico de revisão**.

Exportação de tarefa

O Kaspersky Security Center permite salvar uma tarefa e suas configurações em um arquivo KLT. Você pode usar este arquivo KLT para importar a tarefa salva tanto para o Kaspersky Security Center Windows quanto para o Kaspersky Security Center Linux.

Para exportar uma tarefa:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Marque a caixa de seleção ao lado da tarefa que deseja exportar.

   Você não pode exportar várias tarefas ao mesmo tempo. Se selecionar mais de uma tarefa, o botão **Exportar** será desabilitado. As tarefas do Servidor de Administração também ficam indisponíveis para exportação.

3. Clique no botão **Exportar**.

4. Na janela **Salvar como** que abrir, especifique o nome e o caminho do arquivo de tarefa. Clique no botão **Salvar**.

   A janela **Salvar como** é exibida apenas se você usar Google Chrome, Microsoft Edge ou Opera. Se usar outro navegador, o arquivo da tarefa será salvo automaticamente na pasta **Downloads**.

Importação de uma tarefa

O Kaspersky Security Center permite importar uma tarefa de um arquivo KLT. O arquivo KLT contém a tarefa exportada e suas configurações.

Para importar uma tarefa:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Clique no botão **Importar**.

3. Clique no botão **Procurar** para escolher um arquivo de tarefa que você deseja importar.

4. Na janela aberta, especifique o caminho para o arquivo de tarefa KLT e clique no botão **Abrir**. Observe que você pode selecionar apenas um arquivo de tarefa.

   O processamento da tarefa é iniciado.

5. Após o processamento com êxito da tarefa, selecione os dispositivos aos quais deseja atribuir a tarefa. Para fazer isso, selecione uma das seguintes opções:

   - **Atribuir tarefa a um grupo de administração**

     A tarefa é atribuída aos dispositivos incluídos em um grupo de administração. Você pode especificar um dos grupos existentes ou criar um novo grupo.

     Por exemplo, pode ser necessário usar esta opção para executar uma tarefa para enviar uma mensagem aos usuários caso a mensagem seja específica para os dispositivos incluídos em um grupo de administração específico.

     Caso uma tarefa seja atribuída a um grupo de administração, a guia **Segurança** não será exibida na janela de propriedades da tarefa porque as tarefas de grupo estão sujeitas às configurações de segurança dos grupos aos quais se aplicam.

   - **Especificar endereços de dispositivos manualmente ou importar endereços de uma lista**

     Você pode especificar nomes de NetBIOS, nomes de DNS, endereços IP e sub-redes IP de dispositivos aos quais você precisar atribuir a tarefa.

     Pode ser necessário usar esta opção para executar uma tarefa para uma subrede específica. Por exemplo, pode ser necessário instalar um determinado aplicativo nos dispositivos de contadores ou verificar dispositivos em uma subrede que possivelmente está infectada.

   - **Atribuir a tarefa a uma seleção de dispositivos**

     A tarefa é atribuída aos dispositivos incluídos em uma seleção de dispositivos. Você pode especificar uma das seleções existentes.

     Por exemplo, pode ser necessário usar esta opção para executar uma tarefa em dispositivos com uma versão de sistema operacional específica.

6. Especifique o escopo da tarefa.

7. Clique no botão **Concluir** para encerrar a importação da tarefa.

A notificação com os resultados da importação é exibida. Se a tarefa for importada com êxito, será possível clicar no link **Detalhes** para visualizar as propriedades da tarefa.

Após a importação com êxito, a tarefa será exibida na lista de tarefas. As configurações de tarefa e o agendamento também são importados. A tarefa será iniciada de acordo com seu agendamento.

Se a tarefa recém-importada tiver um nome idêntico a uma tarefa existente, o nome da tarefa importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Iniciar o Assistente para alterar a senha das tarefas

Para uma tarefa não local, você pode especificar uma conta na qual a tarefa deve ser executada. Você pode especificar a conta durante a criação da tarefa ou nas propriedades de uma tarefa existente. Se a conta especificada for usada de acordo com as instruções de segurança da organização, essas instruções poderão exigir a alteração periódica da senha da conta. Quando a senha da conta expirar e você definir uma nova, as tarefas não serão iniciadas até que você especifique a nova senha válida nas propriedades da tarefa.

O Assistente para alterar a senha das tarefas permite substituir automaticamente a senha antiga pela nova em todas as tarefas em que a conta esteja especificada. Como alternativa, você pode alterar esta senha manualmente nas propriedades de cada tarefa.

Para iniciar o Assistente para alterar a senha das tarefas:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Gerenciar as credenciais de contas para iniciar tarefas**.

Siga as instruções do Assistente.

Etapa 1. Especificar as credenciais

Especifique novas credenciais atualmente válidas no seu sistema (por exemplo, no Active Directory). Quando você passa para a próxima etapa do Assistente, o Kaspersky Security Center verifica se o nome da conta especificado corresponde ao nome da conta nas propriedades de cada tarefa não local. Se os nomes das contas corresponderem, a senha nas propriedades da tarefa será automaticamente substituída pela nova.

Para especificar a nova conta, selecione uma opção:

- **Usar a conta atual**

  O Assistente usa o nome da conta na qual você está conectado atualmente ao Kaspersky Security Center Web Console. Em seguida, especifique manualmente a senha da conta no campo **Senha atual para usar em tarefas**.

- **Especificar uma conta diferente**

  Especifique o nome da conta na qual as tarefas devem ser iniciadas. Em seguida, especifique a senha da conta no campo **Senha atual para usar em tarefas**.

Se você preencher o campo **Senha anterior (opcional; caso você deseje substituí-la pela atual)**, o Kaspersky Security Center substitui a senha apenas para as tarefas nas quais o nome da conta e a senha antiga são encontrados. A substituição é realizada automaticamente. Em todos os outros casos, você precisa escolher uma ação a ser executada na próxima etapa do Assistente.

Etapa 2. Selecionar uma ação a ser executada

Se você não especificou a senha antiga na primeira etapa do Assistente ou a senha antiga especificada não correspondeu às senhas nas propriedades da tarefa, deverá escolher uma ação a ser executada para as tarefas encontradas.

Para escolher uma ação para uma tarefa:

1. Marque a caixa de seleção ao lado da tarefa para a qual deseja escolher uma ação.
2. Execute um dos seguintes procedimentos:

   - Para remover a senha nas propriedades da tarefa, clique em **Excluir as credenciais**.

     A tarefa é alternada para ser executada na conta padrão.

   - Para substituir a senha por uma nova, clique em **Impor alteração da senha mesmo se a senha antiga esteja incorreta ou não foi fornecida**.

   - Para cancelar a alteração da senha, clique em **Nenhuma ação está selecionada**.

As ações escolhidas são aplicadas depois que você passar para a próxima etapa do Assistente.

Etapa 3. Visualizar os resultados

Na última etapa do assistente, visualize os resultados para cada uma das tarefas encontradas. Para concluir o Assistente, pressione o botão **Concluir**.

Gerenciamento de dispositivos cliente

O Kaspersky Security Center permite a você gerenciar dispositivos clientes:

- Visualize as configurações e os status dos dispositivos gerenciados, incluindo clusters e matrizes de servidores.
- Configurar os pontos de distribuição.
- Gerenciar tarefas.

É possível usar grupos de administração para combinar dispositivos clientes em um conjunto que pode ser gerenciado como uma unidade única. Um dispositivo cliente pode ser incluído em apenas um grupo de administração. Os dispositivos podem ser alocados a um grupo automaticamente com base nas **Condições da regra**:

- Criar regras para mover dispositivos.
- Copiar regras para mover dispositivos.
- Condições de uma regra de migração de dispositivos.

É possível usar seleções de dispositivos para filtrar dispositivos com base em uma condição. Também é possível marcar dispositivos para criar seleções, localizar dispositivos e distribuir dispositivos entre grupos de administração.

Configurações de um dispositivo gerenciado

Para exibir as configurações de um dispositivo gerenciado:

1. Selecione **Dispositivos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo necessário.

A janela Propriedades do dispositivo selecionado é exibida.

As seguintes guias são exibidas na parte superior da janela de propriedades; elas representam os principais grupos de configurações:

- Geral

Esta guia compreende as seguintes seções:

- A seção **Geral** exibe as informações gerais sobre o dispositivo cliente. As informações são fornecidas com base nos dados recebidos durante a última sincronização do dispositivo cliente com o Servidor de Administração:

  - Nome

    Neste campo, você poderá visualizar e modificar o nome de um dispositivo cliente no grupo de administração.

  - Descrição

    Nesse campo, você poderá inserir uma descrição adicional de um dispositivo cliente.

  - Status do dispositivo

    Status do dispositivo cliente atribuído com base nos critérios definidos pelo administrador para o status de proteção antivírus no dispositivo e na atividade do dispositivo na rede.

  - Nome completo do grupo

    Grupo de administração que inclui o dispositivo cliente.

  - Última atualização da proteção

    Data em que os bancos de dados de antivírus ou os aplicativos foram atualizados pela última vez no dispositivo.

  - Conectado ao Servidor de Administração

    Data e hora da última vez que o Agente de Rede instalado no dispositivo cliente foi conectado ao Servidor de Administração.

  - Última visualização

    Data e hora de quando o dispositivo esteve por último visível na rede.

  - Versão do Agente de Rede

    Versão do Agente de Rede instalado.

  - Criação

    Data de criação do dispositivo no Kaspersky Security Center.

  - Proprietário do dispositivo

Nome do proprietário do dispositivo. É possível atribuir ou remover um usuário como proprietário de um dispositivo ao clicar no link **Gerenciar proprietário do dispositivo**.

- Não desconectar do Servidor de Administração

  Caso a opção seja ativada, será mantida uma conectividade contínua entre o dispositivo gerenciado e o Servidor de Administração. Convém usar a opção caso os servidores push, que fornecem a conectividade, não estejam sendo usados.

  Caso essa opção esteja desativada e os servidores push não estejam sendo utilizados, o dispositivo gerenciado somente se conectará ao Servidor de Administração para sincronizar dados ou transmitir informações.

  O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

  A opção é desativada por padrão em dispositivos gerenciados. A opção é ativada por padrão no dispositivo onde o Servidor de Administração está instalado e permanece ativada mesmo se você tentar desativá-la.

- A seção **Rede** exibe as seguintes informações sobre as propriedades da rede do dispositivo cliente:
  - Endereço IP

    Endereço IP do dispositivo.

  - Domínio do Windows

    O domínio do Windows ou o grupo de trabalho, que contém o dispositivo.

  - Nome DNS

    Nome do domínio DNS do dispositivo cliente.

  - Nome do NetBIOS

    Nome de rede Windows do dispositivo cliente.

  - **Endereço IPv6**

- A seção **Sistema** fornece informações sobre o sistema operacional instalado no dispositivo cliente:
  - **Sistema operacional**
  - **Arquitetura da CPU**
  - **Nome do dispositivo**
  - Tipo de máquina virtual

    O fabricante da máquina virtual.

- **Máquina virtual dinâmica como parte da VDI**

  Esta seta exibe se o dispositivo cliente é uma máquina virtual dinâmica como parte da VDI.

- A seção **Proteção** fornece as seguintes informações sobre o status atual da proteção antivírus no dispositivo cliente:

  - **Visível**

    O status da visibilidade do dispositivo cliente.

  - **Status do dispositivo**

    Status do dispositivo cliente atribuído com base nos critérios definidos pelo administrador para o status de proteção antivírus no dispositivo e na atividade do dispositivo na rede.

  - **Descrição de status**

    Status da proteção do dispositivo cliente e conexão com o Servidor de Administração.

  - **Status da proteção**

    Esse campo exibe o status atual da proteção em tempo real do dispositivo cliente.

    Quando o status é alterado no dispositivo, o novo status é exibido na janela de propriedades do dispositivo só depois que o dispositivo cliente é sincronizado com o Servidor de Administração.

  - **Última verificação completa**

    Data e hora em que a verificação de malwares foi executada por último no dispositivo cliente.

  - **Vírus detectado**

    Número total de ameaças detectadas no dispositivo cliente desde a instalação do aplicativo de segurança (primeira verificação) ou desde a última redefinição do contador de ameaças.

  - **Objetos com desinfecção mal-sucedida**

    Número de arquivos não processados no dispositivo cliente.

    Este campo ignora o número de arquivos não processados nos dispositivos móveis.

  - **Status de criptografia do disco**

    O status atual da criptografia do arquivo nas unidades locais do dispositivo. Para obter uma descrição dos status, consulte a Ajuda do Kaspersky Endpoint Security for Windows.

- A seção **Status do dispositivo definido pelo aplicativo** fornece informações sobre o status do dispositivo definido pelo aplicativo gerenciado e instalado no dispositivo. O status do dispositivo pode ser diferente do definido pelo Kaspersky Security Center.

- Aplicativos

  Essa guia lista todos os aplicativos da Kaspersky instalados no dispositivo cliente. Ela contém os botões **Iniciar** e **Parar**, que permitem iniciar e interromper o aplicativo da Kaspersky selecionado (excluindo o Agente de Rede). Você pode usar esses botões se a porta 15000 UDP estiver disponível no dispositivo gerenciado para notificações push do Servidor de Administração. Se o dispositivo gerenciado não estiver disponível para notificações push, mas o modo estiver configurado para manter uma conexão contínua com o Servidor de Administração (a opção **Não desconectar do Servidor de Administração** na seção **Geral** estiver ativada), os botões **Iniciar** e **Parar** ainda estarão disponíveis. Caso contrário, ao tentar iniciar ou interromper o aplicativo, uma mensagem de erro será exibida. É possível clicar no nome do aplicativo para visualizar informações gerais sobre ele, uma lista de eventos que ocorreram no dispositivo e as configurações do aplicativo.

- Políticas e perfis de política ativos

  Esta guia lista as políticas e perfis de políticas atualmente ativos no dispositivo gerenciado.

- Tarefas

  Na guia **Tarefas**, é possível gerenciar as tarefas do dispositivo cliente: visualizar a lista de tarefas existentes, criar novas, remover, iniciar e interromper tarefas, modificar as suas configurações e visualizar os resultados da execução. A lista de tarefas é fornecida com base nos dados recebidos durante a última sessão de sincronização do cliente com o Servidor de Administração. O Servidor de Administração solicita os detalhes do status de tarefa do dispositivo cliente. Se a porta 15000 UDP estiver disponível no dispositivo gerenciado para receber notificações push do Servidor de Administração, o status da tarefa será exibido e os botões para gerenciar a tarefa serão ativados. Se o dispositivo gerenciado não estiver disponível para notificações push, mas o modo estiver configurado para manter uma conexão contínua com o Servidor de Administração (a opção **Não desconectar do Servidor de Administração** na seção **Geral** estiver ativada), as ações com tarefas também estarão disponíveis.

  Se a conexão não é estabelecida, o status não é exibido e os botões são desabilitados.

- Eventos

  A guia **Eventos** exibe os eventos registrados no Servidor de Administração para o dispositivo cliente selecionado.

- Incidentes

  Na guia **Incidentes**, é possível visualizar, editar e criar incidentes para o dispositivo cliente. Os incidentes podem ser criados automaticamente, através de aplicativos da Kaspersky gerenciados instalados no dispositivo cliente, ou manualmente pelo administrador. Por exemplo, se alguns usuários moverem regularmente malware de suas unidades removíveis para os dispositivos, o administrador poderá criar um incidente. O administrador pode fornecer no texto do incidente uma breve descrição do caso e as ações recomendadas (como ações disciplinares a serem tomadas contra um usuário) e pode adicionar um link para o usuário ou os usuários.

  Um incidente no qual todas as ações necessárias tenham sido tomadas é chamado de *processado*. A presença de incidentes não processados pode ser escolhida como a condição para uma alteração do status do dispositivo para *Crítico* ou *Advertência*.

  Essa seção contém uma lista de incidentes que foram criados para o de dispositivo. Os incidentes são classificados por nível de gravidade e tipo. O tipo de um incidente é definido pelo aplicativo da Kaspersky que cria o incidente. Você pode destacar incidentes processados na lista selecionando a caixa de seleção na coluna **Processado**.

- Tags

  Na guia **Tags**, é possível gerenciar a lista de palavras-chave que são usadas para localizar os dispositivos cliente: visualizar a lista de tags existentes, atribuir tags a partir da lista, configurar regras de identificação automática, adicionar novas tags, renomear as antigas e excluir tags.

- Avançado

Esta guia compreende as seguintes seções:

- **Registro de aplicativos**. Nesta seção, é possível exibir o registro de aplicativos instalados no dispositivo clientes e suas atualizações, assim como configurar a exibição do registro de aplicativos.

  Informações sobre os aplicativos instalados são fornecidas se o Agente de Rede instalado no dispositivo cliente enviar as informações necessárias ao Servidor de Administração. Você pode configurar o envio de informações para o Servidor de Administração na janela Propriedades do Agente de Rede ou sua política, na seção **Repositórios**.

  Clicar no nome de um aplicativo abre uma janela que contém os detalhes do aplicativo e uma lista dos pacotes de atualização instalados para o aplicativo.

- **Arquivos executáveis**. Esta seção exibe os arquivos executáveis encontrados no dispositivo cliente.

- **Pontos de distribuição**. Esta seção fornece uma lista de pontos de distribuição com os quais o dispositivo interage.

  - Exportar para arquivo

    Clique no botão **Exportar para arquivo** para salvar a um arquivo de uma lista de pontos de distribuição com os quais o dispositivo interage. Por padrão, o aplicativo exporta a lista de dispositivos para um arquivo CSV.

  - Propriedades

    Clique no botão **Propriedades** para exibir e configurar o ponto de distribuição com o qual o dispositivo interage.

- **Registro de hardware**. Nesta seção, é possível visualizar as informações sobre o hardware instalado no dispositivo cliente.

- **Atualizações disponíveis**. Esta seção exibe uma lista de atualizações de software encontradas neste dispositivo, mas ainda não instaladas.

- **Vulnerabilidades de software**. Esta seção fornece informações sobre as vulnerabilidades de aplicativos de terceiros instalados nos dispositivos cliente.

  Para salvar as vulnerabilidades em um arquivo, marque as caixas de seleção ao lado das vulnerabilidades que deseja salvar e clique no botão **Exportar linhas para arquivo CSV** ou no botão **Exportar linhas para arquivo TXT**.

  Esta seção contém as seguintes configurações:

  - Exibir somente vulnerabilidades que podem ser corrigidas

    Se esta opção estiver ativada, a seção exibe vulnerabilidades que podem ser corrigidas usando um patch.

    Se essa opção estiver desativada, a seção exibe ambas as vulnerabilidades que podem ser corrigidas usando um patch, bem como as vulnerabilidades para as quais não foi lançado nenhum patch.

    Por padrão, esta opção está ativada.

  - Propriedades de vulnerabilidade

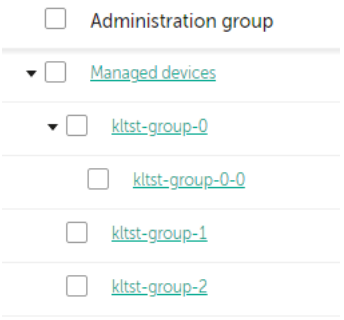
Clique no nome de uma vulnerabilidade de software na lista para visualizar as propriedades da vulnerabilidade de software selecionada em uma janela separada. Na janela, você pode fazer o seguinte:

- Ignore a vulnerabilidade de software neste dispositivo gerenciado (no Console de Administração ou no Kaspersky Security Center Web Console).
- Consulte a lista de correções recomendadas para a vulnerabilidade.
- Especifique manualmente as atualizações de software para corrigir a vulnerabilidade (no Console de Administração ou no Kaspersky Security Center Web Console).
- Exibir as instâncias de vulnerabilidade.
- Consulte a lista de tarefas existentes para corrigir a vulnerabilidade e crie novas tarefas para corrigir a vulnerabilidade.

- **Diagnóstico remoto**. Nesta seção, é possível executar o diagnóstico remoto de dispositivos clientes.

Criação de grupos de administração

Imediatamente após a instalação do Kaspersky Security Center, a hierarquia dos grupos de administração contém apenas um grupo de administração chamado **Dispositivos gerenciados**. Ao criar uma hierarquia de grupos de administração, você poderá adicionar dispositivos e máquinas virtuais ao grupo **Dispositivos gerenciados** e adicionar grupos aninhados (veja a figura abaixo).



Exibir hierarquia de grupos de administração

Para criar um grupo de administração:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Na estrutura do grupo de administração, selecione o grupo de administração que deve incluir o novo grupo de administração.
3. Clique no botão **Adicionar**.
4. Na janela **Nome do novo grupo de administração** que se abre, insira um nome para o grupo e clique no botão **Adicionar**.

Um novo grupo de administração com o nome especificado aparece na hierarquia dos grupos de administração.

O aplicativo permite criar a hierarquia dos grupos de administração com base na estrutura do Active Directory ou na estrutura de domínio da rede. Você também pode criar uma estrutura de grupos a partir de um arquivo de texto.

Para criar a estrutura de grupos de administração:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Clique no botão **Importar**.

   O Assistente de Nova Estrutura de Grupos de Administração é iniciado. Siga as instruções do Assistente.

Adicionar dispositivos manualmente a um grupo de administração

É possível mover dispositivos para grupos de administração automaticamente, criando regras de movimentação de dispositivos, ou manualmente, movendo dispositivos de um grupo de administração para outro, ou adicionando dispositivos a um grupo de administração selecionado. Esta seção descreve como adicionar dispositivos a um grupo de administração manualmente.

Para adicionar manualmente um ou mais dispositivos a um grupo de administração selecionado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no link **Caminho atual:** `<caminho atual>` acima da lista.
3. Na janela exibida, selecione o grupo de administração ao qual deseja adicionar os dispositivos.
4. Clique no botão **Adicionar dispositivos**.

   O Assistente para Mover Dispositivos é iniciado.

5. Faça uma lista dos dispositivos que deseja adicionar ao grupo de administração.

> Só é possível adicionar dispositivos para os quais informações já tenham sido adicionadas ao banco de dados do Servidor de Administração ao conectar o dispositivo ou após a descoberta de dispositivos.

Selecione como deseja adicionar dispositivos à lista:

- Clique no botão **Adicionar dispositivos** e especifique os dispositivos de uma das seguintes maneiras:
  - Selecione dispositivos na lista de dispositivos detectados pelo Servidor de Administração.
  - Especifique o endereço IP de um dispositivo ou um conjunto de IPs.
  - Especifique o nome NetBIOS ou o nome DNS de um dispositivo.

    > O campo do nome do dispositivo não deve conter caracteres de espaço e nem os seguintes caracteres: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

- Clique no botão **Importar dispositivos do arquivo** para importar uma lista de dispositivos a partir de um arquivo .txt. Cada endereço ou nome de dispositivo deve ser especificado em uma linha separada.

  > O arquivo não deve conter caracteres de espaços e nem os seguintes caracteres: \ / * ; : ` ~ ! @ # $ ^ & ( ) = + [ ] { } | , < > %

6. Veja a lista de dispositivos a serem adicionados ao grupo de administração. É possível editar a lista adicionando ou removendo dispositivos.

7. Depois de garantir que a lista esteja correta, clique no botão **Avançar**.

O assistente processa a lista de dispositivos e exibe o resultado. Os dispositivos processados com sucesso são adicionados ao grupo de administração e exibidos na lista de dispositivos sob nomes gerados pelo Servidor de Administração.

Migrando dispositivos manualmente para um grupo de administração

Você pode mover dispositivos de um grupo de administração para outro ou do grupo de dispositivos não atribuídos para um grupo de administração.

Para migrar um ou diversos dispositivos em um grupo de administração selecionado:

1. Abra o grupo de administração do qual você deseja migrar os dispositivos. Para fazer isso, execute um dos seguintes procedimentos:

   - Para abrir um grupo de administração, no menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**, clique no link do caminho no campo **Caminho atual** e selecione um grupo de administração no painel aberto do lado esquerdo.

   - Para abrir o grupo **Dispositivos não atribuídos**, no menu principal, vá para **Descoberta e implementação** → **Dispositivos não atribuídos**.

2. Marque a caixa de seleção ao lado dos dispositivos que deseja migrar para um grupo diferente.

3. Clique no botão **Migrar para grupo**.

4. Na hierarquia de grupos de administração, marque a caixa de seleção ao lado do grupo de administração para o qual deseja migrar os dispositivos selecionados.

5. Clique no botão **Migrar**.

Os dispositivos selecionados são movidos para o grupo de administração selecionado.

Criar regras para mover dispositivos

É possível configurar as regras de migração de dispositivos, ou seja, as regras que alocam automaticamente os dispositivos para grupos de administração.

Para criar uma regra para mover dispositivos:

1. No menu principal, vá para **Dispositivos** → **Regras de migração**.

2. Clique em **Adicionar**.

3. Na janela exibida, especifique as seguintes informações na guia **Geral**:

- Nome da regra

  Digite um nome para a nova regra.

  Se estiver copiando uma regra, a nova regra adquirirá o mesmo nome da regra de origem, mas um índice no formato () será adicionado ao nome, por exemplo: (1).

- Grupo de administração

  Selecione o grupo de administração para o qual os dispositivos devem ser movidos automaticamente.

- Aplicar regra

  Você pode selecionar uma das seguintes opções:

  - **Executar uma vez para cada dispositivo**

    A regra é aplicada uma vez para cada dispositivo que atenda aos critérios.

  - **Executar uma vez para cada dispositivo e depois em cada reinstalação do Agente de Rede**

    A regra é aplicada uma vez para cada dispositivo que atende aos critérios e apenas quando o Agente de Rede é reinstalado nesses dispositivos.

  - **Aplicar regra continuamente**

    A regra é aplicada de acordo com o agendamento que o Servidor de Administração configura automaticamente (normalmente a cada várias horas).

- Somente migrar os dispositivos que não pertencem a um grupo de administração

  Se esta opção estiver ativada, somente os dispositivos não atribuídos serão movidos para o grupo selecionado.

  Se esta opção estiver desativada, os dispositivos que já pertencem a outros grupos de administração, bem como os dispositivos não atribuídos, serão movidos para o grupo selecionado.

- Ativar regra

  Se esta opção estiver ativada, a regra será ativada e começará a funcionar após ser salva.

  Se esta opção estiver desativada, a regra será criada, mas não ativada. Ela não funcionará até que você ative esta opção.

4. Na guia **Condições da regra**, especifique pelo menos um critério pelo qual os dispositivos são movidos para um grupo de administração.

5. Clique em **Salvar**.

A regra de movimentação é criada. Ela é exibida na lista de regras de movimento.

Quanto mais elevada a posição na lista, maior a prioridade da regra. Para aumentar ou diminuir a prioridade de uma regra em movimento, mova a regra para cima ou para baixo na lista, respectivamente, usando o mouse.

Se a opção **Aplicar regra continuamente** estiver selecionada, a regra de migração será aplicada independentemente das configurações de prioridade. Essas regras são aplicadas de acordo com o agendamento que o Servidor de Administração configura automaticamente.

Se os atributos do dispositivo atenderem as condições de múltiplas regras, o dispositivo é movido para o grupo alvo da regra com a prioridade mais alta (ou seja, ele tem a classificação mais alta na lista de regras).

Copiar as regras para mover dispositivos

Você poderá copiar regras de movimento, por exemplo, se quiser ter várias regras idênticas para grupos de administração de destino diferentes.

Para copiar uma regra de movimentação existente:

1. Execute uma das seguintes ações:

   - No menu principal, vá para **Dispositivos** → **Regras de migração**.
   - No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Regras de migração**.

   A lista de regras de movimento é exibida.

2. Marque a caixa de seleção ao lado da regra que deseja copiar.
3. Clique em **Copiar**.

4. Na janela que se abre, modifique as seguintes informações na guia **Geral** ou não faça nenhuma modificação se você só quiser copiar a regra sem modificar as suas configurações:

   - Nome da regra

     Digite um nome para a nova regra.

     Se estiver copiando uma regra, a nova regra adquirirá o mesmo nome da regra de origem, mas um índice no formato () será adicionado ao nome, por exemplo: (1).

   - Grupo de administração

     Selecione o grupo de administração para o qual os dispositivos devem ser movidos automaticamente.

   - Aplicar regra

     Você pode selecionar uma das seguintes opções:

     - **Executar uma vez para cada dispositivo**

       A regra é aplicada uma vez para cada dispositivo que atenda aos critérios.

     - **Executar uma vez para cada dispositivo e depois em cada reinstalação do Agente de Rede**

       A regra é aplicada uma vez para cada dispositivo que atende aos critérios e apenas quando o Agente de Rede é reinstalado nesses dispositivos.

     - **Aplicar regra continuamente**

       A regra é aplicada de acordo com o agendamento que o Servidor de Administração configura automaticamente (normalmente a cada várias horas).

   - Somente migrar os dispositivos que não pertencem a um grupo de administração

     Se esta opção estiver ativada, somente os dispositivos não atribuídos serão movidos para o grupo selecionado.

     Se esta opção estiver desativada, os dispositivos que já pertencem a outros grupos de administração, bem como os dispositivos não atribuídos, serão movidos para o grupo selecionado.

   - Ativar regra

     Se esta opção estiver ativada, a regra será ativada e começará a funcionar após ser salva.

     Se esta opção estiver desativada, a regra será criada, mas não ativada. Ela não funcionará até que você ative esta opção.

5. Na guia **Condições da regra**, especifique pelo menos um critério para os dispositivos que deseja serem movidos automaticamente.

6. Clique em **Salvar**.

A nova regra de movimentação é criada. Ela é exibida na lista de regras de movimento.

Condições para migrar uma regra de um dispositivo

Ao criar ou copiar uma regra para migrar dispositivos cliente para grupos de administração, na guia **Condições da regra**, as condições para migrar os dispositivos serão definidas. Para determinar quais dispositivos migrar, será necessário usar os seguintes critérios:

- Tags atribuídas a dispositivos clientes.
- Parâmetros de rede. Por exemplo, é possível migrar os dispositivos com os endereços IP a partir de um intervalo especificado.
- Aplicativos gerenciados e instalados em dispositivos clientes, por exemplo, o Agente de Rede ou o Servidor de Administração.
- Máquinas virtuais, que são os dispositivos clientes.
- Informações sobre a unidade organizacional (OU) do Active Directory com os dispositivos clientes.
- Informações sobre um segmento da nuvem com os dispositivos clientes.

Abaixo, é possível encontrar a descrição sobre a especificação dessas informações em uma regra de movimentação de dispositivos.

Caso especifique várias condições na regra, o operador lógico AND funcionará e todas as condições serão aplicadas ao mesmo tempo. Caso não selecione nenhuma opção ou alguns campos sejam deixados em branco, essas condições não serão aplicadas.

Guia Tags

Nesta guia, é possível configurar uma regra de migração de dispositivo de acordo com as tags de dispositivo adicionadas anteriormente nas descrições dos dispositivos clientes. Para fazer isso, selecione as tags necessárias. Além disso, é possível ativar as seguintes opções:

- **Aplicar aos dispositivos sem tags especificadas**

  Caso esta opção esteja habilitada, todos os dispositivos com as tags especificadas serão excluídos de uma regra de migração de dispositivos. Caso esta opção esteja desabilitada, a regra de migração de dispositivo será aplicável aos dispositivos com todas as tags selecionadas.

  Por padrão, esta opção está desativada.

- **Aplicar se pelo menos uma tag especificada corresponder**

  Caso esta opção esteja habilitada, uma regra de migração de dispositivo será aplicável aos dispositivos clientes com pelo menos uma das tags selecionadas. Caso esta opção esteja desabilitada, a regra de migração de dispositivo será aplicável aos dispositivos com todas as tags selecionadas.

  Por padrão, esta opção está desativada.

Guia Rede

Nesta guia, é possível especificar os dados de rede dos dispositivos que uma regra de migração de dispositivo considera:

- **Nome do dispositivo na rede Windows**

  Nome da rede Windows (nome NetBIOS) do dispositivo ou o endereço IPv4 ou IPv6.

- **Domínio do Windows**

  Uma regra de migração de dispositivo será aplicável a todos os dispositivos incluídos no domínio do Windows especificado.

- **Nome de DNS do dispositivo**

  Nome do domínio DNS do dispositivo cliente que deseja migrar. Preencha este campo se sua rede incluir um servidor DNS.

  Caso o agrupamento com distinção entre maiúsculas e minúsculas seja definido para o banco de dados usado para o Kaspersky Security Center, mantenha maiúsculas e minúsculas ao especificar um nome DNS de dispositivo. Caso contrário, a regra de movimentação do dispositivo não funcionará.

- **Domínio DNS**

  Uma regra de migração de dispositivo será aplicável a todos os dispositivos incluídos no sufixo DNS principal especificado. Preencha este campo se sua rede incluir um servidor DNS.

- **Intervalo IP**

  Se esta opção estiver ativada, você poderá inserir os endereços IP inicial e final do conjunto de IPs no qual os dispositivos relevantes devem ser incluídos.

  Por padrão, esta opção está desativada.

- **Endereço IP para conexão com o Servidor de Administração**

  Caso esta opção esteja habilitada, será possível definir os endereços IP pelos quais os dispositivos clientes serão conectados ao Servidor de Administração. Para fazer isso, especifique o intervalo de IP que inclui todos os endereços IP necessários.

  Por padrão, esta opção está desativada.

- O dispositivo está no intervalo IP

  Se esta opção estiver habilitada, você poderá selecionar um intervalo de IP que você adicionou anteriormente na seção **Intervalos de IPs**. Os dispositivos relevantes devem ser incluídos no intervalo de IPS selecionado.

  Por padrão, esta opção está desativada.

- Perfil de conexão alterado

  Selecione um dos seguintes valores:

  - **Sim**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente com um perfil de conexão alterado.
  - **Não**. A regra de movimentação de dispositivos se aplica apenas aos dispositivos clientes cujo perfil de conexão não foi alterado.
  - **Nenhum valor está selecionado**. A condição não se aplica.

- Gerenciado por outro Servidor de Administração

  Selecione um dos seguintes valores:

  - **Sim**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente gerenciados por outros Servidores de Administração. Esses servidores são diferentes do servidor no qual a regra de migração de dispositivo é configurada.
  - **Não**. A regra de movimentação de dispositivos aplica-se apenas a dispositivos clientes gerenciados pelo Servidor de Administração atual.
  - **Nenhum valor está selecionado**. A condição não se aplica.

Guia Aplicativos

Nesta guia, é possível configurar uma regra de migração de dispositivo de acordo com os aplicativos gerenciados e sistemas operacionais instalados nos dispositivos cliente:

- **Agente de Rede instalado**

  Selecione um dos seguintes valores:

  - **Sim**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente com o Agente de Rede instalado.
  - **Não**. A regra de movimentação de dispositivos se aplica apenas a dispositivos clientes nos quais o Agente de Rede não está instalado.
  - **Nenhum valor está selecionado**. A condição não se aplica.

- **Aplicativos**

  Especifique quais aplicativos gerenciados devem ser instalados em dispositivos cliente para que uma regra de migração de dispositivo seja aplicável a esses dispositivos. Por exemplo, é possível selecionar **Agente de Rede do Kaspersky Security Center 14.2** ou **Servidor de Administração do Kaspersky Security Center 14.2**.

  Caso nenhum aplicativo gerenciado seja selecionado, a condição não será aplicável.

- **Versão do sistema operacional**

  É possível selecionar os dispositivos cliente de acordo com a versão do sistema operacional. Para isso, especifique os sistemas operacionais que devem ser instalados nos dispositivos cliente. Assim, uma regra de migração de dispositivo será aplicável aos dispositivos cliente com os sistemas operacionais selecionados.

  Caso esta opção não seja habilitada, a condição não será aplicável. Por padrão, a opção está desativada.

- Tipo de bit do sistema operacional

  É possível selecionar os dispositivos cliente pelos tamanhos de bits do sistema operacional. No campo **Tipo de bit do sistema operacional**, será possível selecionar um dos seguintes valores:

  - **Desconhecido**
  - **x86**
  - **AMD64**
  - **IA64**

  Para verificar o tamanho de bits do sistema operacional dos dispositivos cliente:

  1. No menu principal, acesse a seção **Dispositivos** → **Dispositivos gerenciados**.
  2. Clique no botão **Configurações de colunas** ( ) à direita.
  3. Selecione a opção **Tipo de bit do sistema operacional** e clique no botão **Salvar**.

     Depois disso, o tamanho do bit do sistema operacional será exibido para cada dispositivo gerenciado.

- Versão do service pack do sistema operacional

  Neste campo, você pode especificar a versão do pacote do sistema operacional (no formato *X.Y*), o que determinará como a regra de migração será aplicada ao dispositivo. Por padrão, nenhum valor de versão é especificado.

- Certificado do usuário

  Selecione um dos seguintes valores:

  - **Instalado**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos móveis com um certificado móvel.
  - **Não instalado**. A regra de migração de dispositivo se aplicável apenas aos dispositivos móveis sem um certificado móvel.
  - **Nenhum valor está selecionado**. A condição não se aplica.

- Compilação do sistema operacional

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  Você pode especificar se o sistema operacional selecionado deve ter um número de compilação igual, anterior ou posterior. Também é possível configurar a regra de migração de dispositivo para todos os números de compilação, exceto o especificado.

- Número da versão do sistema operacional

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  É possível especificar se o sistema operacional selecionado ter um número de versão igual, anterior ou posterior. Também é possível configurar uma regras de migração de dispositivo para todos os números de versão, exceto o especificado.

Guia Máquinas virtuais

Na guia, é possível configurar a migração de dispositivo de acordo com o fato de que os dispositivos cliente sejam máquinas virtuais ou parte da Virtual Desktop Infrastructure (VDI):

- Esta é uma máquina virtual

  Na lista suspensa, é possível selecionar os seguintes itens:
  - **N/A**. A condição não se aplica.
  - **Não**. Mover dispositivos que não sejam máquinas virtuais.
  - **Sim**. Migrar dispositivos que sejam máquinas virtuais.

- **Tipo de máquina virtual**

- Parte da Virtual Desktop Infrastructure

  Na lista suspensa, é possível selecionar os seguintes itens:
  - **N/A**. A condição não se aplica.
  - **Não**. Mover dispositivos que não fazem parte do VDI.
  - **Sim**. Migre os dispositivos que fazem parte da VDI.

Guia Active Directory

Nesta guia, você pode especificar que é necessário mover os dispositivos incluídos na OU do Active Directory. Também é possível mover os dispositivos de todas as OUs filhas da OU do Active Directory:

- **O dispositivo está em uma unidade organizacional do Active Directory**

  Se esta opção estiver ativada, a regra de migração de dispositivos será aplicada aos dispositivos da unidade organizacional do Active Directory especificada na lista sob a opção.

  Por padrão, esta opção está desativada.

- **Incluir unidades organizacionais secundárias**

  Caso esta opção esteja ativada, a seleção incluirá os dispositivos das unidades de organização secundárias da unidade organizacional do Active Directory especificada.

  Por padrão, esta opção está desativada.

- **Migrar dispositivos de unidades secundárias para os subgrupos correspondentes**
- **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente**
- **Excluir subgrupos não presentes no Active Directory**
- **Este dispositivo é membro de um grupo do Active Directory**

  Se esta opção estiver ativada, a regra de migração de dispositivos será aplicada aos dispositivos do grupo do Active Directory especificado na lista sob a opção.

  Por padrão, esta opção está desativada.

Guia Segmentos da nuvem

Nesta guia, você pode especificar que é necessário mover os dispositivos que pertencem a segmentos da nuvem específicos:

- **O dispositivo está no segmento da nuvem**

  Se você selecionar esta opção, a regra de migração de dispositivos será aplicada aos dispositivos clientes que pertencem a um segmento da nuvem. Você pode selecionar o segmento da nuvem necessário até uma sub-rede na lista sob a opção.

  Por padrão, a opção está desativada.

- **Incluir objetos secundários**

  Se você selecionar esta opção, a regra de migração de dispositivos será aplicada não apenas ao segmento da nuvem selecionado, mas também aos objetos filho deste segmento.

  Por padrão, a opção está desativada.

- **Migrar dispositivos de objetos aninhados para os subgrupos correspondentes**

- **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente**
- **Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem**
- **Dispositivo detectado usando a API**

  Na lista suspensa, você pode selecionar se um dispositivo é detectado pelas ferramentas API:
  - **AWS**. O dispositivo é detectado usando a AWS API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do AWS.
  - **Azure**. O dispositivo é detectado usando a Azure API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do Azure.
  - **Google Cloud.** O dispositivo é descoberto usando a Google API, ou seja, o dispositivo está definitivamente no ambiente em nuvem do Google.
  - **Não**. O dispositivo não pode ser detectado usando API do AWS, Azure ou Google, ou seja, está fora do ambiente em nuvem ou está no ambiente em nuvem, mas não pode ser detectado usando uma API.
  - **Nenhum valor**. Esta condição não se aplica.

Exibir e configurar as ações quando os dispositivos mostram inatividade

Se os dispositivos clientes em um grupo estiverem inativos, você poderá receber notificações sobre isso. Você também pode excluir automaticamente esses dispositivos.

Para exibir ou configurar as ações quando os dispositivos no grupo mostrarem inatividade:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Clique no nome do grupo de administração necessário.

   A janela Propriedades do grupo de administração é aberta.
3. Na janela Propriedades, siga para a guia **Configurações**.

4. Na seção **Herança**, ative ou desative as seguintes opções:

- Herdar do grupo principal

  As configurações desta seção serão herdadas do grupo principal no qual o dispositivo cliente está incluído. Se esta opção estiver ativada, as configurações sob **Atividade de dispositivos na rede** serão bloqueadas contra quaisquer alterações.

  Esta opção está disponível somente se o grupo de administração tiver um grupo principal.

  Por padrão, esta opção está ativada.

- Forçar herança de configurações nos grupos secundários

  Os valores de configuração serão distribuídos aos grupos secundários, mas essas configurações são bloqueadas nas propriedades dos grupos secundários.

  Por padrão, esta opção está desativada.

5. Na seção **Atividade de dispositivos**, ative ou desative as seguintes opções:

- Notificar o administrador se o dispositivo estiver inativo por mais de (dias)

  Se esta opção estiver ativada, o administrador receberá notificações sobre os dispositivos inativos. Você pode especificar o intervalo de tempo após o qual o evento **O dispositivo permaneceu inativo na rede por muito tempo** será criado. O intervalo de tempo predefinido é de 7 dias.

  Por padrão, esta opção está ativada.

- Remover o dispositivo do grupo se estiver inativo por mais de (dias)

  Se esta opção estiver selecionada, você poderá especificar o intervalo de tempo após o qual o dispositivo será automaticamente removido do grupo. O intervalo de tempo predefinido é de 60 dias.

  Por padrão, esta opção está ativada.

6. Clique em **Salvar**.

As suas alterações serão salvas e aplicadas.

Sobre os status do dispositivo

O Kaspersky Security Center atribui um status a cada dispositivo gerenciado. O status específico depende se as condições definidas pelo usuário são atendidas. Em alguns casos, ao atribuir um status a um dispositivo, o Kaspersky Security Center leva em consideração o sinalizador de visibilidade do dispositivo na rede (consulte a tabela abaixo). Se o Kaspersky Security Center não encontrar um dispositivo na rede dentro de duas horas, o sinalizador de visibilidade do dispositivo será definido como *Não visível*.

Os status são os seguintes:

- *Crítico* ou *Crítico/Visível*
- *Advertência* ou *Advertência/Visível*
- *OK* ou *OK/Visível*

A tabela abaixo lista as condições padrão que devem ser atendidas para atribuir o status *Crítico* ou *Advertência* a um dispositivo, com todos os valores possíveis.

Condições para atribuir um status a um dispositivo

Condição	Descrição da condição	Valores disponíveis
O aplicativo de segurança não está instalado	O Agente de Rede é instalado no dispositivo, mas um aplicativo de segurança não é instalado.	• O botão de alternar é ativado. • O botão de alternar é desativado.
Excesso de vírus detectados	Alguns vírus foram encontrados no dispositivo por uma tarefa de detecção de vírus, por exemplo, a tarefa de *verificação de malwares*, e o número de vírus encontrados excede o valor especificado.	Mais de 0.
O nível da proteção em tempo real é diferente do nível definido pelo administrador	O dispositivo está visível na rede, mas o nível de proteção em tempo real difere do nível definido (na condição) pelo administrador para o status do dispositivo.	• Parado. • Pausada. • Executando.
A verificação de vírus não é executada há muito tempo	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas nem a tarefa de *verificação de malware* nem a verificação local foram executadas dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 7 dias ou antes.	Mais de 1 dia.
Os bancos de dados estão desatualizados	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas os bancos de dados antivírus não foram atualizados neste dispositivo dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 1 dia ou antes.	Mais de 1 dia.
Não conectado há muito tempo	O Agente de Rede está instalado no dispositivo, mas o dispositivo não se conectou a um Servidor de Administração dentro do intervalo de tempo especificado, porque o dispositivo estava desativado.	Mais de 1 dia.
Foram detectadas ameaças ativas	O número de objetos não processados na pasta **Ameaças ativas** excede o valor especificado.	Mais de 0 itens.
A reinicialização é necessária	O dispositivo está visível na rede, mas um aplicativo requer o reinício do dispositivo por mais tempo do que o intervalo de tempo especificado e para um dos motivos selecionados.	Mais de 0 minuto.
Aplicativos incompatíveis estão instalados	O dispositivo está visível na rede, mas o inventário de software executado pelo Agente de Rede detectou aplicativos incompatíveis instalados no dispositivo.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Foram detectadas vulnerabilidades de software	O dispositivo está visível na rede, e o Agente de Rede está instalado no dispositivo, mas a tarefa *Encontrar vulnerabilidades e atualizações necessárias* detectou vulnerabilidades com o nível de gravidade especificado nos aplicativos instalados no dispositivo.	• Crítico. • Alto. • Médio. • Ignorar se a vulnerabilidade não puder ser corrigida. • Ignorar se uma atualização for atribuída para instalação.
A licença expirou	O dispositivo está visível na rede, mas a licença expirou.	• O botão de alternar é desativado. • O botão de alternar é ativado.

Condição	Descrição da condição	Valores disponíveis
A licença expira em breve	O dispositivo está visível na rede, mas a licença expirará no dispositivo em tempo menor que o número especificado de dias.	Valor de dias inferior a 0.
A verificação de atualizações do Windows Update não é executada há muito tempo	O dispositivo está visível na rede, mas a tarefa *executar a sincronização com o Windows Update* não foi executada dentro do intervalo de tempo especificado.	Mais de 1 dia.
Status de criptografia inválido	O Agente de Rede está instalado no dispositivo, mas o resultado da criptografia de dispositivo é igual ao valor especificado.	• Não está em conformidade com a política devido à recusa do usuário (somente para dispositivos externos). • Não está em conformidade com a política devido a um erro. • Reiniciar é necessário ao aplicar a política. • Nenhuma política de criptografia está especificada. • Sem suporte. • Ao aplicar a política.
As configurações do dispositivo móvel não estão em conformidade com a política	As configurações do dispositivo móvel são diferentes das especificadas na política do Kaspersky Endpoint Security for Android durante a verificação das regras de conformidade.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Incidentes não processados detectados	Alguns incidentes não processados foram encontrados no dispositivo. Os incidentes podem ser criados automaticamente, através de aplicativos da Kaspersky gerenciados instalados no dispositivo cliente, ou manualmente pelo administrador.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Status do dispositivo definido pelo aplicativo	O status do dispositivo é definido pelo aplicativo gerenciado.	• O botão de alternar é desativado. • O botão de alternar é ativado.
O dispositivo está com espaço em disco insuficiente	O espaço livre em disco no dispositivo é menor do que o valor especificado ou o dispositivo não pôde ser sincronizado com o Servidor de Administração. O status *Crítico* ou *Advertência* é alterado para o status *OK* quando o dispositivo é sincronizado com sucesso com o Servidor de Administração, e o espaço livre no dispositivo é maior que ou igual ao valor especificado.	Mais de 0 MB.
O dispositivo está sem gerenciamento	Durante a descoberta de dispositivos, o dispositivo foi reconhecido como visível na rede, mas houve falha em mais de três tentativas de sincronizar com o Servidor de Administração.	• O botão de alternar é desativado. • O botão de alternar é ativado.
A proteção está desativada	O dispositivo é visível na rede, mas o aplicativo de segurança no dispositivo foi desativado por um tempo mais longo do que o intervalo de tempo especificado. Nesse caso, o estado do aplicativo de segurança é *interrompido* ou *com falha* e diferente de: *iniciando*, *em execução* ou *suspenso*.	Mais de 0 minuto.
O aplicativo de segurança não está em execução	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas não está em execução.	• O botão de alternar é desativado. • O botão de alternar é ativado.

O Kaspersky Security Center lhe permite definir a troca automática do status de um dispositivo em um grupo de administração quando as condições especificadas forem atendida. Quando as condições especificadas forem atendidas, ao dispositivo cliente é atribuído um dos seguintes status: *Crítico* ou *Aviso*. Quando as condições especificadas não são atendidas, o dispositivo cliente recebe o status *OK*.

Diferentes status poderão corresponder a diferentes valores de uma condição. Por exemplo, se por padrão a condição **Os bancos de dados estão desatualizados** possuir o valor **Mais de 3 dias**, o dispositivo cliente recebe o status *Advertência*. Se o valor for **Mais de 7 dias**, é atribuído o status *Crítico*.

Se você atualizar o Kaspersky Security Center da versão anterior, os valores do **Os bancos de dados estão desatualizados** condição para atribuir o status *Crítico* ou *Advertência* não mudam.

Quando o Kaspersky Security Center atribui um status a um dispositivo, para algumas condições (consulte a coluna Descrição da condição), o sinalizador de visibilidade é levado em consideração. Por exemplo, se um dispositivo gerenciado recebeu o status *Crítico* porque a condição Os bancos de dados estão desatualizados foi atendida e, mais tarde, o sinalizador de visibilidade foi definido para o dispositivo, então o dispositivo recebe o status *OK*.

Configurar a alternância dos status do dispositivo

Você pode alterar as condições para atribuir o status *Crítico* ou *Advertência* para um dispositivo.

Para ativar a alteração do status do dispositivo para Crítico:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Crítico**.
5. No painel direito, na seção **Se especificados, definir como Crítico**, ative a condição para alterar o status de um dispositivo para *Crítico*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.

9. Clique em **OK**.

Quando condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Crítico*.

Para ativar a alteração do status do dispositivo para Advertência:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Advertência**.

5. No painel direito, na seção **Se especificados, definir como Advertência**, ative a condição para alterar o status de um dispositivo para *Advertência*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.

9. Clique em **OK**.

Quando as condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Advertência*.

Conexão remota à Área de trabalho de um dispositivo cliente

O administrador pode obter o acesso remoto à área de trabalho de um dispositivo cliente através de um Agente de Rede instalado no dispositivo. A conexão remota a um dispositivo por meio do Agente de Rede é possível mesmo que as portas TCP e UDP do dispositivo cliente estejam fechadas.

Ao estabelecer a conexão com o dispositivo, o administrador obtém o acesso completo às informações armazenadas nesse dispositivo, para que possa gerenciar os aplicativos nele instalados.

A conexão remota deve ser permitida nas configurações do sistema operacional do dispositivo gerenciado de destino. Por exemplo, no Windows 10, essa opção é chamada **Permitir conexões de Assistência Remota para este computador** (é possível encontrar essa opção em **Painel de controle** → **Sistema e Segurança** → **Sistema** → **Configurações remotas**). Caso tenha uma licença para o recurso de Gerenciamento de patches e vulnerabilidades, será possível ativar a opção à força ao estabelecer a conexão com um dispositivo gerenciado. Caso não tenha a licença, ative essa opção localmente no dispositivo gerenciado de destino. Se esta opção estiver desativada, a conexão remota não é possível.

Para estabelecer uma conexão remota com um dispositivo, você deve ter dois utilitários:

- Utilitário Kaspersky chamado klsctunnel. Este utilitário deve ser armazenado na estação de trabalho do administrador. Este utilitário é usado para encapsular a conexão entre um dispositivo cliente e o Servidor de Administração.

  O Kaspersky Security Center permite o tunelamento de conexões de TCP, do Console de Administração via Servidor de Administração, e então via Agente de Rede a uma porta especificada em um dispositivo gerenciado. O tunelamento é projetado para conectar um aplicativo cliente em um dispositivo com o Console de Administração instalado à uma porta TCP em um dispositivo gerenciado – se nenhuma conexão direta for possível entre o Console de Administração e o dispositivo alvo.

  A conexão em túnel entre um dispositivo cliente remoto e Servidor de Administração é necessária se a porta usada para a conexão ao Servidor de Administração não estiver disponível no dispositivo. A porta no dispositivo poderá estar indisponível nos seguintes casos:

  - O dispositivo remoto é conectado à uma rede local que usa o mecanismo NAT.
  - Um dispositivo remoto é parte da rede local, do Servidor de Administração, mas sua porta está fechada por um firewall.

- Componente padrão do Microsoft Windows denominado Conexão de Área de Trabalho Remota. A conexão com uma área de trabalho remota é estabelecida através do utilitário Windows padrão mstsc.exe, de acordo com as configurações do utilitário.

  A conexão com a sessão de área de trabalho remota atual do usuário é estabelecida sem o conhecimento do usuário. Após o administrador se conectar com a sessão, o usuário do dispositivo será desconectado da sessão sem uma notificação antecipada.

Para se conectar à Área de trabalho de um dispositivo cliente:

1. No Console de Administração baseado em MMC, no menu de contexto do Servidor de Administração, selecione **Propriedades**.
2. Na janela de propriedades do Servidor de Administração que é exibida, vá para **Configurações de conexão do Servidor de Administração → Portas de conexão**.
3. Verifique se a opção **Abrir porta RDP para o Kaspersky Security Center Web Console** está ativada.
4. No Kaspersky Security Center Web Console, vá para **Dispositivos → Dispositivos gerenciados**.
5. No campo **Caminho atual**, acima da lista de dispositivos gerenciados, clique no link do caminho.
6. No painel aberto do lado esquerdo, selecione o grupo de administração que contém o dispositivo ao qual deseja obter acesso.
7. Marque a caixa de seleção ao lado do nome do dispositivo ao qual deseja obter acesso.
8. Clique no botão **Conectar-se à área de trabalho remota**.

   A janela Desktop remoto (somente Windows) se abre.

9. Ative a opção **Permitir conexão de área de trabalho remota no dispositivo gerenciado**. Nesse caso, a conexão será estabelecida mesmo se conexões remotas estiverem proibidas no momento nas configurações do sistema operacional no dispositivo gerenciado.

   Essa opção estará disponível apenas se você tiver uma licença para o recurso Gerenciamento de patches e vulnerabilidades.

10. Clique no botão **Baixar** para baixar o utilitário klsctunnel.

11. Clique no botão **Copiar para transferência** para copiar o texto do campo de texto. Este texto é um objeto de dados binário (BLOB) que contém as configurações necessárias para estabelecer a conexão entre o Servidor de Administração e o dispositivo gerenciado.

    Um BLOB é válido por 3 minutos. Se ele expirou, reabra a janela Desktop remoto (somente Windows) para gerar um novo BLOB.

12. Execute o utilitário klsctunnel.

    A janela do utilitário é exibida.

13. Cole o texto copiado no campo de texto.

14. Se você usa um servidor proxy, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão do servidor proxy.

15. Clique no botão **Abrir porta**.

    A janela de login da Conexão de Área de Trabalho Remota é aberta.

16. Especifique as credenciais da conta na qual você está atualmente conectado ao Kaspersky Security Center Web Console.

17. Clique no botão **Conectar**.

Quando a conexão com o dispositivo for estabelecida, a área de trabalho ficará disponível na janela Conexão remota do Microsoft Windows.

Conexão com dispositivos cliente através do Windows Desktop Sharing

O administrador pode obter o acesso remoto à área de trabalho de um dispositivo cliente através de um Agente de Rede instalado no dispositivo. A conexão remota a um dispositivo por meio do Agente de Rede é possível mesmo que as portas TCP e UDP do dispositivo cliente estejam fechadas.

O administrador pode conectar-se a uma sessão existente em um dispositivo cliente sem desconectar o usuário a sessão. Nesse caso, o administrador e o usuário da sessão no dispositivo compartilham o acesso à área de trabalho.

Para estabelecer uma conexão remota com um dispositivo, você deve ter dois utilitários:

- Utilitário Kaspersky chamado klsctunnel. Este utilitário deve ser armazenado na estação de trabalho do administrador. Este utilitário é usado para encapsular a conexão entre um dispositivo cliente e o Servidor de Administração.

  O Kaspersky Security Center permite o tunelamento de conexões de TCP, do Console de Administração via Servidor de Administração, e então via Agente de Rede a uma porta especificada em um dispositivo gerenciado. O tunelamento é projetado para conectar um aplicativo cliente em um dispositivo com o Console de Administração instalado à uma porta TCP em um dispositivo gerenciado – se nenhuma conexão direta for possível entre o Console de Administração e o dispositivo alvo.

  A conexão em túnel entre um dispositivo cliente remoto e Servidor de Administração é necessária se a porta usada para a conexão ao Servidor de Administração não estiver disponível no dispositivo. A porta no dispositivo poderá estar indisponível nos seguintes casos:

  - O dispositivo remoto é conectado à uma rede local que usa o mecanismo NAT.
  - Um dispositivo remoto é parte da rede local, do Servidor de Administração, mas sua porta está fechada por um firewall.

- Compartilhamento da área de trabalho do Windows. Ao conectar-se a uma sessão da área de trabalho remota existente, o usuário da sessão no dispositivo recebe uma solicitação para a conexão do administrador. Nenhuma informação sobre a atividade remota no dispositivo e seus resultados será salva em relatórios criados pelo Kaspersky Security Center.

  O administrador pode configurar uma auditoria da atividade do usuário em um dispositivo cliente remoto. Durante a auditoria, o aplicativo salva as informações sobre arquivos no dispositivo cliente que tenham sido abertos e/ou modificados pelo administrador.

Para conectar-se com a área de trabalho de um dispositivo cliente por meio do Compartilhamento da área de trabalho do Windows, as seguintes condições devem ser satisfeitas:

- Microsoft Windows Vista ou mais recente instalado na estação de trabalho do administrador. O tipo de sistema operacional do dispositivo que hospeda o Servidor de Administração não impõe restrições à conexão através do Compartilhamento da área de trabalho do Windows.

  Para verificar se o recurso Compartilhamento da área de trabalho do Windows está incluído na sua edição do Windows, verifique se há a chave CLSID\{32BE5ED2-5C86-480F-A914-0FF8885A1B3F} no registro do Windows.

- O Microsoft Windows Vista ou mais recente está instalado no dispositivo cliente.

- O Kaspersky Security Center usa uma licença para Gerenciamento de patches e vulnerabilidades.

Para conectar-se com a área de trabalho de um de dispositivo cliente através da tecnologia de Compartilhamento da área de trabalho do Windows:

1. No Console de Administração baseado em MMC, no menu de contexto do Servidor de Administração, selecione **Propriedades**.
2. Na janela de propriedades do Servidor de Administração que é exibida, vá para **Configurações de conexão do Servidor de Administração → Portas de conexão**.
3. Verifique se a opção **Abrir porta RDP para o Kaspersky Security Center Web Console** está ativada.
4. No Kaspersky Security Center Web Console, vá para **Dispositivos → Dispositivos gerenciados**.
5. No campo **Caminho atual**, acima da lista de dispositivos gerenciados, clique no link do caminho.

6. No painel aberto do lado esquerdo, selecione o grupo de administração que contém o dispositivo ao qual deseja obter acesso.

7. Marque a caixa de seleção ao lado do nome do dispositivo ao qual deseja obter acesso.

8. Clique no botão **Windows Desktop Sharing**.

   O Assistente de Windows Desktop Sharing é aberto.

9. Clique no botão **Baixar** para baixar o utilitário klsctunnel e aguarde a conclusão do processo de download.

   Se você já tiver o utilitário klsctunnel, ignore esta etapa.

10. Clique no botão **Avançar**.

11. Selecione a sessão no dispositivo ao qual deseja se conectar e clique no botão **Avançar**.

12. No dispositivo de destino, na caixa de diálogo exibida, o usuário deve permitir uma sessão de compartilhamento de área de trabalho. Caso contrário, a sessão não será possível.

    Depois que o usuário do dispositivo confirmar a sessão de compartilhamento da área de trabalho, a próxima página do assistente será aberta.

13. Clique no botão **Copiar para transferência** para copiar o texto do campo de texto. Este texto é um Objeto de Dados Binário (BLOB) que contém as configurações necessárias para estabelecer a conexão entre o Servidor de Administração e o dispositivo gerenciado.

    > Um BLOB é válido por 3 minutos. Se ele tiver expirado, gere um novo BLOB.

14. Execute o utilitário klsctunnel.

    A janela do utilitário é exibida.

15. Cole o texto copiado no campo de texto.

16. Se você usa um servidor proxy, marque a caixa de seleção **Usar o servidor proxy** e especifique as configurações de conexão do servidor proxy.

17. Clique no botão **Abrir porta**.

O compartilhamento da área de trabalho é iniciado em uma nova janela. Caso queira interagir com o dispositivo, clique no ícone Menu () no canto superior esquerdo da janela e selecione **Modo interativo**.

Seleções de dispositivos

As *Seleções de dispositivos* são uma ferramenta para filtrar dispositivos de acordo com as condições específicas. É possível usar as seleções de dispositivos para gerenciar vários dispositivos: por exemplo, para visualizar um relatório apenas sobre esses dispositivos ou mover todos esses dispositivos para outro grupo.

O Kaspersky Security Center fornece uma ampla variedade de *seleções predefinidas* (por exemplo, **Dispositivos com status Crítico**, **A proteção está desativada**, **Foram detectadas ameaças ativas**). As seleções predefinidas não podem ser excluídas. Também é possível criar e configurar *seleções definidas pelo usuário* adicionais.

Em seleções definidas pelos usuários, você pode definir o escopo da pesquisa e selecionar todos os dispositivos, dispositivos gerenciados ou dispositivos não atribuídos. Os parâmetros de pesquisa são especificados nas condições. Na seleção de dispositivos, você pode criar várias condições com parâmetros de pesquisa diferentes. Por exemplo, você pode criar duas condições e especificar conjuntos de IPs diferentes em cada uma delas. Se várias condições forem especificadas, uma seleção exibirá os dispositivos que atendem a alguma das condições. Por outro lado, os parâmetros de pesquisa dentro de uma condição são sobrepostos. Se um conjunto de IPs e o nome de um aplicativo instalado forem especificados em uma condição, apenas esses dispositivos serão exibidos onde o aplicativo está instalado e o endereço IP pertence ao conjunto especificado.

Visualização da lista de dispositivos a partir de uma seleção de dispositivos

O Kaspersky Security Center permite visualizar a lista de dispositivos a partir de uma seleção de dispositivos.

Para visualizar a lista de dispositivos na seleção de dispositivos:

1. No menu principal, vá para a seção **Dispositivos** → **Seleções de dispositivos** ou **Descoberta e implementação** → **Seleções de dispositivos**.

2. Na lista de seleção, clique no nome da seleção de dispositivos.

   A página exibe uma tabela com informações sobre os dispositivos incluídos na seleção de dispositivos.

3. É possível agrupar e filtrar os dados da tabela do dispositivo da seguinte forma:

   - Clique no ícone de configurações (⚙) e, em seguida, selecione as colunas a serem exibidas na tabela.

   - Clique no ícone de filtro (▽), especifique e aplique o critério de filtro no menu resultante.

     A tabela filtrada de dispositivos é exibida.

É possível selecionar um ou vários dispositivos na seleção de dispositivos e clicar no botão **Nova tarefa** para criar uma tarefa que será aplicada a esses dispositivos.

Para mover os dispositivos selecionados da seleção de dispositivos para outro grupo de administração, clique no botão **Migrar para grupo** e, em seguida, selecione o grupo de administração de destino.

Criar uma seleção de dispositivos

Para criar uma seleção de dispositivos:

1. No menu principal, vá para **Dispositivos** → **Seleções de dispositivos**.

   Uma página com uma lista de seleções de dispositivos é exibida.

2. Clique no botão **Adicionar**.

   A janela **Configurações de seleção de dispositivos** se abre.

3. Digite o nome da nova seleção.

4. Especifique o grupo que contém os dispositivos a serem incluídos na seleção de dispositivos:

   - **Localizar qualquer dispositivo** – Procura dispositivos que atendam aos critérios de seleção e incluídos no grupo **Dispositivos gerenciados** ou **Dispositivos não atribuídos**.
   - **Localizar dispositivos gerenciados** – Procura dispositivos que atendam aos critérios de seleção e incluídos no grupo **Dispositivos gerenciados**.
   - **Localizar dispositivos não atribuídos** – Procura dispositivos que atendam aos critérios de seleção e incluídos no grupo **Dispositivos não atribuídos**.

   É possível ativar a caixa de seleção **Incluir dados dos Servidores de Administração secundários** para ativar a pesquisa de dispositivos que atendam aos critérios de seleção e gerenciados por Servidores de Administração secundários.

5. Clique no botão **Adicionar**.

6. Na janela aberta, especifique as condições que devem ser atendidas para a inclusão de dispositivos nesta seleção e depois clique no botão **OK**.

7. Clique no botão **Salvar**.

A seleção de dispositivos é criada e adicionada à lista de seleções de dispositivos.

Configurar uma seleção de dispositivos

Para configurar uma seleção de dispositivo:

1. No menu principal, vá para **Dispositivos** → **Seleções de dispositivos**.

   Uma página com uma lista de seleções de dispositivos é exibida.

2. Escolha a seleção de dispositivos definida pelo usuário relevante e clique no botão **Propriedades**.

   A janela **Configurações de seleção de dispositivos** se abre.

3. Na guia **Geral**, clique no link **Nova condição**.

4. Especifique as condições que devem ser atendidas para a inclusão de dispositivos nesta seleção.

5. Clique no botão **Salvar**.

As configurações são aplicadas e salvas.

Abaixo estão as descrições das condições para atribuir dispositivos a uma seleção. As condições são combinadas através da utilização do operador lógico OR: a seleção conterá dispositivos que estejam em conformidade com pelo menos uma das condições listadas.

Geral

Na seção **Geral**, você pode mudar o nome de uma condição de seleção e especificar se essa condição deve ser invertida:

Inverter condição de seleção

Por padrão, esta opção está desativada.

Se esta opção estiver ativada, a condição de seleção especificada será invertida. A seleção incluirá todos os dispositivos que não atendem a condição.

O exemplo a seguir mostra a lógica do trabalho de inversão:

- **Condição**: no seu dispositivo, há um sistema operacional com o tipo Linux e o número de compilação 00.0.000.
- **Condição invertida**: no seu dispositivo, há um sistema operacional com NOT (o tipo Linux e o número de compilação 00.0.000), que é equivalente ao seguinte:

  Existe um sistema operacional com o tipo NOT Linux OU número de compilação NOT 00.0.000.

Assim, a seleção incluirá os dispositivos com um sistema operacional, por exemplo, do tipo Windows e o número de compilação 00.0.000, ou o tipo Linux e qualquer número de compilação diferente de 00.0.000.

Infraestrutura de rede

Na subseção **Rede**, é possível especificar o critério que será usado para incluir dispositivos na seleção de acordo com seus dados na rede:

- Nome do dispositivo

  Nome da rede Windows (nome NetBIOS) do dispositivo ou o endereço IPv4 ou IPv6.

- Domínio do Windows

  Exibe todos os dispositivos incluídos no domínio do Windows especificado.

- Grupo de administração

  Exibe os dispositivos incluídos no grupo de administração especificado.

- Descrição

Texto na janela Propriedades do dispositivo: no campo **Descrição** da seção **Geral**.

Para descrever texto no campo **Descrição**, é possível usar os seguintes caracteres:

- Em uma palavra:
  - *. Substitui qualquer sequência por qualquer número de caracteres.

    Exemplo:

    Para descrever as palavras **Servidor** ou **Servidores**, é possível inserir **Servidor***.
  - **?.** Substitui qualquer caractere único.

    Exemplo:

    Para descrever palavras como **Janela** ou **Janelas**, você pode inserir **Janel?.**

    O asterisco (*****) ou o ponto de interrogação (**?**) não pode ser usado como o primeiro caractere na consulta.
- Para encontrar várias palavras:
  - Espaço. Exibe todos os dispositivos cujas descrições contêm qualquer uma das palavras listadas.

    Exemplo:

    Para localizar uma frase que contenha as palavras **Secundário** ou **Virtual**, você pode incluir a linha **Secundário Virtual** na consulta.
  - **+**. Quando o sinal de mais antecede uma palavra, todos os resultados de pesquisa contêm essa palavra.

    Exemplo:

    Para encontrar uma frase que contenha as palavras **Secundário** e **Virtual**, insira **+Secundário+Virtual** na consulta.
  - **-**. Quando um sinal de menos antecede uma palavra, nenhum dos resultados de pesquisa contém essa palavra.

    Exemplo:

    Para encontrar uma frase que contenha **Secundário**, mas que não contenha **Virtual**, insira **+Secundário-Virtual** na consulta.
  - **"<algum texto>"**. O texto dentro de aspas deve estar no texto.

    Exemplo:

    Para encontrar uma expressão que contenha a combinação de palavras **Servidor Secundário**, você pode inserir **"Servidor Secundário"** na consulta.

- Intervalo IP

  Se esta opção estiver ativada, você poderá inserir os endereços IP inicial e final do conjunto de IPs no qual os dispositivos relevantes devem ser incluídos.

  Por padrão, esta opção está desativada.

- Gerenciado por outro Servidor de Administração

  Selecione um dos seguintes valores:

  - **Sim**. Uma regra de migração de dispositivo será aplicável apenas aos dispositivos cliente gerenciados por outros Servidores de Administração. Esses servidores são diferentes do servidor no qual a regra de migração de dispositivo é configurada.
  - **Não**. A regra de movimentação de dispositivos aplica-se apenas a dispositivos clientes gerenciados pelo Servidor de Administração atual.
  - **Nenhum valor está selecionado**. A condição não se aplica.

Na subseção **Active Directory**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com os dados do Active Directory:

- O dispositivo está em uma unidade organizacional do Active Directory

  Se esta opção estiver ativada, a seleção inclui os dispositivos da unidade do Active Directory especificada no campo de entrada.

  Por padrão, esta opção está desativada.

- Incluir unidades organizacionais secundárias

  Caso esta opção esteja ativada, a seleção incluirá os dispositivos das unidades de organização secundárias da unidade organizacional do Active Directory especificada.

  Por padrão, esta opção está desativada.

- Este dispositivo é membro de um grupo do Active Directory

  Se esta opção estiver ativada, a seleção incluirá os dispositivos do grupo do Active Directory especificado no campo de entrada.

  Por padrão, esta opção está desativada.

Na subseção **Atividade de rede**, é possível especificar o critério que será usado para incluir dispositivos na seleção de acordo com a sua atividade de rede:

- Atua como ponto de distribuição

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. A seleção inclui dispositivos que agem como pontos de distribuição.
  - **Não**. Dispositivos que atuam como pontos de distribuição não serão incluídos na seleção.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Não desconectar do Servidor de Administração

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Ativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** está selecionada.
  - **Desativado**. A seleção incluirá dispositivos nos quais a caixa de seleção **Não desconectar do Servidor de Administração** não está selecionada.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Perfil de conexão trocado

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. A seleção incluirá os dispositivos que se conectaram ao Servidor de Administração após o perfil de conexão ter sido alternado.
  - **Não**. A seleção não incluirá os dispositivos que se conectaram com o Servidor de Administração após o perfil de conexão ter sido alternado.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Última conexão com o Servidor de Administração

  Você pode usar essa caixa de seleção para configurar um critério para pesquisar por dispositivos pela hora da sua última conexão com o Servidor de Administração.

  Se essa caixa de seleção estiver selecionada, é possível, nos campos de entrada especificar o intervalo de tempo (data e hora) durante o qual a última conexão entre o Agente de Rede instalado no dispositivo cliente e o Servidor de Administração foi estabelecida. A seleção inclui dispositivos que estejam no intervalo especificado.

  Se essa caixa de seleção for desmarcada, o critério não é aplicado.

  Por padrão, esta caixa de seleção está desmarcada.

- Novos dispositivos detectados pela sondagem da rede

  Procura por novos dispositivos que tenham sido detectados pela sondagem da rede ao longo dos poucos últimos dias.

  Se esta opção estiver ativada, a seleção somente inclui novos dispositivos que tenham sido detectados pela descoberta de dispositivos durante a quantidade de dias especificada no campo **Período de detecção (dias)**.

  Se esta opção estiver ativada, a seleção inclui todos os dispositivos que tenham sido detectados pela descoberta de dispositivos.

  Por padrão, esta opção está desativada.

- Dispositivo visível

  Na lista suspensa, você pode configurar um critério para incluir dispositivos em uma seleção ao executar pesquisas:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos atualmente visíveis na rede.
  - **Não**. O aplicativo é incluído na seleção de dispositivos atualmente invisíveis na rede.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

Na subseção **Segmentos da nuvem**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com os seus respectivos segmentos da nuvem:

- O dispositivo está no segmento da nuvem

  Caso a opção esteja ativada, será possível escolher os dispositivos dos segmentos da nuvem AWS, Azure e Google.

  Caso a opção **Incluir objetos secundários** esteja marcada, a pesquisa será executada em todos os objetos secundários do segmento especificado.

  Os resultados da pesquisa somente incluem dispositivos do segmento selecionado.

- Dispositivo detectado usando a API

  Na lista suspensa, você pode selecionar se um dispositivo é detectado pelas ferramentas API:

  - **Sim**. O dispositivo é detectado usando a API da AWS, Azure ou Google.
  - **Não**. O dispositivo não pode ser detectado usando a API da AWS, do Azure ou do Google. Ou seja, o dispositivo está fora do ambiente de nuvem ou está no ambiente em nuvem, mas não pode ser detectado usando uma API.
  - Nenhum valor. Esta condição não se aplica.

Status do dispositivo

Na seção **Status do dispositivo gerenciado**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com a descrição do status de dispositivos de um aplicativo gerenciado:

- **Status do dispositivo**

  Lista suspensa na qual você pode selecionar um dos status do dispositivo: *OK*, *Crítico* ou *Advertência*.

- **Status da proteção em tempo real**

  Lista suspensa na qual você pode selecionar o status da proteção em tempo real. Os dispositivos com um status da proteção em tempo real especificado serão incluídos na seleção.

- **Descrição do status do dispositivo**

  Neste campo, você poderá selecionar caixas de seleção próximas das condições que, se atendidas, atribuem um dos seguintes status ao dispositivo: *OK, Crítico* ou *Advertência*.

Na subseção **Status dos componentes em aplicativos gerenciados**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o status dos componentes em aplicativos gerenciados:

- **Status da prevenção de vazamento de dados**

  Pesquise dispositivos pelo status da Prevenção de vazamento de dados (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

- **Status da proteção dos servidores de colaboração**

  Procure dispositivos pelo status da proteção de colaboração do servidor (*Sem dados do dispositivo*, *Parado*, *Iniciando, Pausado*, *Executando*, *Falhou*).

- **Status da proteção antivírus dos servidores de correio**

  Procure dispositivos pelo status da proteção do servidor de e-mail (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

- **Status do Endpoints Sensor**

  Procure dispositivos pelo status do componente Endpoint Sensor (*Sem dados do dispositivo, Parado, Iniciando, Pausado, Executando, Falhou*).

Na subseção **Problemas que afetam o status em aplicativos gerenciados**, é possível especificar os critérios que serão usados para incluir os dispositivos na seleção de acordo com a lista de possíveis problemas detectados por um aplicativo gerenciado. Se pelo menos um problema que você selecionar existir em um dispositivo, o dispositivo estará incluído na seleção. Quando você seleciona um problema listado para vários aplicativos, você tem a opção de selecionar esse problema em todas das listas automaticamente.

Você pode selecionar as caixas de seleção para descrições de status do aplicativo gerenciado; ao receber este status, os dispositivos serão incluídos na seleção. Quando você seleciona um status listado para vários aplicativos, você tem a opção de selecionar esse status em todas das listas automaticamente.

Detalhes do sistema

Na seção **Sistema operacional**, você pode especificar o critério que será usado para incluir dispositivos na seleção de acordo com o seu tipo de sistema operacional.

- Tipo de plataforma

  Se esta caixa de seleção estiver marcada, você pode selecionar um sistema operacional da lista. Os dispositivos com o sistema operacional especificado instalado são incluídos nos resultados de pesquisa.

- Versão do service pack do sistema operacional

  Neste campo, você pode especificar a versão do pacote do sistema operacional (no formato *X.Y*), o que determinará como a regra de migração será aplicada ao dispositivo. Por padrão, nenhum valor de versão é especificado.

- Tipo de bit do sistema operacional

  Na lista suspensa, você poderá selecionar a arquitetura para o sistema operacional, que determinará como a regra para mover será aplicada ao dispositivo (**Desconhecido**, **x86**, **AMD64** ou **IA64**). Por padrão, nenhuma opção é selecionada na lista para que a arquitetura do sistema operacional não fique definida.

- Compilação do sistema operacional

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  O número da compilação do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um número de compilação igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de compilação, exceto o especificado.

- Número da versão do sistema operacional

  Esta configuração é aplicável somente aos sistemas operacionais Windows.

  O identificador (ID) da versão do sistema operacional. Você pode especificar se o sistema operacional selecionado deve ter um ID da versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todos os números de ID da versão, exceto o especificado.

Na seção **Máquinas virtuais**, você pode definir o critério para incluir os dispositivos na seleção se estes são máquinas virtuais ou parte da Virtual Desktop Infrastructure (VDI):

- **Esta é uma máquina virtual**

  Na lista suspensa, você pode selecionar as seguintes opções:

  - **Indefinido**.
  - **Não**. Localizar dispositivos que não sejam máquinas virtuais.
  - **Sim**. Localizar dispositivos que são máquinas virtuais.

- **Tipo de máquina virtual**

  Na lista suspensa, você pode selecionar o fabricante da máquina virtual.

  Essa lista suspensa estará disponível se o valor **Sim** ou **Irrelevante** estiver selecionado na lista suspensa **Esta é uma máquina virtual**.

- **Parte da Virtual Desktop Infrastructure**

  Na lista suspensa, você pode selecionar as seguintes opções:

  - **Indefinido**.
  - **Não**. Localizar dispositivos que não fazem parte da Virtual Desktop Infrastructure.
  - **Sim**. Localizar dispositivos que fazem parte da Virtual Desktop Infrastructure (VDI).

Na subseção **Registro de hardware**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o hardware instalado:

Verifique e confirme se o utilitário lshw está instalado nos dispositivos Linux a partir dos quais deseja buscar detalhes de hardware. Os detalhes de hardware obtidos de máquinas virtuais podem estar incompletos, dependendo do hipervisor usado.

- **Dispositivo**

  Na lista suspensa, você pode selecionar um tipo de unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

  O campo suporta a pesquisa de texto completo.

- **Fornecedor**

  Na lista suspensa, você pode selecionar o nome do fabricante da unidade. Todos os dispositivos com esta unidade são incluídos nos resultados da pesquisa.

  O campo suporta a pesquisa de texto completo.

- **Nome do dispositivo**

  Nome do dispositivo na rede Windows. O dispositivo com o nome especificado será incluído na seleção.

- **Descrição**

  Descrição de um dispositivo ou de uma unidade de hardware. Os dispositivos com a descrição especificada neste campo serão incluídos na seleção.

  A descrição de um dispositivo em qualquer formado pode ser inserida na janela de propriedades desse dispositivo. O campo suporta a pesquisa de texto completo.

- **Fornecedor do dispositivo**

  Nome do fabricante do dispositivo. Os dispositivos produzidos pelo fabricante especificado neste campo estão incluídos na seleção.

  Você pode inserir o nome do fabricante na janela de propriedades de um dispositivo.

- **Número de série**

  Todas as unidades hardware com número de série especificado nesse campo serão incluídas na seleção.

- **Número de inventário**

  Equipamentos com o número de inventário especificado neste campo serão incluídos na seleção.

- **Usuário**

  Todas as unidades hardware do usuário especificado nesse campo serão incluídas na seleção.

- **Localização**

  A localização do dispositivo ou unidade de hardware (por exemplo, na sede ou no escritório de uma filial). Computadores ou outros dispositivos que são implementados na localização especificada nesse campo serão incluídos na seleção.

  Você pode descrever a localização de um dispositivo em qualquer formato na janela de propriedades desse dispositivo.

- **Frequência do clock da CPU em MHz, de**

  A taxa de clock mínima de uma CPU. Os dispositivos com uma CPU que corresponda ao intervalo de taxa de clock especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- **Frequência do clock da CPU em MHz, para**

  A taxa de clock máxima de uma CPU. Os dispositivos com uma CPU que corresponda ao intervalo de taxa de clock especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- Número de núcleos da CPU virtual, de

  O número mínimo de núcleos de CPU virtuais. Os dispositivos com uma CPU que corresponda ao intervalo do número de núcleos virtuais especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- Número de núcleos da CPU virtual, até

  O número máximo de núcleos de CPU virtuais. Os dispositivos com uma CPU que corresponda ao intervalo do número de núcleos virtuais especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- Volume do disco rígido, em GB, de

  O volume mínimo do disco rígido no dispositivo. Os dispositivos com um disco rígido que corresponda a faixa especificada nos campos de entrada (inclusive) serão incluídos na seleção.

- Volume do disco rígido, em GB, para

  O volume máximo do disco rígido no dispositivo. Os dispositivos com um disco rígido que corresponda a faixa especificada nos campos de entrada (inclusive) serão incluídos na seleção.

- Tamanho da RAM em MB, de

  O tamanho mínimo da RAM do dispositivo. Os dispositivos com RAM que corresponda ao intervalo de tamanho especificado nos campos de entrada (inclusive) serão incluídos na seleção.

- Tamanho da RAM em MB, para

  O tamanho máximo da RAM do dispositivo. Os dispositivos com RAM que corresponda ao intervalo de tamanho especificado nos campos de entrada (inclusive) serão incluídos na seleção.

Detalhes de software de terceiros

Na subseção **Registro de aplicativos**, é possível definir o critério para pesquisar dispositivos de acordo com os aplicativos neles instalados:

- Nome do aplicativo

  Lista suspensa na qual é possível selecionar um aplicativo. Os dispositivo nos quais o aplicativos especificado estiver instalado, serão incluídos na seleção.

- Versão do aplicativo

  Campo de entrada onde é possível especificar a versão do aplicativo selecionado.

- Fornecedor

  Lista suspensa na qual é possível selecionar o fabricante de um aplicativo instalado no dispositivo.

- Status do aplicativo

  Uma lista suspensa na qual é possível selecionar o status de um aplicativo (*Instalado*, *Não instalado*). Os dispositivos nos quais o aplicativo especificado está ou não instalado, dependendo do status selecionado, serão incluídos na seleção.

- Localizar por atualização

  Se esta opção estiver ativada, a pesquisa será executada usando os dados das atualizações para os aplicativos instalados nos dispositivos relevantes. Após selecionar a caixa de seleção, os campos **Nome do aplicativo**, **Versão do aplicativo** e **Status do aplicativo** mudam para **Nome da atualização**, **Versão da atualização** e **Status** respectivamente.

  Por padrão, esta opção está desativada.

- Nome do aplicativo de segurança incompatível

  Lista suspensa na qual é possível selecionar aplicativos de segurança de terceiros. Durante a pesquisa, os dispositivos nos quais está instalado o aplicativo especificado, serão incluídos na seleção.

- Tag do aplicativo

  Na lista suspensa, você pode selecionar a tag do aplicativo. Todos os dispositivos que instalaram aplicativos com a tag selecionada na descrição são incluídos na seleção de dispositivo.

- Aplicar aos dispositivos sem tags especificadas

  Se esta opção estiver ativada, o perfil da política inclui dispositivos com descrições que não contêm nenhuma das tags selecionadas.

  Se esta opção estiver desativada, o critério não é aplicado.

  Por padrão, esta opção está desativada.

Na subseção **Vulnerabilidades e atualizações**, é possível especificar o critério que será usado para incluir dispositivos na seleção de acordo com a fonte do Windows Update:

WUA foi mudado para o Servidor de Administração

Você pode selecionar uma das seguintes opções de pesquisa da lista suspensa:

- **Sim**. Se essa opção estiver selecionada, os resultados da pesquisa incluirão os dispositivos que recebem atualizações através do Windows Update do Servidor de Administração.
- **Não**. Caso essa opção esteja selecionada, os resultados incluirão os dispositivos que recebem atualizações pelo Windows Update de outras fontes.

Detalhes de aplicativos Kaspersky

Na subseção **Aplicativos Kaspersky**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o aplicativo gerenciado selecionado:

- Nome do aplicativo

  Na lista suspensa, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome de um aplicativo da Kaspersky.

  A lista somente fornece os nomes de aplicativos com plugins de gerenciamento instalados na estação de trabalho do administrador.

  Se nenhum aplicativo for selecionado, o critério não será aplicado.

- Versão do aplicativo

  No campo de entrada, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo número da versão de um aplicativo da Kaspersky.

  Se nenhum número de versão for especificado, o critério não será aplicado.

- Nome da atualização crítica

  No campo de entrada de dados, você poderá configurar um critério para incluir dispositivos em uma seleção ao executar uma pesquisa pelo nome do aplicativo ou pelo número do pacote de atualização.

  Se o campo for deixado em branco, o critério não será aplicado.

- Status do aplicativo

  Uma lista suspensa na qual é possível selecionar o status de um aplicativo (*Instalado*, *Não instalado*). Os dispositivos nos quais o aplicativo especificado está ou não instalado, dependendo do status selecionado, serão incluídos na seleção.

- Última atualização dos módulos

  Você pode usar esta opção para definir um critério para pesquisar dispositivos pela hora da última atualização dos módulos de aplicativos instalados nesses dispositivos.

  Se essa caixa de seleção estiver selecionada, nos campos de entrada você poderá especificar o intervalo de tempo (data e hora) durante o qual a última atualização de módulos de aplicativos instalados nesses dispositivos foi executada.

  Se essa caixa de seleção for desmarcada, o critério não é aplicado.

  Por padrão, esta caixa de seleção está desmarcada.

- O dispositivo é gerenciado através do Kaspersky Security Center 14.2

  Na lista suspensa, você poderá incluir nos dispositivos selecionados gerenciados através do Kaspersky Security Center:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos gerenciados através do Kaspersky Security Center.
  - **Não**. O aplicativo inclui dispositivos na seleção se eles não forem gerenciados pelo Kaspersky Security Center.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

- Aplicativo de segurança instalado

  Na lista suspensa, você poderá incluir na seleção todos os dispositivos com o aplicativo de segurança instalado:

  - **Sim**. O aplicativo é incluído na seleção de dispositivos com o aplicativo de segurança instalado.
  - **Não**. O aplicativo inclui na seleção todos os dispositivos sem nenhum aplicativo de segurança instalado.
  - **Nenhum valor está selecionado**. O critério não será aplicado.

Na subseção **Proteção antivírus**, é possível configurar o critério para a inclusão de dispositivos em uma seleção de acordo com o status da proteção:

- Bancos de dados lançados

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes por data de lançamento de versão do banco de dados antivírus. Nos campos de entrada, você pode definir o intervalo de tempo com base no qual a pesquisa é realizada.

  Por padrão, esta opção está desativada.

- Contagem de registros do banco de dados

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pelo número de registros de banco de dados. Nos campos de entrada, você pode definir os valores do limite inferior e superior para os registros do banco de dados antivírus.

  Por padrão, esta opção está desativada.

- **Última verificação**

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pela hora da última verificação de malwares. No campo de entrada, você poderá especificar o período de tempo no qual a última verificação de malwares foi executada.

  Por padrão, esta opção está desativada.

- **Ameaças detectadas**

  Se esta opção estiver ativada, você poderá pesquisar por dispositivos clientes pelo número de vírus detectados. Nos campos de entrada, você pode definir os valores limite inferiores e superiores pelo número de vírus encontrados.

  Por padrão, esta opção está desativada.

Na subseção **Criptografia**, é possível configurar o critério de inclusão de dispositivos em uma seleção de acordo com o algoritmo de criptografia selecionado:

Algoritmo de criptografia

Algoritmo de criptografia de bloco simétrico Advanced Encryption Standard (AES). Na lista suspensa, você pode selecionar o tamanho de chave de criptografia (de 56 bits, de 128 bits, de 192 bits ou de 256 bits).

Valores disponíveis: *AES56*, *AES128*, *AES192* e *AES256*.

A subseção **Componentes do aplicativo** contém a lista de componentes desses aplicativos que têm plug-ins de gerenciamento correspondentes instalados no Kaspersky Security Center Web Console.

Na subseção **Componentes do aplicativo**, é possível especificar o critério para a inclusão de dispositivos em uma seleção de acordo com o status e os números da versão dos componentes que fazem referência ao aplicativo que for selecionado:

- **Status**

  Pesquise dispositivos segundo o status do componente enviado por um aplicativo ao Servidor de Administração. É possível selecionar um dos seguintes status: *N/A*, *Interrompido*, *Pausado*, *Iniciando*, *Em execução*, *Com falha*, *Não instalado*, *Não compatível com a licença*. Se o componente selecionado do aplicativo instalado em um dispositivo gerenciado tiver o status especificado, o dispositivo será incluído na seleção de dispositivos.

  Status enviados pelos aplicativos:

  - *Interrompido* – O componente está desativado e não está funcionando no momento atual.
  - *Pausado* – O componente está suspenso, por exemplo, depois que o usuário pausou a proteção no aplicativo gerenciado.
  - *Iniciando* – O componente está atualmente em processo de inicialização.
  - *Executando* – O componente está ativado e funcionando corretamente.
  - *Falha* – Um erro ocorreu durante a operação do componente.
  - *Não instalado* – O usuário não selecionou o componente para instalação ao configurar a instalação personalizada do aplicativo.
  - *Não compatível com a licença* – A licença não cobre o componente selecionado.

  Diferentemente de outros status, o status *N/A* não é enviado pelos aplicativos. Esta opção mostra que os aplicativos não têm nenhuma informação sobre o status do componente selecionado. Por exemplo, isto pode acontecer quando o componente selecionado não pertence a nenhum dos aplicativos instalados no dispositivo, ou quando o dispositivo está desligado.

- **Versão**

  Pesquise dispositivos segundo o número da versão do componente que você selecionar na lista. Você pode digitar um número de versão, por exemplo `3.4.1.0`, e especificar se o componente selecionado deve ter uma versão igual, anterior ou posterior. Você também pode configurar a pesquisa de todas as versões, exceto a especificada.

Tags

Na seção **Tags**, você pode configurar o critério para pesquisar por dispositivos com base em palavras-chave (tags) adicionadas anteriormente às descrições dos dispositivos gerenciados:

Aplicar se pelo menos uma tag especificada corresponder

Se esta opção estiver ativada, o resultado da pesquisa mostrará os dispositivos com descrições que contêm ao menos uma das tags selecionadas.

Se esta opção estiver ativada, o resultado da pesquisa irá mostrar os dispositivos com descrições que não contêm todos as tags selecionadas.

Por padrão, esta opção está desativada.

Para adicionar tags ao critério, clique no botão **Adicionar** e selecione as tags clicando no campo de entrada **Tag**. Especifique se deseja incluir ou excluir os dispositivos com as tags selecionadas na seleção de dispositivos.

- **Deve ser incluído**

  Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

  Por padrão, esta opção está selecionada.

- **Deve ser excluído**

  Se esta opção for selecionada, os resultados da pesquisa exibirão os dispositivos cujas descrições não contêm a tag selecionada. Para encontrar dispositivos, você pode usar o asterisco, que indica qualquer sequência de caracteres com qualquer número de caracteres.

Usuários

Na seção **Usuários**, você pode definir o critério para incluir dispositivos na seleção de acordo com as contas de usuários que efetuaram o login no sistema operacional.

- **Último usuário que fez login no sistema**

  Se a opção estiver ativada, será possível selecionar a conta de usuário para configurar o critério. Os resultados da pesquisa incluem os dispositivos nos quais o usuário selecionado efetuou o último login no sistema.

- **Usuário que fez login no sistema pelo menos uma vez**

  Se esta opção estiver ativada, clique no botão **Procurar** para especificar uma conta de usuário. Os resultados da pesquisa incluem os dispositivos nos quais o usuário especificado efetuou o login no sistema ao menos uma vez.

Exportação da lista de dispositivos a partir de uma seleção de dispositivos

O Kaspersky Security Center permite salvar informações sobre dispositivos a partir de uma seleção de dispositivos em um arquivo CSV ou TXT.

Para exportar a lista de dispositivos da seleção de dispositivos para um arquivo:

1. Abra a tabela com os dispositivos a partir da seleção de dispositivos.
2. É possível exportar as informações sobre os dispositivos da tabela de uma das seguintes maneiras:

   - Exportar os dispositivos selecionados.

     Selecione as caixas de seleção ao lado dos dispositivos necessários e, a seguir, clique no botão **Exportar linhas para arquivo CSV** ou **Exportar linhas para arquivo TXT**, dependendo do formato para exportação preferido. Todas as informações sobre os dispositivos selecionados incluídos na tabela serão exportadas para um arquivo TXT ou CSV.

   - Exporte todos os dispositivos exibidos na página atual.

     Clique no botão **Exportar linhas para arquivo CSV** ou **Exportar linhas para arquivo TXT**, dependendo do formato de exportação preferido. Não é necessário selecionar os dispositivos da tabela. Todas as informações sobre os dispositivos exibidos na página atual serão exportadas para um arquivo TXT.

Observe que, se foi aplicado um critério de filtro à tabela de dispositivos, apenas os dados filtrados das colunas exibidas serão exportados para um arquivo CSV ou TXT.

Remover os dispositivos de grupos de administração em uma seleção

Ao trabalhar com uma seleção de dispositivos, você poderá remigrar dispositivos dos grupos de administração diretamente nesta seleção, sem alternar para os grupos de administração dos quais estes dispositivos precisam ser removidos.

Para remigrar dispositivos de grupos de administração:

1. No menu principal, vá para **Dispositivos** → **Seleções de dispositivos** ou **Descoberta e implementação** → **Seleções de dispositivos**.
2. Na lista de seleção, clique no nome da seleção de dispositivos.

   A página exibe uma tabela com informações sobre os dispositivos incluídos na seleção de dispositivos.
3. Selecione os dispositivos que deseja remover e, em seguida, clique em **Excluir**.

   Os dispositivos selecionados serão removidos de seus respectivos grupos de administração.

Tags de dispositivo

Esta seção descreve identificadores do dispositivo e fornece instruções para criá-los e modificá-los, bem como para identificar dispositivos manual ou automaticamente.

Tags de dispositivo

O Kaspersky Security Center permite-lhe *identificar* os dispositivos. Uma tag é um rótulo de um dispositivo e pode ser usada para agrupar, descrever ou encontrar dispositivos. As tags atribuídas aos dispositivos podem ser usadas para criar seleções, para localizar dispositivos e para distribuir dispositivos entre grupos de administração.

Você pode identificar os dispositivos manualmente ou automaticamente. Caso não queira atribuir uma tag a um dispositivo individual, será possível usar tags manuais. A codificação automática é executada pelo Kaspersky Security Center de uma das seguintes formas:

- De acordo com as regras de marcação especificadas.
- Por um aplicativo.

Não recomendamos usar diferentes formas de marcação para atribuir a mesma tag. Por exemplo, se a tag for atribuída pela regra, não é recomendável atribuir manualmente essa tag aos dispositivos.

Se as tags forem atribuídas por regras, os dispositivos serão identificados automaticamente quando as regras especificadas forem atendidas. Uma regra individual corresponde a cada tag. As regras são aplicadas às propriedades da rede do dispositivo, sistema operacional, aplicativos instalados no dispositivo e outras propriedades de dispositivo. Por exemplo, se tiver uma infraestrutura híbrida de máquinas físicas, instâncias de Amazon EC2 e máquinas virtuais do Microsoft Azure, você poderá configurar uma regra que atribuirá a tag `[Azure]` a todas as máquinas virtuais do Microsoft Azure. E você pode usar essa tag ao criar uma seleção de dispositivos; e isso o ajudará a classificar todas as máquinas virtuais do Microsoft Azure e atribuir-lhes uma tarefa.

É possível adicionar apenas uma regra de marcação automática por tag. Se uma regra nova for criada para a mesma tag, a anterior será substituída.

A tag é automaticamente removida de um dispositivo nos seguintes casos:

- Quando o dispositivo deixa de atender às condições da regra que atribui a tag.
- Quando a regra que atribui a tag é desativada ou excluída.

A lista de tags e a lista de regras em cada Servidor de Administração são independentes de todos outros Servidores de Administração, inclusive um Servidor de Administração principal ou Servidores de Administração virtuais subordinados. Uma regra é aplicada somente a dispositivos do mesmo Servidor de Administração no qual a regra é criada.

Criando uma tag de dispositivo

Para criar uma tag de dispositivo:

1. No menu principal, vá para **Dispositivos → Tags → Tags de dispositivos**.
2. Clique em **Adicionar**.

   Uma nova janela de tag é exibida.
3. No campo **Tag**, insira um nome de tag.
4. Clique em **Salvar** para salvar as alterações.

A nova tag aparece na lista de tags de dispositivo.

Renomeando uma tag de dispositivo

Para renomear uma tag de dispositivo:

1. No menu principal, vá para **Dispositivos** → **Tags** → **Tags de dispositivos**.
2. Clique no nome da tag que deseja renomear.

   A janela de propriedades do identificador é exibida.
3. No campo **Tag**, altere o nome da tag.
4. Clique em **Salvar** para salvar as alterações.

A tag atualizada aparece na lista de tags de dispositivo.

Excluindo uma tag de dispositivo

Para excluir uma tag de dispositivo:

1. No menu principal, vá para **Dispositivos** → **Tags** → **Tags de dispositivos**.
2. Na lista, selecione a tag de dispositivo que deseja excluir.
3. Clique no botão **Excluir**.
4. Na janela que se abre, clique em **Sim**.

A tag de dispositivo é excluída. A tag excluída é automaticamente removida de todos os dispositivos aos quais foi atribuída.

A tag excluída não é removida automaticamente das regras de codificação automática. Após a tag ser excluída, ela será atribuída a um novo dispositivo apenas quando o dispositivo atender primeiro às condições de uma regra que atribui a tag.

A tag excluída não é removida automaticamente do dispositivo caso ela seja atribuída ao dispositivo por um aplicativo ou Agente de Rede. Para remover a tag do seu dispositivo, use o utilitário klscflag.

Visualizando dispositivos aos quais uma tag está atribuída

Para visualizar dispositivos aos quais uma tag está atribuída:

1. No menu principal, vá para **Dispositivos** → **Tags** → **Tags de dispositivos**.
2. Clique no link **Visualizar dispositivos** ao lado da tag para a qual deseja visualizar os dispositivos atribuídos.

A lista de dispositivos exibida mostra apenas os dispositivos aos quais a tag está atribuída.

Para retornar à lista de tags de dispositivo, clique no botão **Voltar** do navegador.

Visualizando as tags atribuídas a um dispositivo

Para visualizar as tags atribuídas a um dispositivo:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo cujas tags deseja visualizar.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Tags**.

A lista de tags atribuídas ao dispositivo selecionado é exibida. Na coluna **Tag atribuída**, é possível visualizar como a tag foi atribuída.

Na barra de ferramentas, você pode fazer o seguinte:

- Atribua outra tag ao dispositivo.
- Remova uma tag já atribuída.
- Visualizar todas as tags de dispositivos que existem no Servidor de Administração.

Você não pode visualizar as tags atribuídas localmente no dispositivo.

Identificação de um dispositivo manualmente

Para atribuir uma tag a um dispositivo manualmente:

1. Visualize as tags atribuídas ao dispositivo ao qual deseja atribuir outra tag.
2. Clique em **Adicionar**.
3. Na janela que se abre, execute uma das seguintes ações:
   - Para criar e atribuir uma nova tag, selecione **Criar nova tag** e especifique o nome da nova tag.
   - Para selecionar uma tag existente, selecione **Atribuir tag existente** e depois selecione a tag desejada na lista suspensa.
4. Clique em **OK** para aplicar as alterações.
5. Clique em **Salvar** para salvar as alterações.

A tag selecionada é atribuída ao dispositivo.

Removendo uma tag atribuído de um dispositivo

Para remover uma tag de um dispositivo:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo cujas tags deseja visualizar.
3. Na janela de propriedades do dispositivo exibida, selecione a guia **Tags**.
4. Marque a caixa de seleção ao lado da tag que deseja remover.
5. No topo da lista, clique no botão **Desatribuir tag**.
6. Na janela que se abre, clique em **Sim**.

   A tag é removida do dispositivo.

A tag de dispositivo não atribuída não é excluída. Se quiser, você poderá excluí-lo manualmente.

Não é possível remover manualmente as tags atribuídas ao dispositivo por aplicativos ou pelo Agente de Rede. Para remover essas tags, use o utilitário klscflag.

Visualização de regras para identificar dispositivos automaticamente

Para visualizar regras para identificar dispositivos automaticamente,

Execute alguma das seguintes ações:

- No menu principal, vá para **Dispositivos** → **Tags** → **Regras de aplicação automática de tags**.
- No menu principal, vá para **Dispositivos** → **Tags** → **Tags de dispositivos** e, em seguida, clique no link **Configurar regras de aplicação automática de tags**.
- Visualize as tags atribuídas a um dispositivo e depois clique no botão **Configurações**.

A lista de regras para identificar dispositivos automaticamente é exibida.

Edição de uma regra para identificar dispositivos automaticamente

Para editar uma regra para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Clique no nome da regra que deseja editar.

   Uma janela de configurações de regra é exibida.

3. Edite as propriedades gerais da regra:

   a. No campo **Nome da regra**, altere o nome da regra.

      O nome não pode conter mais de 256 caracteres.

   b. Execute alguma das seguintes ações:

      - Ative a regra mudando o botão de alternar para **Regra ativada**.
      - Desative a regra mudando o botão de alternar para **Regra desativada**.

4. Execute alguma das seguintes ações:

   - Se desejar adicionar uma nova condição, clique no botão **Adicionar** e especifique as configurações da nova condição na janela aberta.
   - Se deseja editar uma condição existente, clique no nome da condição que quer editar e edite as configurações de condição.
   - Se deseja excluir uma condição, marque a caixa de seleção ao lado do nome da condição que deseja excluir e clique em **Excluir**.

5. Clique em **OK** na janela de configurações de condições.

6. Clique em **Salvar** para salvar as alterações.

A regra editada é mostrada na lista.

Criação de uma regra para identificar dispositivos automaticamente

Para criar uma regra para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.

2. Clique em **Adicionar**.

   Uma nova janela de configurações de regra é exibida.

3. Configure as propriedades gerais da regra:

   a. No campo **Nome da regra**, insira o novo nome da regra.

      O nome não pode conter mais de 256 caracteres.

   b. Execute uma das seguintes ações:

      - Ative a regra mudando o botão de alternar para **Regra ativada**.
      - Desative a regra mudando o botão de alternar para **Regra desativada**.

   c. No campo **Tag**, digite o novo nome da tag de dispositivo ou selecione uma das tags de dispositivo existentes na lista.

      O nome não pode conter mais de 256 caracteres.

4. Na seção de condições, clique no botão **Adicionar** para adicionar uma nova condição.

   Uma nova janela de configurações de condição é exibida.

5. Insira o nome da condição.

   O nome não pode conter mais de 256 caracteres. O nome deve ser exclusivo em uma regra.

6. Defina o acionamento da regra de acordo com as seguintes condições. Você pode selecionar múltiplas condições.

   - **Rede** – Propriedades da rede do dispositivo, tal como o nome do dispositivo na rede Windows, ou a inclusão do dispositivo em um domínio ou em uma subrede IP.

     Caso o agrupamento com distinção entre maiúsculas e minúsculas seja definido para o banco de dados usado para o Kaspersky Security Center, mantenha maiúsculas e minúsculas ao especificar um nome DNS de dispositivo. Caso contrário, a regra de marcação automática não funcionará.

   - **Aplicativos** – Presença do Agente de Rede no dispositivo, tipo de sistema operacional, versão e arquitetura.
   - **Máquinas virtuais** – O dispositivo pertence a um tipo específico da máquina virtual.
   - **Active Directory** – Presença do dispositivo em uma unidade organizacional do Active Directory e a associação do dispositivo em um grupo do Active Directory.
   - **Registro de aplicativos** – Presença de aplicativos de diferentes fornecedores no dispositivo.

7. Clique em **OK** para salvar as alterações.

   Se necessário, você pode definir múltiplas condições para única regra. Neste caso, a tag será atribuída um dispositivo se atender ao menos uma condição.

8. Clique em **Salvar** para salvar as alterações.

A regra recém-criada entra em vigor nos dispositivos gerenciados pelo Servidor de Administração selecionado. Se as configurações de um dispositivo atenderem as condições da regra, ao dispositivo é atribuído à tag.

Depois, a regra é aplicada nos seguintes casos:

- Automática e periodicamente, dependendo da carga de trabalho de servidor
- Depois que você editar a regra
- Quando você executar a regra manualmente
- Depois que o Servidor de Administração detectar uma modificação nas configurações de um dispositivo que atende às condições de regra ou nas configurações de um grupo que contém tal dispositivo

Você pode criar múltiplas regras de identificação. A um dispositivo único pode ser atribuído múltiplas regras de identificação e se as respetivas condições destas regras forem atendidas simultaneamente. Você pode exibir a lista de todas as tags atribuídas nas propriedades do dispositivo.

Execução de regras para identificar dispositivos automaticamente

Quando uma regra é executada, a tag especificada nas propriedades dessa regra é atribuída aos dispositivos que atendem às condições especificadas nas propriedades da mesma regra. Você pode executar apenas regras ativas.

Para executar regras para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Marque as caixas de seleção ao lado das regras ativas que você deseja executar.
3. Clique no botão **Executar regra**.

As regras selecionadas são executadas.

Exclusão de uma regra para identificar dispositivos automaticamente

Para excluir uma regra para identificar dispositivos automaticamente:

1. Visualize regras para identificar dispositivos automaticamente.
2. Marque a caixa de seleção ao lado da regra que você deseja excluir.
3. Clique em **Excluir**.
4. Na janela exibida, clique em **Excluir** novamente.

A regra selecionada é excluída. A tag especificada nas propriedades dessa regra tem a atribuição removida de todos dos dispositivos aos quais foi atribuída.

> A tag de dispositivo não atribuída não é excluída. Se quiser, você poderá excluí-lo manualmente.

Gerenciamento de tags de dispositivo usando o utilitário klscflag

Para atribuir um conjunto de tags a um dispositivo, é preciso executar o utilitário klscflag no dispositivo cliente ao qual se deseja atribuir as tags.

O utilitário klscflag substitui as tags existentes atribuídas ao dispositivo. Isso significa que é possível adicionar ou remover tags ao indicar o conjunto de tags desejado no comando. O utilitário não possui comandos separados para adicionar ou remover tags individuais. Em vez disso, todo o conjunto de tags é modificado.

> Ao especificar os nomes de tags em comandos, como o klscflag, é recomendado utilizar um padrão consistente de letras maiúsculas e minúsculas, deixando todas as letras em maiúsculo, por exemplo. Usar todas as letras maiúsculas pode ajudar a evitar possíveis problemas com tags que diferem apenas em maiúsculas e minúsculas, dependendo da configuração do DBMS.

Para atribuir tags ao seu dispositivo com o uso do utilitário klscflag:

1. Execute o prompt de comando do Windows usando direitos de administrador e altere o diretório atual para o diretório com o utilitário klscflag. O utilitário klscflag está localizado na pasta onde o Agente de Rede está instalado. O caminho de instalação padrão é <Disk>:\Program Files (x86)\Kaspersky Lab\NetworkAgent.

2. Insira um dos seguintes comandos:

   - Para atribuir um conjunto de tags:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" NOME DA TAG 1 \",\" NOME DA TAG 2 \",\" NOME DA TAG 3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     onde `[\" NOME DA TAG 1 \",\" NOME DA TAG 2 \",\" NOME DA TAG 3 \"]` é a lista de tags que se deseja atribuir ao dispositivo.

     Caso deixe os colchetes vazios, isso removerá todas as tags do 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\";"
     ```

   - Para atribuir uma nova tag a um conjunto existente de tags:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" NOME DA NOVA TAG \",\" NOME DA NOVA TAG 1 \",\" NOME DA NOVA TAG 2 \",\" NOME DA NOVA TAG 3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

     onde `NOME DA NOVA TAG` é o nome da tag que se deseja atribuir ao dispositivo e `NOME DA TAG 1`, `NOME DA TAG 2` e `NOME DA TAG 3` são os nomes das tags já atribuídas ao dispositivo.

   - Para remover uma tag específica sem remover outras tags já atribuídas ao dispositivo, execute o comando com o conjunto atualizado de tags.

     Por exemplo, caso suas tags atuais sejam `NOME DA TAG 1`, `NOME DA TAG 2` e `NOME DA TAG 3` e se quiser remover `NOME DA TAG 2`, execute o seguinte comando:

     ```
     klscflag -ssvset -pv 1103/1.0.0.0 -s KLNAG_SECTION_TAGS_INFO -n KLCONN_HOST_TAGS -sv "[\" NOME DA TAG 1 \",\" NOME DA TAG 3 \"]" -svt ARRAY_T -ss "|ss_type = \"SS_PRODINFO\";"
     ```

3. Reinicie o serviço do Agente de Rede.

   O utilitário klscflag atribui as tags especificadas ao seu dispositivo.

4. Se você quiser garantir que o utilitário klscflag tenha atribuído com sucesso as tags especificadas, visualize as tags atribuídas ao dispositivo.

Como alternativa, é possível atribuir tags de dispositivo manualmente.

Políticas e perfis da política

No Kaspersky Security Center Web Console, é possível criar políticas para aplicativos da Kaspersky. Esta seção descreve políticas e perfis da política e fornece instruções para criá-las e modificá-las.

Sobre as políticas e perfis de política

Uma *política* é um conjunto de configurações do aplicativo Kaspersky, aplicadas a um grupo de administração e seus subgrupos. Você pode instalar vários aplicativos Kaspersky nos dispositivos de um grupo de administração. O Kaspersky Security Center fornece uma única política para cada aplicativo Kaspersky em um grupo de administração. Uma política tem um dos seguintes status (consulte a tabela abaixo):

O status da política

Status	Descrição
Ativo	A política atual aplicada ao dispositivo. Apenas uma política pode estar ativa por aplicativo Kaspersky em cada grupo de administração. Os dispositivos aplicam os valores de configuração de uma política ativa para um aplicativo Kaspersky.
Inativo	Uma política que não é aplicada atualmente a um dispositivo.
Ausência	Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

As políticas funcionam de acordo com as seguintes regras:

- Várias políticas com valores diferentes podem ser configuradas para um único aplicativo.
- Apenas uma política pode estar ativa para o aplicativo atual.
- É possível ativar uma política desativada quando um evento específico ocorre. Por exemplo, você pode forçar configurações de proteção antivírus mais rigorosas durante surtos de vírus.
- Uma política pode ter políticas secundárias.

Geralmente, você pode usar políticas como preparação para situações de emergência, como um ataque de vírus. Se houver um ataque por meio de unidades flash, você pode ativar uma política que bloqueie o acesso a unidades flash. Nesse caso, a política ativa atual torna-se automaticamente inativa.

Para evitar ter que efetuar manutenção de várias políticas, por exemplo, quando ocasiões diferentes pressupõem a alteração de várias configurações apenas, você pode usar perfis de política.

Um *perfil de política* é um subconjunto nomeado de valores de configuração que substitui os valores de configuração de uma política. Um perfil de política afeta a formação de configurações efetivas em um dispositivo gerenciado. *Configurações em vigor* são um conjunto de configurações de política, configurações de perfil de política e configurações de aplicativo locais aplicadas atualmente ao dispositivo.

Os perfis de política funcionam de acordo com as seguintes regras:

- Um perfil de política entra em vigor quando ocorre uma condição de ativação específica.
- Os perfis contêm valores de configurações que diferem das configurações de política.
- A ativação de um perfil de política altera as configurações em vigor do dispositivo gerenciado.
- Uma política pode incluir no máximo 100 perfis de política.

Sobre as configurações de bloqueio e bloqueadas

Cada configuração de política tem um ícone de botão de bloqueio (). A tabela abaixo mostra os status do botão de bloqueio:

Status do botão de bloqueio

Status	Descrição
Indefinido	Se um cadeado aberto for exibido ao lado de uma configuração e o botão de alternância estiver desativado, a configuração não será especificada na política. Um usuário pode alterar essas configurações na interface gerenciada do aplicativo. Esse tipo de configuração é chamado de *desbloqueado*.
Aplicar	Se um cadeado fechado for exibido ao lado de uma configuração e o botão de alternância estiver ativado, a configuração será aplicada aos dispositivos nos quais essa política é aplicada. O usuário não pode modificar os valores dessas configurações na interface gerenciada do aplicativo. Esse tipo de configuração é chamado de *bloqueado*.

É altamente recomendável que você bloqueie as configurações da política que deseja aplicar nos dispositivos gerenciados. As configurações da política desbloqueadas podem ser reatribuídas pelas configurações do aplicativo da Kaspersky em um dispositivo gerenciado.

Você pode usar um botão de bloqueio para realizar as seguintes ações:

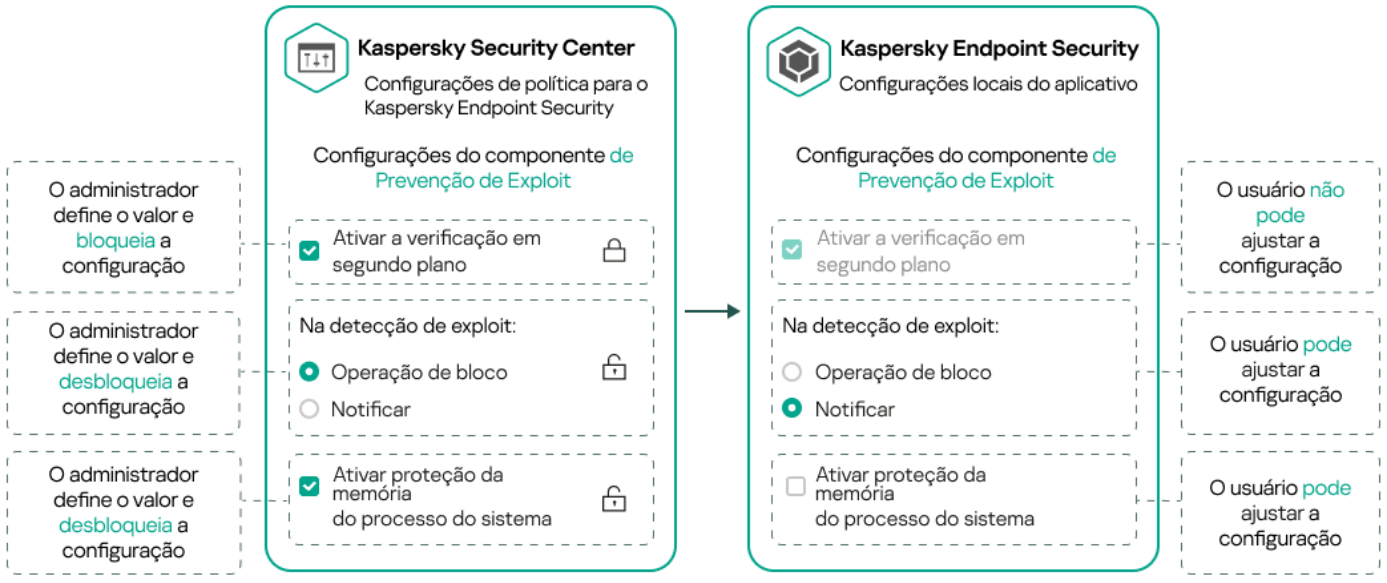
- Configurações de bloqueio para uma política de subgrupo de administração
- Bloqueando as configurações de um aplicativo da Kaspersky em um dispositivo gerenciado

Assim, uma configuração bloqueada é usada para implementar configurações efetivas em um dispositivo gerenciado.

Um processo de implementação de configurações eficazes inclui as seguintes ações:

- O dispositivo gerenciado aplica os valores de configuração do aplicativo da Kaspersky.
- O dispositivo gerenciado aplica valores de configurações bloqueados de uma política.

Uma política e um aplicativo da Kaspersky gerenciado contêm o mesmo conjunto de configurações. Ao definir as configurações de política, as configurações do aplicativo da Kaspersky mudam de valores em um dispositivo gerenciado. Não é possível ajustar as configurações bloqueadas em um dispositivo gerenciado (ver figura abaixo):



Configurações de bloqueio e de aplicativos da Kaspersky

Herança de políticas e perfis de política

Esta seção fornece informações sobre a hierarquia e herança de políticas e perfis de política.

Hierarquia de políticas

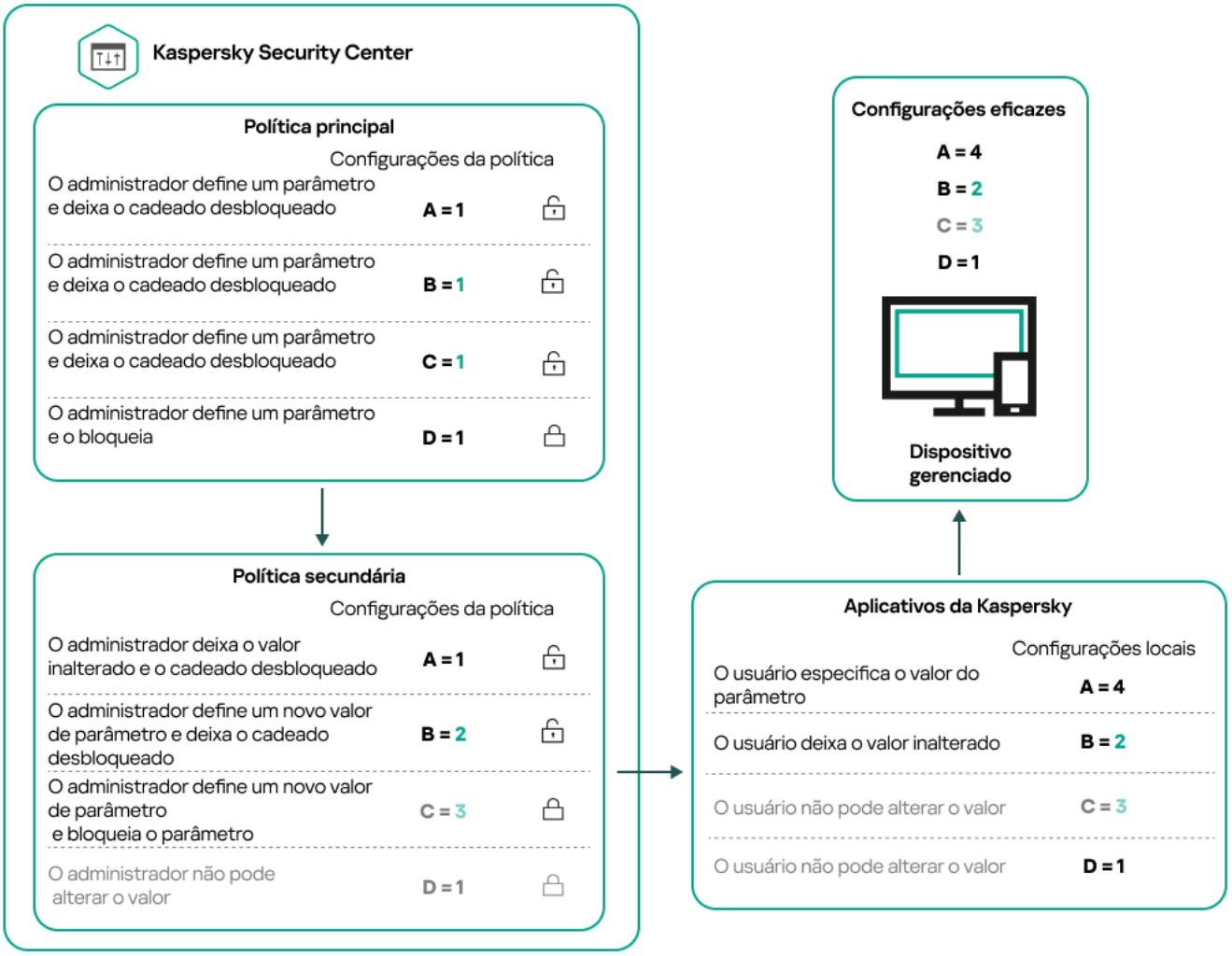
Se dispositivos diferentes precisarem de configurações diferentes, você pode organizar os dispositivos em grupos de administração.

Você pode especificar uma política para um único grupo de administração. As configurações de política podem ser *herdadas*. Herança significa receber valores de configurações de política em subgrupos (grupos secundários) de uma política de um grupo de administração de nível superior (principal).

Depois disso, a política de um grupo principal é também referida como uma *política principal*. Uma política para um subgrupo (grupo secundário) também é chamada de *política secundária*.

Por padrão, pelo menos um grupo de dispositivos gerenciados existe no Servidor de Administração. Se você deseja criar grupos personalizados, esses são criados como subgrupos (grupos secundários) dentro do grupo de dispositivos gerenciados.

Políticas de um mesmo aplicativo atuam entre si, de acordo com uma hierarquia de grupos de administração. As configurações bloqueadas de uma política de um grupo de administração de nível superior (principal) reatribuirão os valores das configurações de política de um subgrupo (ver figura abaixo).



Hierarquia de políticas

Perfis de política em uma hierarquia de políticas

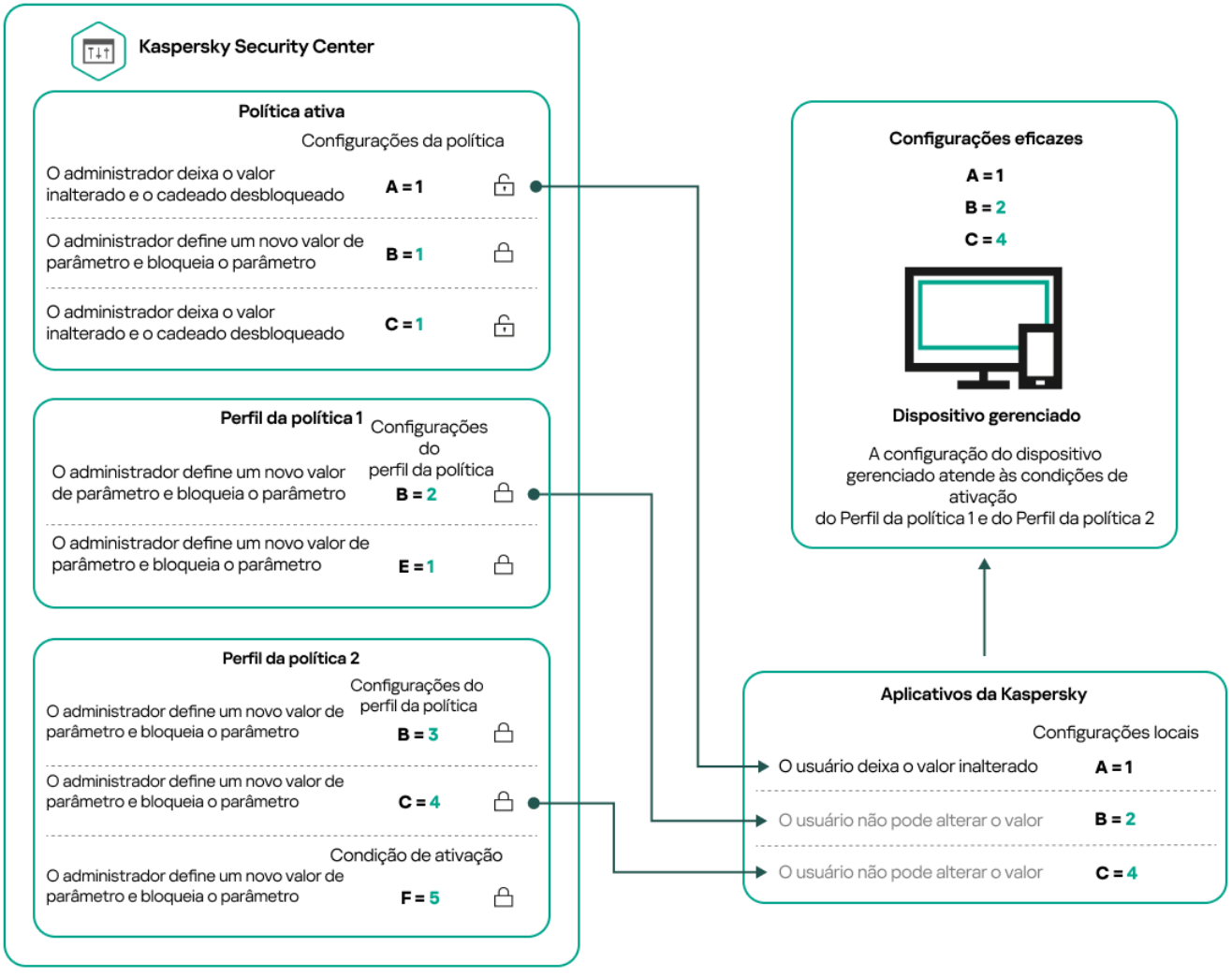
Os perfis de política têm as seguintes condições de atribuição de prioridade:

- A posição de um perfil em uma lista de perfis de política indica sua prioridade. Você pode alterar uma prioridade de perfil da política. A posição mais alta em uma lista indica a prioridade mais alta (veja a figura abaixo).



Definição de prioridade de um perfil de política

- As condições de ativação dos perfis de política não dependem umas das outras. Vários perfis de política podem ser ativados simultaneamente. Se vários perfis de política afetam a mesma configuração, o dispositivo obtém o valor de configuração do perfil de política com a prioridade mais alta (veja a figura abaixo).

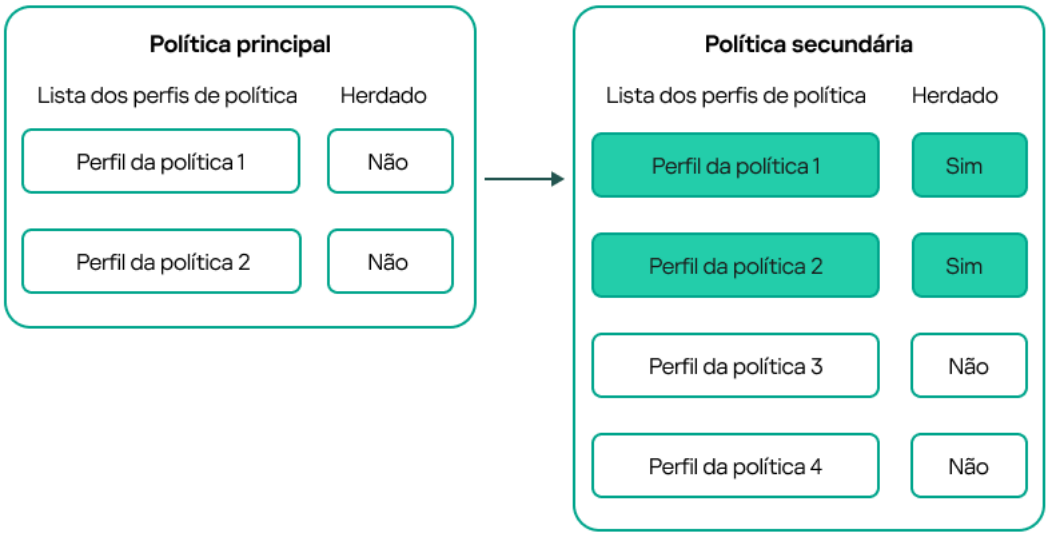


A configuração do dispositivo gerenciado atende às condições de ativação de vários perfis de política

Perfis de política em uma hierarquia de herança

Os perfis de política de diferentes políticas de nível de hierarquia estão em conformidade com as seguintes condições:

- Uma política de nível inferior herda perfis de política de uma política de nível superior. Um perfil de política herdado de uma política de nível superior obtém prioridade mais alta do que o nível do perfil de política original.
- Você não pode alterar a prioridade de um perfil de política herdado (veja a figura abaixo).

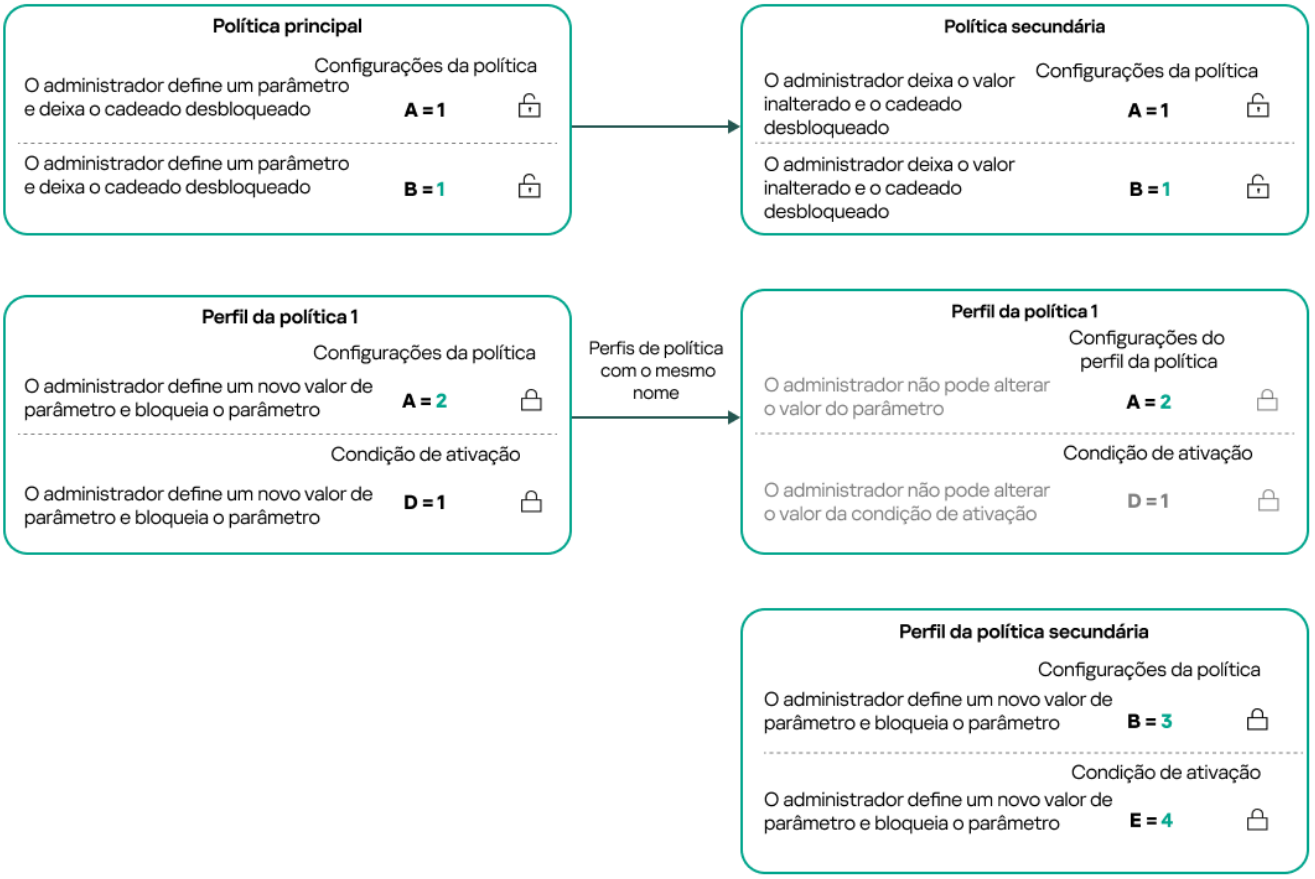


Herança de perfis de política

Perfis de política com o mesmo nome

Se houver duas políticas com o mesmo nome em diferentes níveis de hierarquia, essas funcionarão de acordo com as seguintes regras:

- As configurações bloqueadas e a condição de ativação de perfil de um perfil de política de nível superior alteram as configurações e a condição de ativação de perfil de um perfil de política de nível inferior (ver figura abaixo).



O perfil secundário herda os valores de configuração de um perfil de política principal

- As configurações desbloqueadas e a condição de ativação de perfil de um perfil de política de nível superior não alteram as configurações e a condição de ativação de perfil de um perfil de política de nível inferior.

Como as configurações são implementadas em um dispositivo gerenciado

A implementação eficaz de configurações em um dispositivo gerenciado pode ser descrita da seguinte forma:

- Os valores de todas as configurações não bloqueadas são obtidos a partir da política.
- Em seguida, são substituídos pelos valores das configurações do aplicativo gerenciado.
- Em seguida, os valores das configurações bloqueadas da política em vigor são aplicados. Os valores das configurações bloqueadas alteram os valores das configurações em vigor desbloqueadas.

Gerenciamento de políticas

Esta seção descreve o gerenciamento de políticas e fornece informações sobre como visualizar a lista de políticas, criar, modificar, copiar, mover políticas, sincronização forçada, visualizar o gráfico de status de distribuição de política e excluir uma política.

Visualização da lista de políticas

Você pode visualizar listas de políticas criadas para o Servidor de Administração ou para qualquer grupo de administração.

Para visualizar uma lista de políticas:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Na estrutura de grupos de administração, selecione o grupo de administração para o qual você deseja exibir a lista de políticas.

A lista de políticas aparece em formato tabular. Se não houver políticas, a tabela ficará vazia. Você pode mostrar ou ocultar as colunas da tabela, modificar a sua ordem, exibir apenas linhas que contenham um valor especificado ou usar a pesquisa.

Criação de uma política

Você pode criar políticas; pode também modificar e excluir as políticas existentes.

Para criar uma política:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Selecione o grupo de administração para o qual a política deve ser criada:
   - Para o grupo raiz.

     Neste caso, é necessário prosseguir para a próxima etapa.
   - Para um subgrupo:

     a. Clique no link do caminho atual na parte superior da janela.

     b. No painel aberto, clique no link com o nome do subgrupo necessário.

     O caminho atual muda para refletir o subgrupo selecionado.
3. Clique em **Adicionar**.

   A janela **Selecione o aplicativo** se abre.
4. Selecione o aplicativo para o qual você deseja criar uma política.
5. Clique em **Avançar**.

   A nova janela de configurações de política é exibida com a guia **Geral** selecionada.
6. Se quiser, altere o nome padrão, o status padrão e as configurações de herança padrão da política.
7. Selecione a guia **Configurações do aplicativo**.

   Ou você pode clicar em **Salvar** e sair. A política aparecerá na lista de políticas, e você poderá editar as suas configurações depois.

8. Na guia **Configurações do aplicativo**, no painel esquerdo, selecione a categoria desejada e, no painel de resultados à direita, edite as configurações da política. Você pode editar as configurações da política em cada categoria (seção).

   O conjunto de configurações depende do aplicativo para o qual você cria uma política. Para mais detalhes, consulte:

   - Configuração do Servidor de Administração
   - Configurações de política do Agente de Rede
   - Documentação do Kaspersky Endpoint Security for Windows

   Para detalhes sobre as configurações de outros aplicativos de segurança, consulte a documentação do aplicativo correspondente.

   Ao editar as configurações, você pode clicar em **Cancelar** para cancelar a última operação.

9. Clique em **Salvar** para salvar a política.

A política será exibida na lista de políticas.

Modificar uma política

Para modificar uma política:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique na política que deseja modificar.

   A janela Propriedades da política será aberta.

3. Especifique as configurações gerais e as configurações do aplicativo para o qual a política está sendo criada. Para mais detalhes, consulte:

   - Configuração do Servidor de Administração
   - Configurações de política do Agente de Rede
   - Documentação do Kaspersky Endpoint Security for Windows

   Para detalhes sobre as configurações de outros aplicativos de segurança, consulte a documentação desse aplicativo.

4. Clique em **Salvar**.

As alterações feitas à política serão salvas nas propriedades da política e aparecerão na seção **Histórico de revisões**.

Configurações da política gerais

Geral

Na guia **Geral**, você pode modificar o status da política e especificar a herança das configurações da política:

- No bloco **Status da política**, você poderá selecionar um dos modos de política:
  - Ativo

    Se esta opção estiver selecionada, a política é habilitada.

    Por padrão, esta opção está selecionada.

  - Fora do escritório

    Se esta opção estiver selecionada, a política se tornará ativa quando um dispositivo deixar a rede corporativa.

  - Inativo

    Se esta opção estiver selecionada, a política é habilitada, mas continua armazenada na pasta **Políticas**. Se necessário, a política pode ser habilitada.

- No grupo de configurações **Herança de configurações**, você pode configurar a herança de política:
  - Herdar configurações da política principal

    Se esta opção estiver ativada, os valores das configurações de política são herdados da política de grupo de nível superior e, portanto são bloqueados.

    Por padrão, esta opção está ativada.

  - Forçar herança de configurações nas políticas secundárias

    Se esta opção estiver ativada, após a aplicação das alterações da política, as seguintes ações serão realizadas:

    - Os valores das configurações da política serão propagados às políticas de subgrupos de administração, ou seja, às políticas secundárias.
    - No bloco **Herança de configurações** da seção **Geral** na janela Propriedades de cada política secundária, a opção **Herdar configurações da política principal** será automaticamente ativada.

    Se a opção estiver ativada, as configurações das políticas secundárias são bloqueadas.

    Por padrão, esta opção está desativada.

Configuração de eventos

Na guia **Configuração de eventos**, configure o registro e a notificação de eventos. Os eventos são distribuídos por nível de importância nas seguintes guias:

- **Crítico**

  A seção **Crítico** não é exibida nas propriedades de política do Agente de Rede.

- **Falha funcional**
- **Advertência**
- **Informações**

Na cada seção, a lista de eventos exibe os tipos de eventos e o prazo de armazenamento de eventos padrão no Servidor de Administração (em dias). Clicar em um tipo de evento permite especificar as seguintes configurações:

- **Registro de eventos**

  Você pode especificar por quantos dias armazenar o evento e selecionar onde armazená-lo:

  - **Exportar para o sistema SIEM usando o Syslog**
  - **Armazenar no log de eventos do SO no dispositivo**
  - **Armazenar no log de eventos do SO no Servidor de Administração**

- **Notificações de eventos**

  Você pode selecionar se deseja ser notificado sobre o evento de uma das seguintes formas:

  - **Notificar por e-mail**
  - **Notificar por SMS**
  - **Notificar ao executar o arquivo executável ou o script**
  - **Notificar via SNMP**

  Por padrão, as configurações de notificação especificadas na guia Propriedades do Servidor de Administração (como endereço do destinatário) são usadas. Se desejar, você pode alterar as configurações na guia **E-mail**, **SMS** e **Arquivo executável a ser executado**.

Histórico de revisões

A guia **Histórico de revisões** permite exibir a lista das revisões de política e reverter alterações feitas na política, se necessário.

Ativando o desativando uma opção de herança de política

Para ativar ou desativar a opção de herança em uma política:

1. Abra a política necessária.
2. Abra a guia **Geral**.
3. Ative ou desative a herança de política:
   - Se você ativar **Herdar configurações da política principal** em uma política secundária e um administrador bloquear algumas configurações na política principal, então você não poderá alterar essas configurações na política do grupo secundário.
   - Se você desativar **Herdar configurações da política principal** em uma política secundária, então você poderá alterar todas as configurações na política secundária, mesmo se algumas configurações estiverem bloqueadas na política principal.
   - Se você ativar **Forçar herança de configurações nas políticas secundárias** no grupo principal, isso ativará a opção **Herdar configurações da política principal** para cada política secundária. Nesse caso, você não pode desativar esta opção para nenhuma política secundária. Todas as configurações bloqueadas na política principal são herdadas por imposição nos grupos secundários, e você não pode alterar essas configurações nos grupos secundários.
4. Clique no botão **Salvar** para salvar as alterações ou clique no botão **Cancelar** para rejeitar as alterações.

Por padrão, a opção **Herdar configurações da política principal** está ativada para uma nova política.

Se uma política tiver perfis, todas as políticas secundárias herdarão esses perfis.

Cópia de uma política

Você pode copiar políticas de um grupo de administração para outro.

Para copiar uma política para outro grupo de administração:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Marque a caixa de seleção ao lado da política (ou políticas) que deseja copiar.
3. Clique no botão **Copiar**.

   No lado direito da tela, a árvore dos grupos de administração aparece.
4. Na árvore, selecione o grupo de destino, isto é, o grupo para o qual deseja copiar a política (ou políticas).
5. Clique no botão **Copiar** na parte inferior da tela.
6. Clique em **OK** para confirmar a operação.

A política (políticas) será copiada para o grupo de destino com todos os seus perfis. O status de cada política copiada no grupo de destino será **Inativo**. Você pode alterar o status para **Ativo** a qualquer momento.

Se uma política com um nome idêntico ao da política recém-movida já existir no grupo de destino, o nome da política recém-movida será expandido com o índice (<próximo número da sequência>), por exemplo: (1).

Mover uma política

Você pode mover políticas de um grupo de administração para outro. Por exemplo, você quer excluir um grupo, mas deseja usar as políticas dele para outro grupo. Nesse caso, você move a política do grupo antigo para o novo antes de excluir o antigo.

Para mover uma política para outro grupo de administração:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Marque a caixa de seleção ao lado da política (ou políticas) que deseja mover.
3. Clique no botão **Migrar**.

   No lado direito da tela, a árvore dos grupos de administração aparece.
4. Na árvore, selecione o grupo de destino, isto é, o grupo para o qual deseja mover a política (ou políticas).
5. Clique no botão **Migrar** na parte inferior da tela.
6. Clique em **OK** para confirmar a operação.

Caso uma política não seja herdada do grupo de origem, ela será movida para o grupo de destino com todos os seus perfis. O status da política no grupo de destino é **Inativo**. Você pode alterar o status para **Ativo** a qualquer momento.

Caso uma política seja herdada do grupo de origem, ela permanecerá no grupo de origem. Ela é copiada para o grupo de destino com todos os seus perfis. O status da política no grupo de destino é **Inativo**. Você pode alterar o status para **Ativo** a qualquer momento.

Se uma política com um nome idêntico ao da política recém-movida já existir no grupo de destino, o nome da política recém-movida será expandido com o índice (<próximo número da sequência>), por exemplo: (1).

Exportação de uma política

O Kaspersky Security Center permite salvar uma política, suas configurações e os perfis da política em um arquivo KLP. Você pode usar este arquivo KLP para importar a política salva tanto para o Kaspersky Security Center Windows quanto para o Kaspersky Security Center Linux.

Para exportar uma política:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Marque a caixa de seleção ao lado da política que deseja exportar.

   Você não pode exportar várias políticas ao mesmo tempo. Se selecionar mais de uma política, o botão **Exportar** será desabilitado.

3. Clique no botão **Exportar**.

4. Na janela **Salvar como** que abrir, especifique o nome e o caminho do arquivo de política. Clique no botão **Salvar**.

   A janela **Salvar como** é exibida apenas se você usar Google Chrome, Microsoft Edge ou Opera. Caso outro navegador seja usado, o arquivo da política será salvo automaticamente na pasta **Downloads**.

Importação de uma política

O Kaspersky Security Center permite importar uma política de um arquivo KLP. O arquivo KLP contém a política exportada, suas configurações e os perfis da política.

Para importar uma política:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.

2. Clique no botão **Importar**.

3. Clique no botão **Procurar** para escolher um arquivo de política que você deseja importar.

4. Na janela aberta, especifique o caminho para o arquivo de política KLP e clique no botão **Abrir**. Observe que você pode selecionar apenas um arquivo de política.

   O processamento da política é iniciado.

5. Após o processamento com êxito da política, selecione o grupo de administração ao qual deseja aplicar a política.

6. Clique no botão **Concluir** para encerrar a importação da política.

A notificação com os resultados da importação é exibida. Se a política for importada com êxito, você poderá clicar no link **Detalhes** para visualizar as propriedades da política.

Após a importação com êxito, a política será exibida na lista de políticas. As configurações e os perfis da política também são importados. Independentemente do status da política selecionada durante a exportação, a política importada está inativa. Você pode alterar o status da política nas propriedades da política.

Se a política recém-importada tiver um nome idêntico ao de uma política existente, o nome da política importada será expandido com o índice **(<próximo número da sequência>)**, por exemplo: **(1)**, **(2)**.

Visualizar o gráfico de status de distribuição da política

No Kaspersky Security Center, você pode ver o status de aplicação da política em cada dispositivo através de um gráfico de status de distribuição de política.

Para analisar o status de distribuição da política em cada dispositivo:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.

2. Marque a caixa de seleção ao lado da política para a qual deseja visualizar o status de distribuição nos dispositivos.

3. No menu exibido, selecione o link **Distribuição**.

   A janela **Resultados de distribuição <Nome da política>** é aberta.

4. Na janela aberta **Distribuição de resultados <Nome da política>** a **descrição do status** da política é exibida.

É possível alterar o número de resultados exibidos na lista com a distribuição da política. O número máximo de dispositivos é 100.000.

Para alterar o número de dispositivos exibidos na lista com os resultados de distribuição da política:

1. No menu principal, acesse as configurações da conta e selecione **Opções da interface**.

2. Em **Limite de dispositivos exibidos nos resultados da distribuição de políticas**, insira o número de dispositivos (até 100 mil).

   Por padrão, o número é 5.000.

3. Clique em **Salvar**.

   As configurações são salvas e aplicadas.

Exclusão de uma política

Você pode excluir uma política se não precisar mais dela. Você pode excluir apenas uma política que não é herdada no grupo de administração especificado. Se uma política for herdada, você só poderá exclui-la no grupo de nível superior para o qual ela foi criada.

Para excluir uma política:

1. No menu principal, vá para **Dispositivos → Políticas e perfis**.

2. Marque a caixa de seleção ao lado da política que deseja excluir e clique em **Excluir**.

   O botão **Excluir** ficará indisponível (esmaecido) se você selecionar uma política herdada.

3. Clique em **OK** para confirmar a operação.

A política é excluída em conjunto com todos os seus perfis.

Gerenciando perfis de política

Esta seção descreve o gerenciamento de perfis de política e fornece informações sobre como visualizá-los, alterar a prioridade, criar, modificar, copiar, criar uma regra de ativação e excluir perfis de política.

Visualização dos perfis de uma política

Para visualizar os perfis de uma política:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política cujos perfis deseja exibir.

   A janela de propriedades da política é exibida com a guia **Geral** selecionada.
3. Abra a guia **Perfis de política**.

A lista de perfis da política é exibida em formato tabular. Se a política não tiver perfis, uma tabela vazia será exibida.

Alteração de uma prioridade de perfil da política

Para alterar uma prioridade de perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.
2. Na guia **Perfis de política**, marque a caixa de seleção ao lado do perfil da política para o qual deseja alterar a prioridade.
3. Defina uma nova posição do perfil da política na lista clicando em **Priorizar** ou **Desspriorizar**.

   Quanto mais alto um perfil da política estiver localizado na lista, mais alta será sua prioridade.
4. Clique no botão **Salvar**.

A prioridade do perfil da política selecionado é alterada e aplicada.

Criar um perfil da política

Para criar um perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida. Se a política não tiver perfis, uma tabela vazia será exibida.
2. Clique em **Adicionar**.
3. Se quiser, altere o nome padrão e as configurações de herança padrão do perfil.
4. Selecione a guia **Configurações do aplicativo**.

   Ou então, é possível clicar em **Salvar** e sair. O perfil criado aparecerá na lista de perfis da política, e será possível editar as suas configurações depois.

5. Na guia **Configurações do aplicativo**, no painel esquerdo, selecione a categoria desejada e, no painel de resultados à direita, edite as configurações do perfil. Você pode editar as configurações do perfil da política em cada categoria (seção).

   Ao editar as configurações, você pode clicar em **Cancelar** para cancelar a última operação.

6. Clique em **Salvar** para salvar o perfil.

O perfil aparecerá na lista de perfis da política.

Modificar um perfil da política

A capacidade para editar um perfil da política somente está disponível para políticas do Kaspersky Endpoint Security for Windows.

Para modificar um perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.

2. Na guia **Perfis de política**, selecione o perfil da política que deseja modificar.

   A janela Propriedades do perfil da política será aberta.

3. Configure o perfil na janela de propriedades:

   - Se necessário, na guia **Geral**, altere o nome do perfil e ative ou desative o perfil.
   - Edite as regras de ativação de perfil.
   - Edite as configurações do aplicativo.

   Para detalhes sobre configurações de aplicativos de segurança, veja a documentação do aplicativo correspondente.

4. Clique em **Salvar**.

As configurações que você modificou serão aplicadas após o dispositivo ser sincronizado com o Servidor de Administração (se o perfil da política estiver ativo) ou após a regra de ativação ser acionada (se o perfil da política estiver inativo).

Copiar um perfil de política

Você pode copiar um perfil da política para política atual ou outra, por exemplo, se quiser ter perfis idênticos para políticas diferentes. Você também pode usar a cópia se quiser ter dois ou mais perfis que se diferenciam em apenas um pequeno número de configurações.

Para copiar um perfil de política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida. Se a política não tiver perfis, uma tabela vazia será exibida.

2. Na guia **Perfis de política**, selecione o perfil da política que deseja copiar.

3. Clique em **Copiar**.

4. Na janela exibida, selecione a política para a qual deseja copiar o perfil.

   É possível copiar um perfil da política para a mesma política ou uma política que você especificar.

5. Clique em **Copiar**.

   O perfil da política é copiado para a política que você selecionou. O perfil recentemente copiado adquire a prioridade mais baixa. Se você copiar o perfil para a mesma política, o nome do perfil recentemente copiado será expandido com o índice (), por exemplo: (1), (2).

Depois, você pode modificar as configurações do perfil, inclusive o nome e a prioridade dele; o perfil da política original não será modificado nesse caso.

Criar uma regra de ativação do perfil da política

Para criar uma regra de ativação do perfil da política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.

2. Na guia **Perfis de política**, clique no perfil da política para o qual é preciso criar uma regra de ativação.

   Se a lista de perfis da política estiver vazia, você pode criar um perfil da política.

3. Na guia **Regras de ativação**, clique no botão **Adicionar**.

   A janela com as regras de ativação do perfil da política é aberta.

4. Especifique um nome para a regra.

5. Selecione as caixas junto as condições que devem afetar a ativação do perfil da política que você estiver criando:

- Regras gerais para a ativação do perfil de política

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo do status do modo offline de dispositivo, a regra para a conexão ao Servidor de Administração e as tags atribuídas ao dispositivo.

  Para esta opção, especifique na etapa seguinte:

  - Status do dispositivo

    Define a condição da presença do dispositivo na rede:

    - **Online** – O dispositivo está na rede, portanto o Servidor de Administração está disponível.
    - **Offline** – O dispositivo está em uma rede externa, o que significa que o Servidor de Administração não está disponível.
    - **N/A** – O critério não será aplicado.

  - A regra para conexão do Servidor de Administração está ativa neste dispositivo

    Escolha a condição de ativação do perfil da política (se a regra está ou não sendo executada) e selecione o nome da regra.

    A regra define o local de rede do dispositivo para conexão ao Servidor de Administração, cujas condições devem ser atendidas (ou não devem ser atendidas) para a ativação do perfil da política.

    Uma descrição da localização da rede de dispositivos para conexão a um Servidor de Administração pode ser criada ou configurada em uma regra de troca de Agente de Rede.

- **Regras para o proprietário do dispositivo específico**

  Para esta opção, especifique na etapa seguinte:

  - Proprietário do dispositivo

    Ative esta opção para configurar e ativar a regra para a ativação do perfil no dispositivo para seu proprietário. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

    - O dispositivo pertence ao proprietário especificado (sinal "=").
    - O dispositivo não pertence ao proprietário especificado (sinal "#").

      Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o proprietário do dispositivo se a opção estiver ativada. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

  - O proprietário do dispositivo está incluído em um grupo de segurança interno

Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pela associação do proprietário em um grupo de segurança interna do Kaspersky Security Center. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

- O proprietário do dispositivo é um membro do grupo de segurança especificado (sinal "=").
- O proprietário do dispositivo não é um membro do grupo de segurança especificado (sinal "#").

  Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar um grupo de segurança do Kaspersky Security Center. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- Regras para especificações de hardware

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo do volume de memória e do número de processadores lógicos.

  Para esta opção, especifique na etapa seguinte:

  - Tamanho da RAM, em MB

    Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pelo volume de RAM disponível naquele dispositivo. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

    - O tamanho da RAM do dispositivo é menos do que o valor especificado (sinal "<").
    - O tamanho de RAM de dispositivo é maior do que o valor especificado (sinal ">").

    Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o volume da RAM no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

  - Número de processadores lógicos

    Ative esta opção para configurar e ativar a regra de ativação do perfil no dispositivo pelo número de processadores lógicos nesse dispositivo. Na lista suspensa sob esta caixa de seleção, você pode selecionar um critério para a ativação do perfil:

    - O número de processadores lógicos no dispositivo é menor do que ou igual ao valor especificado (sinal "<").
    - O número de processadores lógicos no dispositivo é maior do que ou igual ao valor especificado (sinal ">").

    Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados. Você pode especificar o número de processadores lógicos no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- **Regras para atribuição de funções**

  Para esta opção, especifique na etapa seguinte:

  Ativar o perfil de política por função específica do proprietário do dispositivo

Selecione esta opção para configurar e ativar a regra da ativação do perfil no dispositivo, dependendo da função do proprietário. Adicione a função manualmente da lista de funções existentes.

Se essa opção é ativada, o perfil é ativado no dispositivo de acordo com os critérios especificados.

- **Regras para uso de tag**

  Marque esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo das tags atribuídas ao dispositivo. Você pode ativar o perfil da política para os dispositivos com ou sem tags selecionadas.

  Para esta opção, especifique na etapa seguinte:

  - **Tag**

    Na lista de tags, especifique uma regra para a inclusão do dispositivo no perfil da política, selecionando as caixas de seleção ao lado das tags relevantes.

    Você pode adicionar novas tags à lista inserindo-as no campo sobre a lista e clicando no botão **Adicionar**.

    O perfil da política inclui dispositivos com descrições que contêm todas as tags selecionadas. Se as caixas de seleção forem desmarcadas, o critério não é aplicado. Por padrão, estas caixas de seleção estão desmarcadas.

  - **Aplicar aos dispositivos sem tags especificadas**

    Ative esta opção se tiver de inverter a seleção de tags.

    Se esta opção estiver selecionada, o perfil da política inclui dispositivos com descrições que não contêm nenhuma das tags selecionadas. Se esta opção estiver desativada, o critério não é aplicado.

    Por padrão, esta opção está desativada.

- **Regras para uso do Active Directory**

  Selecione esta caixa de seleção para definir as regras de ativação do perfil da política no dispositivo dependendo da presença do dispositivo em uma unidade organizacional (UO) do Active Directory ou em uma associação do dispositivo (ou seu proprietário) em um grupo de segurança do Active Directory.

  Para esta opção, especifique na etapa seguinte:

  - **Associação do proprietário do dispositivo no grupo de segurança do Active Directory**

    Se esta opção estiver ativada, o perfil da política será ativado no dispositivo cujo proprietário for um membro do grupo de segurança especificado. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

  - **Associação do dispositivo no grupo de segurança do Active Directory**

Se esta opção estiver ativada, o perfil da política será ativado no dispositivo. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado. Por padrão, esta opção está desativada.

- A alocação do dispositivo está na unidade organizacional do Active Directory

  Se esta opção estiver ativada, o perfil da política será ativado no dispositivo que estiver incluído na unidade organizacional (OU) do Active Directory especificada. Se essa opção estiver desativada, o critério de ativação do perfil não é aplicado.

  Por padrão, esta opção está desativada.

O número de páginas adicionais do assistente depende das configurações que você seleciona no primeiro passo. Você pode modificar as regras de ativação do perfil da política em outro momento.

6. Verifique a lista dos parâmetros configurados. Se a lista estiver correta, clique em **Criar**.

O perfil será salvo. O perfil será ativado no dispositivo quando as regras de ativação forem acionadas.

As regras de ativação do perfil da política criadas para o perfil são exibidas nas propriedades do perfil da política na guia **Regras de ativação**. Você pode modificar ou remover qualquer regra de ativação do perfil da política.

Múltiplas regras de ativação podem ser acionadas simultaneamente.

Excluir um perfil de política

Para excluir um perfil de política:

1. Prossiga para a lista de perfis de uma política desejada.

   A lista de perfis de política é exibida.

2. Na guia **Perfis de política**, marque a caixa de seleção ao lado do perfil de política que deseja excluir e clique em **Excluir**.

3. Na janela exibida, clique em **Excluir** novamente.

O perfil da política é excluído. Se a política for herdada por um grupo de nível mais baixo, o perfil permanecerá nesse grupo, mas se tornará o perfil da política desse grupo. Isso é feito para eliminar a alteração significativa nas configurações dos aplicativos gerenciados instalados nos dispositivos de grupos de nível mais baixo.

Criptografia e proteção de dados

A criptografia de dados reduz o risco de vazamentos não intencionais, caso seu laptop ou disco rígido seja roubado ou perdido, ou por acesso não autorizado por usuários e aplicativos.

Os seguintes aplicativos da Kaspersky são compatíveis com criptografia:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Mac

Você pode mostrar ou ocultar alguns dos elementos da interface relacionados ao recurso de gerenciamento de criptografia usando as configurações da interface do usuário.

Não recomendamos ativar a criptografia na VDI.

Criptografia de dados no Kaspersky Endpoint Security for Windows

É possível gerenciar os seguintes tipos de criptografia:

- Criptografia de unidade de disco BitLocker em dispositivos que executam um sistema operacional Windows para servidores
- Criptografia de unidade de disco Kaspersky em dispositivos que executam um sistema operacional Windows para estações de trabalho

Ao usar esses componentes do Kaspersky Endpoint Security for Windows, é possível, por exemplo, ativar ou desativar a criptografia, visualizar a lista de unidades criptografadas ou gerar e visualizar relatórios sobre criptografia.

Configure a criptografia definindo as políticas do Kaspersky Endpoint Security for Windows no Kaspersky Security Center. O Kaspersky Endpoint Security for Windows executa a criptografia e a descriptografia de acordo com a política ativa em vigor. Para obter instruções detalhadas sobre como configurar regras e uma descrição dos recursos de criptografia, veja a Ajuda do Kaspersky Endpoint Security for Windows.

Criptografia de dados no Kaspersky Endpoint Security for Mac

Você pode usar a criptografia FileVault em dispositivos que executam macOS. Ao trabalhar com o Kaspersky Endpoint Security for Mac, você pode ativar ou desativar essa criptografia.

Configure a criptografia definindo as políticas do Kaspersky Endpoint Security for Mac no Kaspersky Security Center. O Kaspersky Endpoint Security for Mac executa a criptografia e a descriptografia de acordo com a política ativa em vigor. Para obter uma descrição detalhada sobre os recursos de criptografia, veja a Ajuda do Kaspersky Endpoint Security for Mac.

Visualização da lista de unidades criptografadas

No Kaspersky Security Center, é possível visualizar detalhes sobre unidades criptografadas e dispositivos criptografados no nível da unidade. Após as informações de uma unidade serem descriptografadas, a unidade é automaticamente removida da lista.

Para exibir a lista de unidades criptografadas,

No menu principal, vá para **Operações** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.

Se a seção não estiver no menu, isso significa que ela está oculta. Nas configurações da interface do usuário, habilite a opção **Mostrar a criptografia e proteção de dados** para exibir a seção.

É possível exportar a lista de unidades criptografadas para um arquivo CSV ou TXT. Para fazer isso, clique no botão **Exportar linhas para arquivo CSV** ou **Exportar linhas para arquivo TXT**.

Visualização da lista de eventos de criptografia

Ao executar tarefas de criptografia ou descriptografia de dados nos dispositivos, o Kaspersky Endpoint Security for Windows envia ao Kaspersky Security Center informações sobre os eventos dos seguintes tipos:

- Não é possível criptografar ou descriptografar um arquivo, ou criar um arquivo criptografado devido à falta de espaço livre em disco.
- Não é possível criptografar ou descriptografar um arquivo, ou criar um arquivo criptografado devido a problemas com a licença.
- Não é possível criptografar ou descriptografar um arquivo, ou criar um arquivo criptografado devido à ausência de direitos de acesso.
- O aplicativo foi proibido de acessar um arquivo criptografado.
- Erros desconhecidos.

Para exibir uma lista de eventos que ocorreram durante a criptografia de dados nos dispositivos,

No menu principal, vá para **Operações → Criptografia e proteção de dados → Eventos de criptografia**.

Se a seção não estiver no menu, isso significa que ela está oculta. Nas configurações da interface do usuário, habilite a opção **Mostrar a criptografia e proteção de dados** para exibir a seção.

É possível exportar a lista de unidades criptografadas para um arquivo CSV ou TXT. Para fazer isso, clique no botão **Exportar linhas para arquivo CSV** ou **Exportar linhas para arquivo TXT**.

Como alternativa, você pode examinar a lista de eventos de criptografia para cada dispositivo gerenciado.

Para visualizar os eventos de criptografia de um dispositivo gerenciado:

1. No menu principal, vá para **Dispositivos → Dispositivos gerenciados**.
2. Clique no nome de um dispositivo gerenciado.
3. Na guia **Geral**, vá para a seção **Proteção**.
4. Clique no link **Exibir erros de criptografia de dados**.

Criação e visualização de relatórios de criptografia

É possível gerar os seguintes relatórios:

- Relatório de status da criptografia dos dispositivos gerenciados. Este relatório fornece detalhes sobre a criptografia de dados de vários dispositivos gerenciados. Por exemplo, o relatório mostra o número de dispositivos aos quais a política com regras de criptografia configuradas se aplica. Além disso, você pode descobrir, por exemplo, quantos dispositivos precisam ser reinicializados. Ele também contém informações sobre a tecnologia de criptografia e o algoritmo para cada dispositivo.

- Relatório de status da criptografia dos dispositivos de armazenamento em massa. Este relatório contém informações semelhantes ao relatório sobre o status de criptografia de dispositivos gerenciados, mas fornece dados apenas para dispositivos de armazenamento em massa e unidades removíveis.

- Relatório de direitos de acesso aos dispositivos criptografados. Este relatório mostra quais contas de usuário têm acesso a unidades criptografadas.

- Relatório de erros na criptografia de arquivos. Este relatório contém informações sobre os erros que ocorreram ao executar as tarefas de criptografia ou a descriptografia dos dados nos dispositivos.

- Relatório de bloqueio de acesso aos arquivos criptografados. Este relatório contém informações sobre como bloquear o acesso dos aplicativos aos arquivos criptografados. Este relatório será útil se um usuário ou aplicativo não autorizado tentar acessar arquivos ou unidades criptografadas.

É possível gerar qualquer relatório na seção **Monitoramento e relatórios** → **Relatórios**. Alternativamente, na seção **Operações** → **Criptografia e proteção de dados**, você pode gerar os seguintes relatórios de criptografia:

- Relatório de status da criptografia dos dispositivos de armazenamento em massa

- Relatório de direitos de acesso aos dispositivos criptografados

- Relatório de erros na criptografia de arquivos

*Para gerar um relatório de criptografia na seção **Criptografia e proteção de dados**:*

1. Certifique-se de ter ativado a opção **Mostrar a criptografia e proteção de dados** nas opções de interface.

2. Nas propriedades da política, abra a guia **Configuração de eventos**.

3. Na seção **Crítico**, clique em **Adicionar evento** e marque a caixa de seleção ao lado do evento *Erro na aplicação das regras de criptografia/descriptografia do arquivo*.

4. Clique em **OK**.

5. No menu principal, vá para **Operações** → **Criptografia e proteção de dados**.

6. Abra uma das seguintes seções:

   - **Dispositivos criptografados** gera o relatório sobre o status de criptografia de status de dispositivos de armazenamento em massa ou o relatório sobre direitos de acesso a unidades criptografadas.
   - **Eventos de criptografia** gera o relatório sobre erros de criptografia de arquivo.

7. Clique no nome do relatório que deseja gerar.

A geração do relatório começa.

Concessão de acesso a uma unidade criptografada no modo offline

Um usuário pode solicitar acesso a um dispositivo criptografado, por exemplo, quando o Kaspersky Endpoint Security for Windows não estiver instalado no dispositivo gerenciado. Depois que você receber a solicitação, poderá criar um arquivo de chave de acesso e enviá-lo ao usuário. Todos os casos de uso e instruções detalhadas são fornecidas na Ajuda do Kaspersky Endpoint Security for Windows.

Para conceder acesso a uma unidade criptografada no modo offline:

1. Obtenha um arquivo de solicitação de acesso de um usuário (com a extensão FDERTC). Siga as instruções da Ajuda do Kaspersky Endpoint Security for Windows para gerar o arquivo no Kaspersky Endpoint Security for Windows.
2. No menu principal, vá para **Operações** → **Criptografia e proteção de dados** → **Dispositivos criptografados**.

   Uma lista de unidades criptografadas é exibida.
3. Selecione a unidade à qual o usuário solicitou acesso.
4. Clique no botão **Permitir acesso ao dispositivo em modo offline**.
5. Na janela que se abre, selecione o plug-in correspondente ao aplicativo da Kaspersky usado para criptografar a unidade selecionada.

   > Se uma unidade estiver criptografada com um aplicativo Kaspersky incompatível com o Kaspersky Security Center Web Console, use o Console de Administração baseado no Console de Gerenciamento Microsoft para conceder o acesso offline.

6. Siga as instruções fornecidas na Ajuda do Kaspersky Endpoint Security for Windows (veja os blocos de expansão no final da seção).

Depois disso, o usuário aplica o arquivo recebido para acessar a unidade criptografada e ler os dados armazenados na unidade.

Usuários e funções dos usuários

Esta seção descreve usuários e funções de usuário e fornece instruções para criá-los e modificá-los, atribuir funções e grupos a usuários e associar perfis de política a funções.

Sobre as funções dos usuários

A *função de usuário* (também mencionada como uma *função*) é um objeto que contém um conjunto de direitos e privilégios. Uma função pode ser associada às configurações de aplicativos da Kaspersky instalados em um dispositivo de usuário. É possível atribuir uma função a um conjunto de usuários ou a um conjunto de grupos de segurança em qualquer nível na hierarquia de grupos de administração, Servidores de Administração, ou em nível de objetos específicos.

Caso gerencie dispositivos por meio de uma hierarquia de Servidores de Administração, a qual inclui Servidores de Administração virtuais, observe que é possível criar, modificar ou excluir as funções de usuário somente do Servidor de Administração físico. Em seguida, é possível propagar as funções do usuário para os Servidores de Administração secundários, incluindo os virtuais.

Você pode associar funções de usuário a perfis da política. Se uma função for atribuída a um usuário, esse usuário receberá as configurações de segurança necessárias para desempenhar suas funções profissionais.

Uma função de usuário pode ser associada a usuários de dispositivos em um grupo de administração específico.

Escopo da função do usuário

O *escopo da função do usuário* é uma combinação de usuários e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

Vantagem de usar funções

Uma vantagem de usar funções é que você não precisa especificar configurações de segurança para cada um dos dispositivos gerenciados ou cada um dos usuários separadamente. O número de usuários e dispositivos em uma empresa pode ser bastante grande, mas o número de funções de trabalho diferentes que necessitam de configurações de segurança diferentes é consideravelmente menor.

Diferenças do uso de perfis da política

Os perfis da política são as propriedades da política criada para cada aplicativo da Kaspersky separadamente. Uma função é associada a muitos perfis de política criados para aplicativos diferentes. Por isso, a função é um método da união de configurações para um determinado tipo de usuário em um lugar.

Visualização de contas de usuário e sessões

O Kaspersky Security Center lhe permite gerenciar contas de usuário e grupos de contas. O aplicativo é compatível com dois tipos de contas:

- Contas dos funcionários da organização. O Servidor de Administração obtém dados das contas desses usuários ao amostrar a rede da organização.
- Contas de usuários internos. Estas contas são aplicadas quando os Servidores de Administração virtuais são usados. As contas de usuários internos são criadas e usadas somente dentro do Kaspersky Security Center.

É possível visualizar a lista de contas de usuário e sessões por meio de uma das seguintes formas:

- No menu principal, vá para **Usuários e funções** → **Usuários**.
- No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados** → link <nome do dispositivo> → guia **Geral** → seção **Geral** → bloco **Sessões**.

  A seção **Sessões** exibe contas de usuários com sessões ativas em dispositivos que executam Windows.

A lista de contas de usuário e sessões será exibida corretamente caso os seguintes requisitos sejam atendidos:

- Use o Agente de Rede da mesma versão ou uma posterior à do Servidor de Administração.
- A sondagem do Active Directory está ativada para exibir as contas dos usuários do domínio.
- Em dispositivos gerenciados que executam o Windows, o serviço **Server** (**LanmanServer**) está em execução.

Configurar direitos de acesso aos recursos do aplicativo. Controle de acesso baseado em função

O Kaspersky Security Center fornece meios de acesso baseado em função para os recursos do Kaspersky Security Center e aplicativos gerenciados da Kaspersky.

Você pode configurar os direitos de acesso aos recursos do aplicativo para usuários do Kaspersky Security Center de uma das seguintes maneiras:

- Configurando os direitos para cada usuário ou grupo de usuários individualmente.
- Criando funções de usuário padrão com um conjunto predefinido de direitos e atribuindo tais funções aos usuários dependendo do escopo de obrigações deles.

A aplicação de funções de usuário tem como objetivo simplificar e reduzir os procedimentos de rotina de configuração de direitos de acesso dos usuários aos recursos do aplicativo. Os direitos de acesso com em uma função são configurados de acordo com as tarefas "padrão" e o escopo de deveres do usuário.

As funções de usuários podem ter nomes que correspondem a suas finalidades respetivas. Você pode criar um número ilimitado de funções no aplicativo.

É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado ou criar novas funções e configurar os direitos necessários por conta própria.

Direitos de acesso aos recursos do aplicativo

A tabela abaixo mostra os recursos do Kaspersky Security Center com os direitos de acesso para gerenciar as tarefas, relatórios e configurações associadas, bem como executar as ações do usuário associadas.

Para executar as ações do usuário listadas na tabela, o usuário deve ter o direito especificado ao lado da ação.

Os direitos de **Leitura**, **Gravar** e **Executar** são aplicáveis a qualquer tarefa, relatório ou configuração. Além desses direitos, o usuário precisa ter o direito de **Executar as operações nas seleções de dispositivos** para gerenciar tarefas, relatórios ou configurações nas seleções de dispositivos.

> Todas as tarefas, relatórios, configurações e pacotes de instalação que não constam na tabela pertencem à área funcional **Funcionalidades gerais: Funcionalidade básica**.

Direitos de acesso aos recursos do aplicativo

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: **Gerenciamento de grupos de administração**	**Gravar**	• Adicionar o dispositivo a um grupo de administração: **Gravar** • Excluir o dispositivo de um grupo de administração: **Gravar** • Adicionar um grupo de administração a outro grupo de administração: **Gravar** • Excluir um grupo de administração de outro grupo de administração: **Gravar**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: **Acessar objetos independentemente de suas ACLs**	**Ler**	Obter acesso de Ler a todos os objetos: **Ler**	Nenhum	Nenhum	A área funcional **Funcionalidades gerais: Acessar objetos independentemente de suas ACLs** destina-se a fins de auditoria. Quando os usuários recebem direitos de **Ler** nesta área funcional, eles obtêm acesso total de **Ler** a todos os objetos e podem executar quaisquer tarefas criadas em seleções de dispositivos conectados ao Servidor de Administração por meio do Agente de Rede com direitos de administrador local (root no Linux). Recomendamos conceder esses direitos com cuidado e a um conjunto limitado de usuários que precisam deles para desempenhar suas funções oficiais. O acesso é concedido independentemente de outros direitos, mesmo que estes proíbam o acesso de Ler a objetos específicos.

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: **Funcionalidade básica**	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Regras de movimentação de dispositivos (criar, modificar ou excluir) para o servidor virtual: **Gravar**, **Executar as operações nas seleções de dispositivos** • Obter um certificado personalizado para o Protocolo móvel (LWNGT): **Ler** • Configurar o certificado personalizado para o Protocolo móvel (LWNGT): **Gravar** • Obter a lista de redes definidas pela NLA: **Ler** • Adicionar, modificar ou excluir a lista de redes definidas por NLA: **Gravar** • Exibir a Lista de controle de acesso dos grupos: **Ler** • Visualizar o Log de eventos da Kaspersky: **Ler** • Visualizar a chave de recuperação para restaurar o acesso a um disco rígido criptografado pelo BitLocker: **Executar**	• "Baixar atualizações no repositório do Servidor de Administração" • "Entregar relatórios" • "Distribuir pacote de instalação" • "Instalar aplicativos nos Servidores de Administração secundários remotamente"	• "Relatório do status de proteção" • "Relatório de ameaças" • "Relatório de dispositivos mais infectados" • "Relatório de status dos bancos de dados antivírus" • "Relatório de erros" • "Relatório de ataques de rede" • "Relatório resumido de aplicativos de proteção do sistema de e-mail instalados" • "Relatório resumido de aplicativos de defesa de perímetro instalados" • "Relatório resumido dos tipos de aplicativos instalados" • "Relatório de usuários de dispositivos infectados" • "Relatório de incidentes" • "Relatório de eventos" • "Relatório de atividade dos pontos de distribuição" • "Relatório de Servidores de Administração secundários" • "Relatório de eventos de Controle de Dispositivos" • "Relatório de vulnerabilidades" • "Relatório de aplicativos proibidos" • "Relatório de Controle da Web" • "Relatório de status da criptografia de	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
				dispositivos gerenciados" • "Relatório de status da criptografia de dispositivos de armazenamento em massa" • "Relatório de erros de criptografia de arquivos" • "Relatório de bloqueio de acesso a dispositivos criptografados" • "Relatório de direitos de acesso a dispositivos criptografados" • "Relatório de permissões do usuário em vigor" • "Relatório de direitos"	
Funcionalidades gerais: **Objetos excluídos**	• **Ler** • **Gravar**	• Visualizar objetos excluídos na Lixeira: **Ler** • Excluir objetos da Lixeira: **Gravar**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: **Processamento de eventos**	• **Excluir eventos** • **Editar as configurações de notificação de eventos** • **Editar as configurações de log de eventos** • **Gravar**	• Alterar as configurações de registro de eventos: **Editar as configurações de log de eventos** • Alterar configurações de notificação de eventos: **Editar as configurações de notificação de eventos** • Excluir eventos: **Excluir eventos**	Nenhum	Nenhum	Configurações: • Configurações de ataque de vírus: número de detecções de vírus necessárias para criar um evento de ataque de vírus • Configurações de ataque de vírus: período de tempo para avaliação das detecções de vírus • O número máximo de eventos armazenados no banco de dados • Período de tempo para armazenar eventos dos dispositivos excluídos

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: Operações no Servidor de administração	• **Ler** • **Gravar** • **Executar** • **Modificar os objetos ACLs** • **Executar as operações nas seleções de dispositivos**	• Especificar as portas do Servidor de Administração para a conexão do Agente de Rede: **Gravar** • Especificar as portas do Proxy de ativação iniciado no Servidor de Administração: **Gravar** • Especificar as portas do Proxy de ativação para dispositivos móveis iniciadas no Servidor de Administração: **Gravar** • Especificar as portas do Servidor Web para distribuição de pacotes independentes: **Gravar** • Especificar as portas do Servidor Web para distribuição de perfis MDM: **Gravar** • Especificar as portas SSL do Servidor de Administração para a conexão pelo Kaspersky Security Center Web Console: **Gravar** • Especificar as portas do Servidor de Administração para a conexão móvel: **Gravar** • Especificar o número máximo de eventos armazenados no banco de dados do Servidor de Administração: **Gravar** • Especificar o número máximo de eventos que podem ser enviados pelo Servidor de Administração: **Gravar** • Especificar o período de tempo durante o qual os eventos podem ser enviados pelo Servidor de Administração: **Gravar**	• "Backup de dados do Servidor de Administração" • "Manutenção do banco de dados"	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: **Implementação do software da Kaspersky**	• **Gerenciar patches da Kaspersky** • **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	Aprovar ou rejeitar a instalação do patch: **Gerenciar patches da Kaspersky**	Nenhum	• "Relatório de uso da chave de licença pelo Servidor de Administração virtual" • "Relatório de versões de software da Kaspersky" • "Relatório de aplicativos incompatíveis" • "Relatório de versões das atualizações dos módulos de software da Kaspersky" • "Relatório de implementação da proteção"	Pacote de instalação: "Kaspersky"
Funcionalidades gerais: **Gerenciamento de chaves de licença**	• **Exportar arquivo de chave** • **Gravar**	• Exportar arquivo de chave: **Exportar arquivo de chave** • Modificar as configurações da chave de licença do Servidor de Administração: **Gravar**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: **Gerenciamento de relatórios forçado**	• **Ler** • **Gravar**	• Criar relatórios independentemente das suas ACLs: **Gravar** • Executar relatórios independentemente de suas ACLs: **Ler**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: **Hierarquia de Servidores de Administração**	**Configurar a hierarquia de Servidores de Administração**	Registrar, atualizar ou excluir Servidores de Administração secundários: **Configurar a hierarquia de Servidores de Administração**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Funcionalidades gerais: **Permissões do usuário**	**Modificar os objetos ACLs**	• Alterar as Propriedades de segurança de qualquer objeto: **Modificar os objetos ACLs** • Gerenciar funções de usuário: **Modificar os objetos ACLs** • Gerenciar usuários internos: **Modificar os objetos ACLs** • Gerenciar grupos de segurança: **Modificar os objetos ACLs** • Gerenciar aliases: **Modificar os objetos ACLs**	Nenhum	Nenhum	Nenhum
Funcionalidades gerais: **Servidores de Administração virtuais**	• **Gerenciar Servidores de Administração virtuais** • **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Obter a lista de Servidores de Administração virtuais: **Ler** • Obter informações sobre o Servidor de Administração virtual: **Ler** • Criar, atualizar ou excluir um Servidor de Administração virtual: **Gerenciar Servidores de Administração virtuais** • Mover um Servidor de Administração virtual para outro grupo: **Gerenciar Servidores de Administração virtuais** • Definir permissões do Servidor de Administração virtual: **Gerenciar Servidores de Administração virtuais**	Nenhum	"Relatório de resultados da instalação de atualizações de software de terceiros"	Nenhum
Funcionalidades gerais: **Gerenciamento de chaves de criptografia**	**Gravar**	Importar as chaves de criptografia: **Gravar**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Gerenciamento de Dispositivos Móveis: Geral	• **Conectar novos dispositivos** • **Enviar somente comandos de informações para dispositivos móveis** • **Enviar comandos para dispositivos móveis** • **Gerenciar certificados** • **Ler** • **Gravar**	• Obter os dados de restauração do Serviço de gerenciamento de chaves: **Ler** • Excluir os certificados de usuário: **Gerenciar certificados** • Obter a parte pública do certificado do usuário: **Ler** • Verificar se a Infraestrutura de chave pública está ativada: **Ler** • Verificar a conta da Infraestrutura de chave pública: **Ler** • Obter modelos de Infraestrutura de chave pública: **Ler** • Obter modelos de Infraestrutura de chave pública por meio do certificado de Uso de chave estendido: **Ler** • Verificar se o certificado da Infraestrutura de chave pública foi revogado: **Ler** • Atualizar as configurações de emissão de certificado do usuário: **Gerenciar certificados** • Obter as configurações de emissão de certificado do usuário: **Ler** • Obter pacotes pelo nome e versão do aplicativo: **Ler** • Definir ou cancelar o certificado do usuário: **Gerenciar certificados** • Renovar o certificado do usuário: **Gerenciar certificados** • Definir etiqueta de certificado do usuário: **Gerenciar certificados** • Executar a geração do pacote de instalação do MDM; cancelar a geração do pacote de instalação do MDM: **Conectar novos dispositivos**	Nenhum	Nenhum	Nenhum

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Gerenciamento do sistema: Conectividade	• **Iniciar sessões RDP** • **Conexão para sessões RDP existentes** • **Iniciar túnel** • **Salvar os arquivos dos dispositivos na estação de trabalho do administrador** • **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Criar sessão de compartilhamento da área de trabalho: **Iniciar sessões RDP** • Criar sessão RDP: **Conexão para sessões RDP existentes** • Criar túnel: **Iniciar túnel** • Salvar a lista de conteúdo da rede: **Salvar os arquivos dos dispositivos na estação de trabalho do administrador**	Nenhum	"Relatório de usuários dos dispositivos"	Nenhum
Gerenciamento do sistema: Inventário de hardware	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Obter ou exportar objeto de inventário de hardware: **Ler** • Adicionar, definir ou excluir objeto de inventário de hardware: **Gravar**	Nenhum	• "Relatório do registro de hardware" • "Relatório de alterações de configuração" • "Relatório de hardware"	Nenhum
Gerenciamento do sistema: Controle de Acesso de Rede	• **Ler** • **Gravar**	• Visualizar configurações da CISCO: **Ler** • Alterar configurações da CISCO: **Gravar**	Nenhum	Nenhum	Nenhum
Gerenciamento do sistema: Implementação do sistema operacional	• **Implementar servidores PXE** • **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Implementar servidores PXE: **Implementar servidores PXE** • Visualizar uma lista de servidores PXE: **Ler** • Iniciar ou interromper o processo de instalação em clientes PXE: **Executar** • Gerenciar drivers para WinPE e imagens de sistema operacional: **Gravar**	"Criar pacote de instalação mediante imagem do SO do dispositivo de referência"	Nenhum	Pacote de instalação: "Imagem do SO"

Área funcional	Direito	Ação do usuário: são necessários direitos para executar a ação	Tarefa	Relatório	Outro
Gerenciamento do sistema: Gerenciamento de Patches e Vulnerabilidades	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Visualizar propriedades de patches de terceiros: **Ler** • Alterar propriedades de patches de terceiros: **Gravar**	• "Executar a sincronização com o Windows Update" • "Instalar atualizações do Windows Update" • "Corrigir vulnerabilidades" • "Instalar as atualizações necessárias e corrigir vulnerabilidades"	"Relatório de atualizações de software"	Nenhum
Gerenciamento do sistema: Instalação remota	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	• Visualizar as propriedades do pacote de instalação de terceiros com base no Gerenciamento de vulnerabilidades e patches: **Ler** • Alterar as propriedades do pacote de instalação de terceiros com base no Gerenciamento de vulnerabilidades e patches: **Gravar**	Nenhum	Nenhum	Pacotes de instalação: • "Aplicativo personalizado" • "Pacote VAPM"
Gerenciamento do sistema: Inventário de software	• **Ler** • **Gravar** • **Executar** • **Executar as operações nas seleções de dispositivos**	Nenhum	Nenhum	• "Relatório de aplicativos instalados" • "Relatório do histórico de registro de aplicativos" • "Relatório de status dos grupos de aplicativos licenciados" • "Relatório de chaves de licença de software de terceiros"	Nenhum

Funções de usuário predefinidas

As funções de usuário atribuídas aos usuários do Kaspersky Security Center fornecem conjuntos de direitos de acesso aos recursos do aplicativo.

Os usuários criados em um servidor virtual não podem receber uma função no Servidor de Administração.

É possível usar as funções de usuário predefinidas com um conjunto de direitos já configurado ou criar novas funções. Ao criar uma nova função, defina o escopo da função e atribua os direitos de acessibilidade aos recursos do Kaspersky Security Center manualmente. Algumas das funções de usuário predefinidas disponíveis no Kaspersky Security Center podem ser associadas a cargos específicos, por exemplo, **Auditor**, **Diretor de segurança**, **Supervisor** (essas funções estão presentes no Kaspersky Security Center a partir da versão 11). Os direitos de acesso dessas funções são pré-configurados de acordo com as tarefas padrão e o escopo das obrigações dos cargos associados. A tabela abaixo mostra como as funções podem ser associadas a cargos específicos.

Exemplos de funções para cargos específicos

Função	Comentário
Auditor	Permite realizar todas as operações de visualização e execução de qualquer tarefa em seleções de dispositivos conectados ao Servidor de Administração via Agente de Rede, com privilégios de administrador local (root no Linux). Recomendamos designar essa função com cautela, restrita a um grupo limitado de usuários que realmente necessitam dela para cumprir suas funções oficiais.
Supervisor	Permite a visualização de todas as operações; não permite outras operações. Você pode atribuir esta função a um diretor de segurança e a outros gerentes responsáveis pela segurança de TI em sua organização.
Diretor de segurança	Permite todas as operações de visualização, permite o gerenciamento de relatórios; concede permissões limitadas na área **Gerenciamento do sistema**: **Conectividade**. Você pode atribuir esta função a um diretor responsável pela segurança de TI em sua organização.

A tabela abaixo mostra os direitos de acesso atribuídos a cada função de usuário predefinida.

Direitos de acesso de funções de usuário predefinidas

Função	Descrição

Administrador do Servidor de Administração	Permite todas as operações nas seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Processamento de eventos**
	  • **Hierarquia de Servidores de Administração**
	  • **Servidores de Administração virtuais**
	• **Gerenciamento do sistema**:
	  • **Conectividade**
	  • **Inventário de hardware**
	  • **Inventário de software**
	Concede os direitos de **Leitura** e **Gravação** na área funcional **recursos gerais: gerenciamento de chaves de criptografia**.

Operador do Servidor de Administração	Concede os direitos de **Leitura** e **Execução** em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Servidores de Administração virtual**
	• **Gerenciamento do sistema**:
	  • **Conectividade**
	  • **Inventário de hardware**
	  • **Inventário de software**

Função	Descrição
Auditor	Permite todas as operações nas áreas funcionais, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Objetos excluídos** • **Gerenciamento de relatórios aplicado** Você pode atribuir esta função a uma pessoa que realiza a auditoria da sua organização.

Administrador de instalação	Permite todas as operações nas seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Implementação de software da Kaspersky**
	  • **Gerenciamento de chaves de licença**
	• **Gerenciamento do sistema**:
	  • **Implementação do sistema operacional**
	  • **Gerenciamento de patches e vulnerabilidades**
	  • **Instalação remota**
	  • **Inventário de software**
	Concede os direitos de **Leitura** e **Execução** na área funcional **Recursos gerais: Servidores de Administração virtuais**.

Operador de instalação	Concede os direitos de **Ler** e **Executar** em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Implementação de software Kaspersky** (também concede o direito de **Gerenciar patches da Kaspersky** nesta área)
	  • **Servidores de Administração virtual**
	• **Gerenciamento do sistema**:
	  • **Implementação do sistema operacional**
	  • **Gerenciamento de patches e vulnerabilidades**
	  • **Instalação remota**
	  • **Inventário de software**

Administrador do Kaspersky Endpoint Security	Permite todas as operações nas seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • Área do Kaspersky Endpoint Security, incluindo todos os recursos Concede os direitos de **Leitura** e **Gravação** na área funcional **recursos gerais: gerenciamento de chaves de criptografia**.
Operador do Kaspersky Endpoint Security	Concede os direitos de **Ler** e **Executar** em todas as seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • Área do Kaspersky Endpoint Security, incluindo todos os recursos
Administrador Principal	Permite todas as operações em áreas funcionais, *exceto* as seguintes áreas, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Gerenciamento de relatórios aplicado** Concede os direitos de **Leitura** e **Gravação** na área funcional **recursos gerais: gerenciamento de chaves de criptografia**.

Função	Descrição

Operador Principal	Concede os direitos de **Leitura** e **Execução** (quando aplicável) em todas as seguintes áreas funcionais:
	• **Recursos gerais**:
	  • **Funcionalidade básica**
	  • **Objetos excluídos**
	  • **Operações no Servidor de Administração**
	  • **Implementação do software da Kaspersky**
	  • **Servidores de Administração virtual**
	• **Gerenciamento de Dispositivos Móveis: Geral**
	• **Gerenciamento do sistema**, incluindo todos os recursos
	• Área do Kaspersky Endpoint Security, incluindo todos os recursos

Administrador do Gerenciamento de Dispositivos Móveis	Permite todas as operações nas seguintes áreas funcionais: • **Recursos gerais: Funcionalidade básica** • **Gerenciamento de Dispositivos Móveis: Geral**
Operador do Gerenciamento de Dispositivos Móveis	Concede os direitos de **Leitura** e **Execução** na área funcional **Recursos gerais: Funcionalidade básica**. Concede os comandos **Leitura** e **Enviar somente informações para dispositivos móveis** na área funcional **Gerenciamento de dispositivos móveis**: **Geral**.
Diretor de segurança	Permite todas as operações nas seguintes áreas funcionais, em **Recursos gerais**: • **Acessar objetos independentemente de suas ACLs** • **Gerenciamento de relatórios aplicado** Concede os direitos de **Leitura**, **Gravação**, **Execução** e **Salvamento dos arquivos dos dispositivos na estação de trabalho do administrador** e **executar operações nas seleções de dispositivos** na área funcional **gerenciamento do sistema: conectividade**. Você pode atribuir esta função a um diretor responsável pela segurança de TI em sua organização.
Usuário do Self Service Portal	Permite todas as operações na área funcional **Gerenciamento de Dispositivos Móveis: Self Service Portal**. Este recurso não é compatível com o Kaspersky Security Center 11 e versões posteriores.
Supervisor	Concede o direito de **Leitura** nas áreas funcionais **Recursos gerais**: **Acessar objetos independentemente de suas ACLs** e **Recursos gerais**: **Gerenciamento de relatórios aplicado**. Você pode atribuir esta função a um diretor de segurança e a outros gerentes responsáveis pela segurança de TI em sua organização.
Administrador de gerenciamento de patches e vulnerabilidades	Permite todas as operações nas áreas funcionais **Recursos gerais**: **Funcionalidade básica** e **Gerenciamento do sistema** (incluindo todos os recursos).
Operador de gerenciamento de patches e vulnerabilidades	Concede os direitos de **Leitura** e **Execução** (quando aplicável) nas áreas funcionais **Recursos gerais**: **Funcionalidade básica** e **Gerenciamento do sistema** (incluindo todos os recursos).
Web Console como administrador de serviço	Concede os direitos de **Leitura** e **Gravação** nos **Recursos gerais**:área funcional **Integração de aplicativos**.

Atribuição de direitos de acesso a objetos específicos

Além de atribuir direitos de acesso no nível do servidor, é possível configurar o acesso a objetos específicos, por exemplo, a uma tarefa específica. O aplicativo permite especificar direitos de acesso aos seguintes tipos de objetos:

- Grupos de administração
- Tarefas
- Relatórios

- Seleções de dispositivos
- Seleções de eventos

Para atribuir direitos de acesso a um objeto específico:

1. Dependendo do tipo de objeto, no menu principal, vá para a seção correspondente:
   - **Dispositivos → Hierarquia de grupos**
   - **Dispositivos → Tarefas**
   - **Monitoramento e relatórios → Relatórios**
   - **Dispositivos → Seleções de dispositivos**
   - **Monitoramento e relatórios → Seleções de eventos**
2. Abra as propriedades do objeto para o qual deseja configurar os direitos de acesso.

   Para abrir a janela de propriedades de um grupo de administração ou de uma tarefa, clique no nome do objeto. As propriedades de outros objetos podem ser abertas usando o botão na barra de ferramentas.
3. Na janela de propriedades, abra a seção **Direitos de acesso**.

   A lista de usuários é aberta. Os usuários e grupos de segurança listados têm direitos de acesso ao objeto. Por padrão, se você usar uma hierarquia de grupos de administração ou Servidores, a lista e os direitos de acesso serão herdados do grupo de administração principal ou do Servidor principal.
4. Para poder modificar a lista, ative a opção **Usar permissões personalizadas**.
5. Configure os direitos de acesso:
   - Use os botões **Adicionar** e **Excluir** para modificar a lista.
   - Especifique os direitos de acesso para um usuário ou grupo de segurança. Execute uma das seguintes ações:
     - Caso queira especificar os direitos de acesso manualmente, selecione o usuário ou grupo de segurança, clique no botão **Direitos de acesso** e, em seguida, especifique os direitos de acesso.
     - Caso queira atribuir uma função de usuário ao usuário ou grupo de segurança, selecione o usuário ou grupo de segurança, clique no botão **Funções** e, em seguida, selecione a função a ser atribuída.
6. Clique no botão **Salvar**.

Os direitos de acesso ao objeto são configurados.

Atribuição de direitos de acesso a usuários e grupos de segurança

É possível conceder aos usuários e grupos de segurança direitos de acesso para usar diferentes recursos do Servidor de Administração, por exemplo, Kaspersky Endpoint Security for Linux.

Para atribuir direitos de acesso a um usuário ou grupo de segurança:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Direitos de acesso**, marque a caixa de seleção ao lado do nome do usuário ou do grupo de usuários ao qual os direitos serão atribuídos e clique no botão **Direitos de acesso**.

   Não é possível selecionar vários usuários ou grupos de segurança ao mesmo tempo. Caso mais de um item seja selecionado, o botão **Direitos de acesso** será desativado.

3. Configure o conjunto de direitos para o usuário ou grupo:

   a. Expanda o nó com recursos do Servidor de Administração ou outro aplicativo da Kaspersky.

   b. Marque a caixa de seleção **Permitir** ou **Negar** ao lado do recurso ou do direito de acesso desejado.

      Exemplo 1: marque a caixa de seleção **Allow** ao lado do nó **Application integration** para conceder todos os direitos de acesso disponíveis ao recurso Integração de aplicativos (**Read**, **Write** e **Execute**) para um usuário ou grupo.

      Exemplo 2: expanda o nó **Encryption key management** e marque a caixa de seleção **Allow** ao lado da permissão **Write** para conceder o direito de acesso de **Write** ao recurso de gerenciamento de chaves de criptografia para um usuário ou grupo.

4. Depois de configurar o conjunto de direitos de acesso, clique em **OK**.

O conjunto de direitos do usuário ou do grupo de usuários será configurado.

As permissões do Servidor de Administração (ou do grupo de administração) estão divididas nas seguintes áreas:

- Funcionalidades gerais:
  - Gerenciamento de grupos de administração
  - Acessar objetos independentemente de suas ACLs
  - Funcionalidade básica
  - Objetos excluídos
  - Gerenciamento de chaves de criptografia
  - Processamento de eventos
  - Operações no Servidor de administração (somente na janela de propriedades do Servidor de Administração)
  - Implementação do software da Kaspersky
  - Gerenciamento de chaves de licença
  - A Integração do aplicativo (para integração com o Kaspersky Managed Detection and Response e para a função de Identity and Access Manager)
  - Gerenciamento de relatórios forçado
  - Hierarquia de Servidores de Administração
  - Permissões do usuário
  - Servidores de Administração virtuais
- Gerenciamento de Dispositivos Móveis:
  - Geral
  - Self Service Portal
- Gerenciamento do sistema:
  - Conectividade
  - Inventário de hardware
  - Controle de Acesso de Rede
  - Implementação do sistema operacional
  - Gerenciamento de Patches e Vulnerabilidades
  - Instalação remota
  - Inventário de software

Se nem **Permitir** nem **Negar** estiverem selecionados para um direito de acesso, então, o direito de acesso será considerado como *indefinido*: será negado até que seja explicitamente negado ou permitido pelo usuário.

Os direitos de um usuário são a soma:

- Dos direitos do próprio usuário
- Dos direitos de todas as funções atribuídas a esse usuário
- Dos direitos de todo o grupo de segurança ao qual o usuário pertence
- Dos direitos de todas as funções atribuídas aos grupos de segurança aos quais o usuário pertence

Se pelo menos um desses conjuntos de direitos tiver **Negar** em uma permissão, a permissão será negada ao usuário, mesmo se outros conjuntos permitirem-na ou deixarem-na indefinida.

Também é possível adicionar usuários e grupos de segurança ao escopo de uma função do usuário para usar diferentes recursos do Servidor de Administração. As configurações associadas com uma função de usuário se aplicarão somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

Adicionar uma conta de usuário interno

Para adicionar uma nova conta de usuário interno ao Kaspersky Security Center:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Clique em **Adicionar**.

3. Na janela **Nova entidade** que se abre, especifique as configurações da conta do novo usuário:

- Mantenha a opção padrão **Usuário**.
- **Nome**.
- **Senha** para a conexão do usuário ao Kaspersky Security Center.

  A senha deve estar em conformidade com as seguintes regras:

  - A senha deve ter de 8 a 16 caracteres.
  - A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
    - Letras maiúsculas (A-Z)
    - Letras minúsculas (a-z)
    - Números (0-9)
    - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - A senha não deve conter nenhum espaço em branco, caracteres Unicode ou a combinação dos caracteres "." e "@", quando "." estiver colocado antes de "@".

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

  > O número de tentativas de entrada da senha é limitado. Por padrão, o número máximo de tentativas permitidas de entrada da senha é de 10. Você pode modificar o número permitido de tentativas de inserção de senha, como descrito em "Alterar o número permitido de tentativas de entrada de senha".

  > Se o usuário inserir uma senha inválida no número especificado de vezes, a conta do usuário é bloqueada por um hora. Você pode desbloquear a conta do usuário somente ao alterar a senha.

- **Nome completo**
- **Descrição**
- **Endereço de e-mail**
- **Telefone**

4. Clique em **OK** para salvar as alterações.

A nova conta de usuário aparece na lista de grupos de usuários e segurança.

Criação de um grupo de segurança

Para criar um grupo de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Clique em **Adicionar**.
3. Na janela que se abre **Nova entidade**, selecione **Grupo**.
4. Especifique as seguintes configurações para o novo grupo de segurança:
   - **Nome do grupo**
   - **Descrição**
5. Clique em **OK** para salvar as alterações.

O novo grupo de segurança aparece na lista de grupos de usuários e segurança.

Editar uma conta de usuário interno

Para editar uma nova conta de usuário interno ao Kaspersky Security Center:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Clique no nome da conta de usuário que deseja editar.

3. Na janela de configurações do usuário exibida, na guia **Geral**, altere as configurações da conta de usuário:

- **Descrição**
- **Nome completo**
- **Endereço de e-mail**
- **Telefone principal**
- **Configurar nova senha** para a conexão do usuário com o Kaspersky Security Center.

  A senha deve estar em conformidade com as seguintes regras:

  - A senha deve ter de 8 a 256 caracteres.
  - A senha deve conter caracteres de pelo menos três dos grupos listados abaixo:
    - Letras maiúsculas (A-Z)
    - Letras minúsculas (a-z)
    - Números (0-9)
    - Caracteres especiais (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;)
  - A senha não deve conter nenhum espaço em branco, caracteres Unicode ou a combinação dos caracteres "." e "@", quando "." estiver colocado antes de "@".

  Para ver a senha inserida, mantenha pressionado o botão **Exibir**.

  > O número de tentativas de entrada da senha é limitado. Por padrão, o número máximo de tentativas permitidas de entrada da senha é de 10. É possível alterar o número permitido de tentativas; no entanto, por motivos de segurança, não recomendamos diminuir esse número. Se o usuário inserir uma senha inválida no número especificado de vezes, a conta do usuário é bloqueada por um hora. Você pode desbloquear a conta do usuário somente ao alterar a senha.

- Se necessário, mude o botão de alternar para **Desativado** para impedir o usuário de se conectar ao aplicativo. Você pode desativar uma conta, por exemplo, depois que um funcionário sai da empresa.

4. Na guia **Segurança de autenticação**, você pode especificar as configurações de segurança para esta conta.

5. Na guia **Grupos**, você pode adicionar o usuário a grupos de segurança.

6. Na guia **Dispositivos**, você pode atribuir dispositivos ao usuário.

7. Na guia **Funções**, você pode atribuir funções ao usuário.

8. Clique em **Salvar** para salvar as alterações.

A conta de usuário atualizada aparece na lista de grupos de segurança e usuários.

Edição de um grupo de segurança

Você pode editar apenas grupos internos.

Para editar um grupo de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Clique no nome do grupo de segurança que deseja editar.
3. Na janela de configurações do grupo que é aberta, altere as configurações do grupo de segurança:
   - **Nome**
   - **Descrição**
4. Clique em **Salvar** para salvar as alterações.

O grupo de segurança atualizado aparece na lista de grupos de usuários e segurança.

Adicionar as contas de usuário em um grupo interno

Você somente pode adicionar contas de usuários internos em um grupo interno.

Para adicionar as contas de usuários em um grupo interno:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Marque as caixas de seleção ao lado das contas de usuário que deseja adicionar a um grupo.
3. Clique no botão **Atribuir grupo**.
4. Na janela **Atribuir grupo** exibida, selecione o grupo ao qual deseja adicionar contas de usuário.
5. Clique no botão **Atribuir**.

As contas de usuário são adicionadas ao grupo.

Atribuir um usuário como um proprietário de dispositivo

Para obter informações sobre como atribuir um usuário como proprietário do dispositivo móvel, consulte a Ajuda do Kaspersky Security for Mobile.

Para atribuir um usuário como proprietário do dispositivo:

1. Caso queira atribuir um proprietário de um dispositivo conectado a um Servidor de Administração virtual, primeiro alterne para o Servidor de Administração virtual:

   a. No menu principal, clique no ícone de Sinalização ( ) à direita do nome atual do Servidor de Administração.

   b. Selecione o Servidor de Administração necessário.

2. No menu principal, vá para **Usuários e funções** → **Usuários**.

   Uma lista de usuários é aberta. Caso você esteja conectado a um Servidor de Administração virtual, a lista incluirá usuários do Servidor de Administração virtual atual e do Servidor de Administração principal.

3. Clique no nome da conta de usuário que deseja atribuir como proprietário do dispositivo.

4. Na janela aberta de configurações do usuário, clique na guia **Dispositivos**.

5. Clique em **Adicionar**.

6. Na lista de dispositivos, selecione o dispositivo que deseja atribuir ao usuário.

7. Clique em **OK**.

O dispositivo selecionado é adicionado à lista de dispositivos atribuídos ao usuário.

Você pode executar a mesma operação em **Dispositivos** → **Dispositivos gerenciados**, clicando no nome do dispositivo que deseja atribuir e clicando no link **Gerenciar proprietário do dispositivo**.

Excluir um usuário ou um grupo de segurança

Você pode excluir apenas usuários internos ou grupos de segurança internos.

Para excluir um usuário ou um grupo de segurança:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.

2. Marque a caixa de seleção ao lado do usuário ou do grupo de segurança que deseja excluir.

3. Clique em **Excluir**.

4. Na janela que se abre, clique em **OK**.

O usuário ou o grupo de segurança é excluído.

Criar uma função de usuário

Para criar uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique em **Adicionar**.
3. Na janela **Nome da nova função** exibida, digite o nome da nova função.
4. Clique em **OK** para aplicar as alterações.
5. Na janela de propriedades da função exibida, altere as configurações da função:
   - Na guia **Geral**, edite o nome da função.
     Você não pode editar o nome de uma função predefinida.
   - Na guia **Configurações**, edite o escopo da função e as políticas e os perfis associados à função.
   - Na guia **Direitos de acesso**, edite os direitos de acesso a aplicativos da Kaspersky.
6. Clique em **Salvar** para salvar as alterações.

A nova função aparece na lista de funções de usuário.

Editar uma função de usuário

Para editar uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função que deseja editar.
3. Na janela de propriedades da função exibida, altere as configurações da função:
   - Na guia **Geral**, edite o nome da função.
     Você não pode editar o nome de uma função predefinida.
   - Na guia **Configurações**, edite o escopo da função e as políticas e os perfis associados à função.
   - Na guia **Direitos de acesso**, edite os direitos de acesso a aplicativos da Kaspersky.
4. Clique em **Salvar** para salvar as alterações.

A função atualizada aparece na lista de funções de usuário.

Editar o escopo de uma função de usuário

O *escopo da função do usuário* é uma combinação de usuários e grupos de administração. As configurações associadas com uma função de usuário aplicam-se somente a dispositivos que pertencem a usuários que têm essa função, e apenas se esses dispositivos pertencerem a grupos associados à função, incluindo grupos secundários.

Para adicionar usuários, grupos de segurança e grupos de administração ao escopo de uma função de usuário, você pode usar qualquer dos seguintes métodos:

Método 1:

1. No menu principal, vá para **Usuários e funções** → **Usuários**.
2. Marque as caixas de seleção ao lado dos usuários e grupos de segurança que deseja adicionar ao escopo da função de usuário.
3. Clique no botão **Atribuir função**.

   O Assistente de Atribuição de Funções é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
4. Na etapa **Selecionar função**, selecione a função de usuário que deseja atribuir.
5. Na etapa **Definir escopo**, selecione o grupo de administração que deseja adicionar ao escopo da função de usuário.
6. Clique no botão **Atribuir função** para fechar a janela.

Os usuários ou os grupos de segurança selecionados e o grupo de administração selecionado são adicionados ao escopo da função de usuário.

Método 2:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função para a qual deseja definir o escopo.
3. Na janela de propriedades da função exibida, selecione a guia **Configurações**.
4. Na seção **Escopo da função**, clique em **Adicionar**.

   O Assistente de Atribuição de Funções é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
5. Na etapa **Definir escopo**, selecione o grupo de administração que deseja adicionar ao escopo da função de usuário.
6. Na etapa **Selecionar usuários**, selecione os usuários e os grupos de segurança que deseja adicionar ao escopo da função de usuário.
7. Clique no botão **Atribuir função** para fechar a janela.
8. Clique no botão **Fechar** (⨯) para fechar a janela de propriedades da função.

Os usuários ou os grupos de segurança selecionados e o grupo de administração selecionado são adicionados ao escopo da função de usuário.

Método 3:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Direitos de acesso**, marque a caixa de seleção ao lado do nome do usuário ou do grupo de segurança que deseja adicionar ao escopo de funções do usuário e, em seguida, clique no botão **Funções**.

   Não é possível selecionar vários usuários ou grupos de segurança ao mesmo tempo. Caso mais de um item seja selecionado, o botão **Funções** será desativado.

3. Na janela **Funções**, selecione a função do usuário que deseja atribuir, clique em **OK** e salve as alterações.

   Os usuários ou os grupos de segurança selecionados são adicionados ao escopo da função de usuário.

Excluir uma função de usuário

Para excluir uma função de usuário:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Marque a caixa de seleção ao lado do nome da função que deseja excluir.
3. Clique em **Excluir**.
4. Na janela que se abre, clique em **OK**.

A função de usuário é excluída.

Associação de perfis da política a funções

Você pode associar funções de usuário a perfis da política. Nesse caso, a regra de ativação desse perfil da política é baseada na função: o perfil da política fica ativo para um usuário com a função especificada.

Por exemplo, a política proíbe qualquer software de navegação de GPS em todos os dispositivos em um grupo de administração. O software de navegação de GPS é necessário em um dispositivo único no grupo de administração de Usuários, notadamente que for de propriedade do courier. Nesse caso, você pode atribuir uma função "Courier" ao seu proprietário e criar um perfil da política, permitindo que o software de navegação de GPS seja executado apenas nos dispositivos a cujos proprietários é atribuída a função "Courier". Todas as outras configurações de política são preservadas. Somente o usuário com a função "Courier" poderá executar o software de navegação de GPS. Depois, se outro funcionário receber a função "Courier", o novo funcionário também poderá executar o software de navegação no dispositivo da sua organização. Executar o software de navegação de GPS ainda será proibido em outros dispositivos no mesmo grupo de administração.

Para associar uma função a um perfil da política:

1. No menu principal, vá para **Usuários e funções** → **Funções**.
2. Clique no nome da função que deseja associar a um perfil da política.

   A janela de propriedades da função é exibida com a guia **Geral** selecionada.
3. Selecione a guia **Configurações** e role para baixo até a seção **Políticas e perfis**.
4. Clique em **Editar**.
5. Para associar a função a:

   - **Um perfil da política existente** – Clique no ícone de insígnia (>) ao lado do nome de política necessário e marque a caixa de seleção ao lado do perfil ao qual você deseja associar a função.
   - **Um novo perfil da política**:

     a. Marque a caixa de seleção ao lado da política para a qual deseja criar um perfil.

     b. Clique em **Novo perfil de política**.

     c. Especifique um nome para o novo perfil e defina as configurações de perfil.

     d. Clique no botão **Salvar**.

     e. Selecione a caixa de seleção junto ao novo perfil.
6. Clique em **Atribuir à função**.

O perfil é associado à função e aparece nas propriedades da função. O perfil se aplica automaticamente a qualquer dispositivo cujo proprietário seja atribuído à função.

Propagando funções de usuário aos Servidores de Administração secundários

Por padrão, as listas de funções de usuário dos Servidores de Administração principal e secundários são independentes. Você pode configurar o aplicativo para propagar automaticamente as funções de usuário criadas no Servidor de Administração principal a todos dos Servidores de Administração secundários. As funções de usuário também podem ser propagadas de um Servidor de Administração secundário para seus próprios Servidores de Administração secundários.

Para propagar funções de usuário do Servidor de Administração principal aos Servidores de Administração secundários:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.
2. Vá para a seção **Hierarquia de Servidores de Administração**.
3. Ative a opção **Retransmitir lista de funções para Servidores de Administração secundários** e depois clique no botão **Salvar**.

O aplicativo copia as funções de usuário do Servidor de Administração principal para os Servidores de Administração secundários.

Quando a opção **Retransmitir lista de funções para Servidores de Administração secundários** for ativada e as funções do usuário forem propagadas, elas não poderão ser editadas nem excluídas nos Servidores de Administração secundários. Ao criar uma nova função ou editar uma função existente no Servidor de Administração principal, as modificações são automaticamente copiadas para os Servidores de Administração secundários. Ao excluir uma função de usuário no Servidor de Administração principal, essa função permanece nos Servidores de Administração secundários posteriormente, mas pode ser editada, nem excluída.

As funções propagadas do Servidor de Administração principal para o Servidor de Administração secundário serão exibidas com marcas de seleção verdes (✓). Você não pode editar essas funções no Servidor de Administração secundário.

Se você criar uma função no Servidor de Administração principal e existir uma função com o mesmo nome no Servidor de Administração secundário, a nova função será copiada para o Servidor de Administração secundário com o índice adicionado ao nome, por exemplo, ~~1, ~~2 (o índice pode ser aleatório).

Se você desativar a opção **Retransmitir lista de funções para Servidores de Administração secundários**, todas as funções do usuário permanecerão nos Servidores de Administração secundários, mas serão independentes das que estão no Servidor de Administração principal. Após se tornarem independentes, as funções de usuário nos Servidores de Administração secundários podem ser editadas ou excluídas.

Gerenciar objetos no Kaspersky Security Center Web Console

Esta seção contém informações sobre o gerenciamento de revisão de objeto. O Kaspersky Security Center lhe permite acompanhar a modificação de objeto. Cada vez quando você salva modificações feitas à um objeto, uma *revisão* é criada. Cada revisão tem um número.

Os objetos do aplicativo suportam o gerenciamento de revisão incluem:

- Propriedades do Servidor de Administração
- Políticas
- Tarefas
- Grupos de administração
- Contas de usuário
- Pacotes de instalação

Você pode exibir a lista de revisões e reverter as alterações feitas em um objeto para uma revisão selecionada.

Na janela de propriedades de qualquer objeto que suporta o gerenciamento de revisão, a seção **Histórico de revisões** exibe uma lista de revisões de objeto com os seguintes detalhes:

- **Revisão** – Número de revisão do objeto.
- **Hora** – Data e hora em que o objeto foi modificado.
- **Usuário** – Nome do usuário que modificou o objeto.

- **Ação** - A ação executada no objeto.
- **Descrição** - A Descrição da revisão em relação à modificação feita nas configurações do objeto.

  Por padrão, a descrição da revisão do objeto está em branco. Para adicionar uma descrição a uma revisão, selecione a revisão relevante e clique no botão **Editar descrição**. Na janela aberta, insira algum texto para a descrição da revisão.

Adicionar uma descrição da revisão

O Kaspersky Security Center lhe permite acompanhar a modificação de objeto. Cada vez quando você salva modificações feitas à um objeto, uma revisão é criada. Cada revisão tem um número.

Você pode adicionar uma descrição da revisão para simplificar a procura por revisões na lista.

Para adicionar uma descrição para uma revisão:

1. Na janela de propriedades do objeto, abra a guia **Histórico de revisões**.
2. Na lista de revisões de objeto, selecione a revisão para a qual você precisa adicionar uma descrição.
3. Clique no botão **Editar descrição**.

   A janela **Descrição** se abre.
4. Na janela **Descrição**, insira algum texto para a descrição da revisão.

   Por padrão, a descrição da revisão do objeto está em branco.
5. Salve a descrição da revisão.

A descrição é adicionada na revisão do objeto.

Exclusão de objetos

Esta seção fornece informações sobre como excluir objetos.

Você pode excluir objetos, como os seguintes:

- Políticas
- Tarefas
- Pacotes de instalação
- Servidores de Administração virtual
- Usuários
- Grupos de segurança
- Grupos de administração

Para excluir um objeto:

1. Abra a seção necessária do Kaspersky Security Center Web Console e selecione o objeto.
2. Na barra de ferramentas, clique no botão **Excluir**.
3. Na janela que se abre, clique em **OK** para confirmar a sua seleção.

O objeto selecionado será excluído.

Quando você exclui um objeto, as informações sobre ele permanecem no banco de dados. O período de armazenamento das informações sobre os objetos excluídos é igual ao período de armazenamento das revisões de objetos (o período recomendado é de 90 dias). Você pode alterar o prazo de armazenamento somente se tiver a permissão **Modificar** na área de direitos **Objetos excluídos**.

Sobre a exclusão de dispositivos clientes

Quando um dispositivo gerenciado é excluído de um grupo de administração, o aplicativo move o dispositivo para o grupo dispositivos não atribuídos. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados, o Agente de Rede e qualquer aplicativo de segurança, por exemplo, o Kaspersky Endpoint Security, permanecem no dispositivo.

O Kaspersky Security Center gerencia os dispositivos no grupo Dispositivos não atribuídos de acordo com as seguintes regras:

- Caso tenha configurado as regras de movimentação de dispositivo e um dispositivo atenda aos critérios de uma regra de movimentação, o dispositivo é automaticamente movido para um grupo de administração de acordo com a regra.

- O dispositivo é armazenado no grupo dispositivos não atribuídos e é automaticamente removido do grupo de acordo com as regras de retenção de dispositivos.

  As regras de retenção de dispositivo não afetam os dispositivos que têm uma ou mais unidades criptografadas com criptografia completa do disco. Esses dispositivos não são excluídos automaticamente. Somente é possível excluí-los manualmente. Caso necessite excluir um dispositivo com uma unidade criptografada, primeiro descriptografe a unidade e, em seguida, exclua o dispositivo.

  > Ao excluir um dispositivo com unidade criptografada, os dados necessários para descriptografar a unidade também são excluídos. Se você marcar a caixa de seleção **Eu entendo o risco e desejo excluir os dispositivos selecionados** na janela de confirmação que é aberta quando você exclui esses dispositivos (do grupo **Dispositivos não atribuídos** ou **Dispositivos gerenciados**), significa que você está ciente da exclusão de dados.

  Para descriptografar o dispositivo, as seguintes condições devem ser atendidas:

  - O dispositivo é reconectado ao Servidor de Administração para restaurar os dados necessários para descriptografar a unidade.

  - O usuário do dispositivo lembra a senha de descriptografia.

  - O aplicativo de segurança usado para criptografar o dispositivo, por exemplo, o Kaspersky Endpoint Security for Windows, ainda está instalado nele.

  Caso o dispositivo seja criptografado pela tecnologia Kaspersky Disk Encryption, também é possível tentar recuperar os dados usando o utilitário de restauração FDERT.

> Na VDI, se você tiver um equipamento com dispositivos criptografados, as informações no dispositivo criptografado serão excluídas após a exclusão do equipamento.

Quando um dispositivo é excluído manualmente do grupo dispositivos não atribuídos, o aplicativo remove o dispositivo da lista. Após a exclusão do dispositivo, os aplicativos Kaspersky instalados (se houver) permanecem no dispositivo. Assim, caso o dispositivo ainda esteja visível para o Servidor de Administração e a sondagem de rede regular tenha sido configurada, o Kaspersky Security Center descobre o dispositivo durante a sondagem e o recoloca no grupo Dispositivos não atribuídos. Portanto, é razoável excluir um dispositivo manualmente somente se o dispositivo estiver invisível para o Servidor de Administração.

Kaspersky Security Network (KSN)

Essa seção descreve como usar uma infraestrutura de serviços on-line, denominada Kaspersky Security Network (KSN). A seção fornece os detalhes sobre a KSN, assim como instruções sobre como ativar a KSN, configurar o acesso à KSN e visualizar as estatísticas sobre o uso do Servidor proxy da KSN.

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Sobre a KSN

A Kaspersky Security Network (KSN) é uma infraestrutura de serviços on-line que fornece o acesso à Base de Dados de Conhecimento on-line da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software. O uso de dados a partir da Kaspersky Security Network garante uma resposta mais rápida dos aplicativos Kaspersky a ameaças, melhora a efetividade de alguns componentes de proteção e reduz o risco de falsos positivos. A KSN permite usar os bancos de dados de reputação da Kaspersky para obter informações sobre os aplicativos instalados nos dispositivos gerenciados.

O Kaspersky Security Center oferece suporte às seguintes soluções de infraestrutura KSN:

- *KSN Global* é uma solução que permite trocar informações com a Kaspersky Security Network. Se você participar da KSN, você concorda em enviar informações à Kaspersky, no modo automático, sobre a operação dos aplicativos Kaspersky instalados nos dispositivos cliente gerenciados por meio do Kaspersky Security Center. As informações são transferidas de acordo com as configurações de acesso da KSN atuais. Os analistas da Kaspersky também averiguam as informações recebidas e as incluem nos bancos de dados estatísticos e de reputação da Kaspersky Security Network. O Kaspersky Security Center usa essa solução por padrão.

- A *KSN Privada* é uma solução que permite aos usuários de dispositivos com aplicativos Kaspersky instalados obter acesso aos bancos de dados de reputação da Kaspersky Security Network, bem como a outros dados estatísticos, sem enviar dados para a KSN de seus próprios computadores. A Kaspersky Private Security Network (KSN Privada) foi projetada para clientes corporativos que não podem participar do Kaspersky Security Network por algum dos seguintes motivos:

  - Os dispositivos do usuário não estão conectados à Internet.

  - A transmissão de quaisquer dados fora do país ou fora da LAN corporativa é proibida pela lei ou limitada por políticas de segurança corporativas.

  Você pode definir configurações de acesso da Kaspersky Private Security Network na seção **Configurações de Proxy da KSN** da janela de propriedades do Servidor de Administração.

O aplicativo solicita a você participar da KSN durante a execução do Assistente de Início Rápido. Você pode iniciar ou parar de usar a KSN em qualquer momento durante o uso do aplicativo.

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração KSN for atualizada, a nova versão será exibida ao atualizar ou fazer upgrade do Servidor de Administração. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Se recusar, continuará usando a KSN de acordo com a versão Declaração KSN aceita anteriormente.

Quando o KSN está habilitado, o Kaspersky Security Center verifica se os servidores da KSN estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos. Isso é necessário para garantir que o nível de segurança seja mantido para os dispositivos gerenciados.

Os dispositivos cliente gerenciados pelo Servidor de Administração interagem com a KSN por meio do servidor proxy da KSN. O servidor proxy da KSN fornece os seguintes recursos:

- Os dispositivos cliente podem enviar solicitações à KSN e transferir informações para a KSN mesmo que não tenham acesso direto à Internet.
- O servidor proxy KSN armazena em cache os dados processados, o que reduz a carga de trabalho no canal de saída e o período de tempo despendido para aguardar por informações solicitadas por um dispositivo cliente.

Você pode configurar o Servidor Proxy KSN na seção **Configurações de Proxy da KSN** da janela Propriedades do Servidor de Administração.

Configurar o acesso à KSN

Você pode configurar o acesso ao Kaspersky Security Network (KSN) no Servidor de Administração e em um ponto de distribuição.

Para configurar o acesso do Servidor de Administração à KSN:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.

3. Alterne o botão para a posição **Ativar Proxy da KSN no Servidor de Administração Ativado**.

   Os dados são enviados dos dispositivos cliente para a KSN de acordo com a política do Kaspersky Endpoint Security que estiver ativa naqueles dispositivos cliente. Se essa caixa de seleção estiver desmarcada, nenhum dado será serão enviado a KSN do Servidor de Administração e de dispositivos cliente através do Kaspersky Security Center. No entanto, os dispositivos cliente podem enviar dados para a KSN diretamente (evitando o Kaspersky Security Center), de acordo com suas respectivas configurações. A política do Kaspersky Endpoint Security, que está ativa nos dispositivos cliente, determina quais dados serão enviados diretamente (evitando o Kaspersky Security Center) pelos dispositivos para a KSN.

4. Alterne o botão para a posição **Usar a Kaspersky Security Network Ativado**.

   Se essa opção estiver ativada, os dispositivos cliente enviarão os resultados da instalação de patches para a Kaspersky. Ao ativar esta opção, certifique-se de ler e aceitar os termos da Declaração da KSN.

   Se estiver usando a KSN Privada, alterne o botão para a posição **Usar a Kaspersky Private Security Network Ativado** e clique no botão **Selecionar arquivo com config. proxy da KSN** para baixar as configurações da KSN Privada (arquivos com as extensões pkcs7 e pem). Após as configurações serem baixadas, a interface exibe o nome do provedor e os contatos, assim como a data de criação do arquivo com as configurações da KSN Privada.

   > Ao ativar a KSN Privada, preste atenção aos pontos de distribuição configurados para enviar solicitações da KSN diretamente ao Cloud KSN. Os pontos de distribuição que possuem o Agente de Rede versão 11 (ou anterior) instalado continuarão a enviar solicitações da KSN ao Cloud KSN. Para reconfigurar os pontos de distribuição para enviar solicitações da KSN à KSN Privada, ative a opção **Encaminhar solicitações da KSN para o Servidor de Administração** para cada ponto de distribuição. Você pode ativar esta opção nas propriedades do ponto de distribuição ou na política do Agente de Rede.

   Ao alternar o botão para a posição **Usar a Kaspersky Private Security Network Ativado**, é exibida uma mensagem com detalhes sobre a KSN Privada.

   Os seguintes aplicativos Kaspersky são compatíveis com a KSN privada:

   - Kaspersky Security Center
   - Kaspersky Endpoint Security for Windows
   - Kaspersky Endpoint Security for Linux
   - Service Pack 2 do Kaspersky Security for Virtualization 3.0 Agentless
   - Service Pack 1 do Kaspersky Security for Virtualization 3.0 Light Agent

   Se você ativar a opção KSN Privada no Kaspersky Security Center, esses aplicativos receberão informações sobre compatibilidade com a KSN Privada. Na janela de configurações do aplicativo, na subsecção **Kaspersky Security Network** da seção **Proteção Avançada Contra Ameaças**, **Provedor da KSN: KSN Privada** é exibido. Caso contrário, **Provedor da KSN: KSN Global** será exibido.

   > Se você usa versões do aplicativo anteriores ao Service Pack 2 do Kaspersky Security for Virtualization 3.0 Agentless ou anteriores ao Service Pack 1 do Kaspersky Security for Virtualization 3.0 Light Agent ao executar a KSN Privada, recomendamos que você use Servidores de Administração secundários para os quais o uso da KSN Privada não foi ativado.

   > O Kaspersky Security Center não enviará nenhum dado estatístico à Kaspersky Security Network se a KSN Privada estiver configurada na seção **Configurações de Proxy da KSN** da janela Propriedades do Servidor de Administração.

5. Se você tiver as configurações do servidor proxy definidas nas propriedades do Servidor de Administração, mas sua arquitetura de rede requer o uso direto da KSN Privada, ative a opção **Ignorar configurações do Servidor Proxy ao conectar à KSN Privada**. Caso contrário, as solicitações dos aplicativos gerenciados não alcançarão a KSN Privada.

6. Configure a conexão do Servidor de Administração ao serviço de proxy da KSN:

   - Em **Configurações de conexão**, para a **Porta TCP**, especifique o número da porta TCP que será usada para se conectar ao Servidor proxy da KSN. A porta padrão para conectar-se ao servidor proxy da KSN é 13111.

   - Se desejar que o Servidor de Administração seja conectado ao servidor proxy da KSN por meio de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de porta para **Porta UDP**. Por padrão, esta opção está desativada e a porta TCP é usada. Se essa opção estiver ativada, a porta UDP padrão para se conectar ao servidor proxy da KSN será 15111.

   - Se quiser que o Servidor de Administração se conecte com o servidor proxy da KSN por meio de uma porta HTTPS, ative a opção **Use HTTPS** e especifique um número de porta para **HTTPS through port**. Por padrão, esta opção está desativada e a porta TCP é usada. Se essa opção estiver ativada, a porta HTTPS padrão para se conectar ao servidor proxy da KSN será 17111.

7. Alterne o botão para a posição **Conectar os Servidores de Administração secundários na KSN pelo Servidor de Administração principal Ativado**.

   Se esta opção estiver ativada, Servidores de Administração secundários usam o Servidor de Administração principal como servidor proxy KSN. Se esta opção estiver desativada, os Servidores de Administração secundários conectam-se à KSN por conta própria. Neste caso, os dispositivos gerenciados usam Servidores de Administração secundários como servidores proxy KSN.

   > Os Servidores de Administração secundários usam o Servidor de Administração principal como servidor proxy se, no painel direito da seção **Configurações de Proxy da KSN** nas propriedades do Servidores de Administração secundários, o botão estiver alternado para a posição **Ativar Proxy da KSN no Servidor de Administração Ativado**.

8. Clique no botão **Salvar**.

As configurações de acesso à KSN serão salvas.

Você também pode configurar o acesso ao ponto de distribuição à KSN, por exemplo, se quiser reduzir a carga no Servidor de Administração. O ponto de distribuição que atua como um servidor proxy da KSN envia solicitações da KSN de dispositivos gerenciados para a Kaspersky diretamente, sem usar o Servidor de Administração.

Para configurar o acesso dos pontos de distribuição ao Kaspersky Security Network (KSN):

1. Certifique-se de que o ponto de distribuição seja atribuído manualmente.

2. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

3. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

4. Clique no nome do ponto de distribuição para abrir a janela de propriedades da tarefa.

5. Na janela de propriedades do ponto de distribuição, na seção **Proxy da KSN**, ative a opção **Ativar Proxy KSN no lado do ponto de distribuição** e, em seguida, ative a opção **Acessar a KSN Cloud/KSN Privada diretamente pela internet**.

6. Clique em **OK**.

O ponto de distribuição atuará como um servidor proxy da KSN.

Ativar e desativar a KSN

Para ativar a KSN:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.

3. Alterne o botão para a posição **Ativar Proxy da KSN no Servidor de Administração Ativado**.

   O serviço de Proxy da KSN será ativado.

4. Alterne o botão para a posição **Usar a Kaspersky Security Network Ativado**.

   A KSN será ativada.

   Se o botão de alternância estiver ativado, os dispositivos cliente enviarão os resultados da instalação de patches para a Kaspersky. Ao ativar este botão de alternância, você deve ler e aceitar os termos da Declaração da KSN.

5. Clique no botão **Salvar**.

Para desativar a KSN:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.

3. Alterne o botão para a posição **Ativar Proxy da KSN no Servidor de Administração Desativado** para desativar o serviço de proxy da KSN ou alterne para a posição **Usar a Kaspersky Security Network Desativado**.

   Se um desses botões estiver desativado, os dispositivos cliente não enviarão resultados da instalação de patches para a Kaspersky.

   Se estiver usando a KSN Privada, alterne o botão para a posição **Usar a Kaspersky Private Security Network Desativado**.

   A KSN será desativada.

4. Clique no botão **Salvar**.

Visualizando a Declaração da KSN aceita

Ao ativar o Kaspersky Security Network (KSN), você deve ler e aceitar a Declaração da KSN. Você pode ver a Declaração da KSN aceita a qualquer momento.

Para visualizar a declaração KSN aceita:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.

3. Clique no link **Ver Declaração sobre coleta de dados do KSN**.

Na janela aberta, você pode ver o texto da Declaração KSN aceita.

Aceitando uma declaração da KSN atualizada

Você usa o KSN de acordo com a Declaração KSN lida e aceita ao ativar a KSN. Se a Declaração da KSN for atualizada, ela será exibida quando você atualizar uma versão do Servidor de Administração. Você pode aceitar a Declaração KSN atualizada ou recusá-la. Caso a declaração seja recusada, o usuário continuará usando a KSN de acordo com a versão Declaração da KSN aceita anteriormente.

Depois de atualizar uma versão do Servidor de Administração, a Declaração da KSN atualizada será exibida automaticamente. Se você recusar a declaração da KSN atualizada, você poderá ainda vê-la e aceitá-la posteriormente.

Para visualizar e aceitar ou recusar uma Declaração da KSN atualizada:

1. Clique no link **Exibir notificações** no canto superior direito da janela do aplicativo principal.

   A janela **Notificações** se abre.

2. Clique no link **Ver a Declaração da KSN atualizada**.

   A janela **Atualização da Declaração da Kaspersky Security Network** se abre.

3. Leia a Declaração da KSN e, em seguida, decida-se clicando em um dos seguintes botões:

   - **Eu aceito a declaração da KSN atualizada**
   - **Usar KSN sob as condições da Declaração anterior**

Dependendo da sua escolha, a KSN continuará funcionando de acordo com os termos da Declaração da KSN em vigor ou atualizada. Você pode ver o texto da Declaração da KSN aceita nas propriedades do Servidor de Administração a qualquer momento.

Verificar se o ponto de distribuição funciona como servidor proxy da KSN

Em um dispositivo gerenciado atribuído como ponto de distribuição é possível ativar o servidor proxy da KSN. Um dispositivo gerenciado funciona como servidor proxy da KSN quando o serviço ksnproxy está sendo executado no dispositivo. É possível verificar, ativar ou desativar esse serviço localmente no dispositivo.

Você pode atribuir um dispositivo baseado em Windows ou Linux como um ponto de distribuição. O método de verificação do ponto de distribuição depende de seu sistema operacional.

Para verificar se o ponto de distribuição baseado em Windows funciona como servidor proxy da KSN:

1. No dispositivo de ponto de distribuição, no Windows, abra **Serviços** (**Todos os programas** → **Ferramentas administrativas** → **Serviços**).

2. Na lista de serviços, verifique se o serviço ksnproxy está sendo executado.

   Se o serviço ksnproxy estiver em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Se desejar, você pode desativar o serviço ksnproxy. Nesse caso, o Agente de Rede no ponto de distribuição para de participar da Kaspersky Security Network. Isso requer direitos de administrador local.

Para verificar se o ponto de distribuição baseado em Linux funciona como servidor proxy da KSN:

1. No dispositivo do ponto de distribuição, exiba a lista de processos em execução.

2. Na lista de processos em execução, verifique se o processo `/opt/kaspersky/ksc64/sbin/ksnproxy` está em execução.

Caso o processo `/opt/kaspersky/ksc64/sbin/ksnproxy` esteja em execução, o Agente de Rede do dispositivo participa da Kaspersky Security Network e funciona como servidor proxy da KSN para os dispositivos gerenciados incluídos no escopo do ponto de distribuição.

Atualização dos bancos de dados e dos aplicativos da Kaspersky

Esta seção descreve as etapas que você deve seguir para atualizar regularmente o seguinte:

- Bancos de dados e módulos de software da Kaspersky
- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center

A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Cenário: Atualização regular dos bancos de dados e dos aplicativos Kaspersky

Esta seção fornece um cenário para a atualização regular de bancos de dados, módulos de software e aplicativos da Kaspersky. Após ter concluído o Cenário de configuração de proteção da rede, você precisará manter a confiabilidade do sistema de proteção para ter certeza de que os Servidores de Administração e os dispositivos gerenciados estejam permanentemente protegidos contra várias ameaças, incluindo vírus, ataques à rede e ataques de phishing.

A proteção da rede é mantida atualizada por atualizações regulares dos seguintes:

- Bancos de dados e módulos de software da Kaspersky
- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center

Quando concluir este cenário, você poderá ter certeza do seguinte:

- A sua rede está protegida pelo software da Kaspersky mais recente, inclusive aplicativos de segurança e componentes do Kaspersky Security Center.
- Os bancos de dados de antivírus e outros bancos de dados da Kaspersky críticos para a segurança de rede são sempre atualizados.

Pré-requisitos

Os dispositivos gerenciados devem ter uma conexão com o Servidor de Administração. Se eles não tiverem uma conexão, considere atualizar os bancos de dados, módulos de software e aplicativos da Kaspersky manualmente ou diretamente nos servidores de atualização da Kaspersky.

O Servidor de Administração deve ter uma conexão com a Internet.

Antes de iniciar, assegure-se de que você tenha feito o seguinte:

1. Implementado os aplicativos de segurança da Kaspersky nos dispositivos gerenciados de acordo com o cenário de implementação de aplicativos Kaspersky através do Kaspersky Security Center Web Console.
2. Criado e configurado todos os perfis da política, políticas e tarefas necessários segundo o cenário de configuração da proteção de rede.
3. Atribuído um volume apropriado de pontos de distribuição conforme o número de dispositivos gerenciados e a topologia de rede.

A atualização dos bancos de dados e dos aplicativos da Kaspersky prossegue em estágios:

1. **Seleção de um esquema de atualização**

   Há vários esquemas que você pode usar para instalar atualizações para componentes e aplicativos de segurança do Kaspersky Security Center. Selecione o esquema ou vários esquemas que atendem aos requisitos de sua melhor rede.

2. **Criar a tarefa para baixar as atualizações no repositório do Servidor de Administração**

   Essa tarefa é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Se você não tiver executado o assistente, crie a tarefa agora.

   Essa tarefa é necessária para baixar atualizações de servidores de atualização da Kaspersky para o repositório do Servidor de Administração, bem como atualizar bancos de dados e módulos do software da Kaspersky para o Kaspersky Security Center. Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

   Se a rede tiver pontos de distribuição atribuídos, as atualizações serão baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Nesse caso, os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.

   Instruções de como proceder:

- Console de Administração: Criação da tarefa para baixar as atualizações para o repositório do Servidor de Administração
- Kaspersky Security Center Web Console: Criação da tarefa para baixar as atualizações para o repositório do Servidor de Administração

3. **Criar a tarefa para baixar as atualizações para os repositórios de pontos de distribuição (opcional)**

   Por padrão, as atualizações são baixadas para os pontos de distribuição do Servidor de Administração. Você pode configurar o Kaspersky Security Center para baixar as atualizações para os pontos de distribuição diretamente dos servidores de atualização da Kaspersky. Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.

   Quando a rede tiver atribuído pontos de distribuição e a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for criada, os pontos de distribuição baixarão atualizações dos servidores de atualização da Kaspersky, e não do repositório do Servidor de Administração.

   Instruções de como proceder:

   - Console de Administração: Criar a tarefa ao baixar atualizações nos repositórios dos pontos de distribuição
   - Kaspersky Security Center Web Console: Criação da tarefa para baixar as atualizações para os repositórios de pontos de distribuição

4. **Configurar os pontos de distribuição**

   Quando a sua rede tem pontos de distribuição atribuídos, certifique-se de que a opção **Implementar atualizações** esteja ativada nas propriedades de todos os pontos de distribuição necessários. Quando essa opção é desativada para um ponto de distribuição, os dispositivos incluídos no escopo das atualizações de download do ponto de distribuição do repositório do Servidor de Administração.

   Se quiser que os dispositivos gerenciados recebam atualizações somente dos pontos de distribuição, ative a opção **Distribuir os arquivos somente através dos pontos de distribuição** na política de Agente de Rede.

5. **Otimizando o processo de atualização usando o modelo offline de download de atualização ou arquivos diff (opcionais)**

   Você pode otimizar o processo de atualização usando o modelo offline de download de atualização (ativado por padrão) ou usando arquivos diff. Para cada segmento de rede, você precisa escolher qual desses dois recursos ativar, porque eles não podem funcionar simultaneamente.

   Quando o modelo offline de download das atualizações for ativado, o Agente de Rede baixará as atualizações necessárias para o dispositivo gerenciado quando as atualizações forem baixadas para o repositório do Servidor de Administração, antes de o aplicativo de segurança solicitar as atualizações. Isso melhora a confiabilidade do processo de atualização. Para usar o recurso, ative a opção **Fazer antecipadamente o download das atualizações e dos bancos de dados de antivírus via Servidor de Administração (recomendado)** na política do agente de rede.

   Se não usar o modelo offline de download das atualizações, você poderá otimizar o tráfego entre o Servidor de Administração e os dispositivos gerenciados usando arquivos diff. Quando esse recurso for ativado, o Servidor de Administração ou um ponto de distribuição baixará arquivos diff em vez de arquivos inteiros de bancos de dados ou módulos de software da Kaspersky. Um arquivo diff descreve as diferenças entre duas versões de um arquivo de banco de dados ou módulo de software. Por isso, um arquivo diff ocupa menos espaço do que um arquivo inteiro. Isso resulta na redução no tráfego entre o Servidor de Administração ou os pontos de distribuição e os dispositivos gerenciados. Para usar esse recurso, ative a opção **Baixar arquivos diff** nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e/ou da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*.

   Instruções de como proceder:

   - Uso de arquivos diff para atualizar bancos de dados e módulos do software da Kaspersky

- Console de Administração: Ativar e desativar o modelo offline para o download das atualizações
- Kaspersky Security Center Web Console: Ativar e desativar o modelo offline para o download das atualizações

6. **Verificação das atualizações baixadas (opcional)**

   Antes de instalar as atualizações baixadas, é possível verificar as atualizações pela tarefa de *Verificação de atualizações*. Essa tarefa executa em sequência as tarefas de atualização de dispositivo e as tarefas de verificação de malwares configuradas por meio configurações da coleção especificada de dispositivos de teste. Para obter os resultados da tarefa, o Servidor de Administração inicia ou bloqueia a propagação de atualização para os dispositivos restantes.

   A tarefa de *Verificação de atualizações* pode ser executada como parte da tarefa *Baixar atualizações para o repositório do Servidor de Administração*. Nas propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*, ative a opção **Verificar atualizações antes de distribuir** no Console de Administração ou na opção **Executar verificação de atualizações** no Kaspersky Security Center Web Console.

   Instruções de como proceder:

   - Console de Administração: Verificação das atualizações baixadas
   - Kaspersky Security Center Web Console: Verificar as atualizações baixadas

7. **Aprovar e recusar atualizações de software**

   Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Você pode alterar o status para *Aprovado* ou *Negado*. As atualizações aprovadas sempre são instaladas. Se uma atualização necessitar de análise e aceitação dos termos do Contrato de Licença do Usuário Final, você primeiro precisará aceitar os termos. Depois disso, a atualização poderá ser propagada para os dispositivos gerenciados. As atualizações não definidas só podem ser instaladas no Agente de Rede e em outros componentes do Kaspersky Security Center conforme as configurações de política do Agente de Rede. As atualizações para as quais você define o status *Negado* não serão instaladas em dispositivos. Se uma atualização recusada para um aplicativo de segurança tiver sido instalada anteriormente, o Kaspersky Security Center tentará desinstalar a atualização de todos os dispositivos. As atualizações de componentes do Kaspersky Security Center não podem ser desinstaladas.

   Instruções de como proceder:

   - Console de Administração: Aprovação e recusa de atualizações de software
   - Kaspersky Security Center Web Console: Aprovação e recusa de atualizações de software

8. **Configuração da instalação automática de atualizações e correções para componentes do Kaspersky Security Center**

   As atualizações e os patches baixados para o Agente de Rede e outros componentes do Kaspersky Security Center são instalados automaticamente. Se você deixou a opção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido** ativada nas propriedades do Agente de Rede, todas as atualizações serão instaladas automaticamente após o download no repositório (ou em vários repositórios). Se esta opção estiver desativada, as correções da Kaspersky que foram baixadas e identificadas com o status *Indefinido* somente serão instaladas após você alterar o status para *Aprovado*.

   Instruções de como proceder:

   - Console de Administração: Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center
   - Kaspersky Security Center Web Console: Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center

9. **Instalação de atualizações para o Servidor de Administração**

As atualizações de software para o Servidor de Administração não dependem dos status de atualização. Elas não são instaladas automaticamente e devem ser previamente aprovadas pelo administrador na guia **Monitoramento** no Console de Administração (**Servidor de Administração** `<nome do servidor>` → **Monitoramento**) ou na seção **Notificações** no Kaspersky Security Center Web Console (**Monitoramento e relatórios** → **Notificações**). Depois disso, o administrador deve executar explicitamente a instalação das atualizações.

10. **Configuração da instalação automática de atualizações para os aplicativos de segurança**

    Crie as tarefas de *atualização* para os aplicativos gerenciados para que forneçam prontamente as atualizações para os aplicativos, módulos do software e bancos de dados Kaspersky, inclusive bancos de dados de antivírus. Para garantir atualizações oportunas, recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório** quando configurar a agenda de tarefas.

    Se sua rede inclui somente dispositivos IPv6 e você deseja atualizar regularmente os aplicativos de segurança instalados neles, certifique-se de que o Servidor de Administração (versão não inferior a 13.2) e o Agente de Rede (versão não inferior a 13.2) estejam instalados nos dispositivos gerenciados.

    Por padrão, atualizações para o Kaspersky Endpoint Security for Windows e Kaspersky Endpoint Security for Linux são instaladas apenas depois que você modifica o status de atualização para *Aprovado*. É possível alterar as configurações de atualização na tarefa de *atualização*.

    Se uma atualização necessitar de análise e aceitação dos termos do Contrato de Licença do Usuário Final, você primeiro precisará aceitar os termos. Depois disso, a atualização poderá ser propagada para os dispositivos gerenciados.

    Instruções de como proceder:

    - Console de Administração: A instalação automática do Kaspersky Endpoint Security atualiza em dispositivos
    - Kaspersky Security Center Web Console: Instalação automática de atualizações do Kaspersky Endpoint Security em dispositivos

Resultados

Após a conclusão do cenário, o Kaspersky Security Center será configurado para atualizar os bancos de dados da Kaspersky e os aplicativos da Kaspersky instalados após o download das atualizações no repositório do Servidor de Administração ou nos repositórios de pontos de distribuição. Você poderá prosseguir para monitorar o status da rede.

Sobre atualização de bancos de dados, módulos de software e aplicativos da Kaspersky

Para ter certeza de que a proteção dos seus Servidores de Administração e dispositivos gerenciados esteja atualizada, você deverá fornecer atualizações oportunas dos seguintes:

- Bancos de dados e módulos de software da Kaspersky

  Antes de baixar os bancos de dados e módulos de software da Kaspersky, o Kaspersky Security Center verifica se os servidores da Kaspersky estão acessíveis. Caso não seja possível acessar os servidores usando o DNS do sistema, o aplicativo usa os servidores DNS públicos. Isso é necessário para garantir que os bancos de dados antivírus sejam atualizados e que o nível de segurança seja mantido para os dispositivos gerenciados.

- Aplicativos da Kaspersky instalados, incluindo componentes e aplicativos de segurança do Kaspersky Security Center

Dependendo da configuração da rede, você pode usar os seguintes esquemas de download e distribuição das atualizações necessárias para os dispositivos gerenciados:

- Ao usar uma única tarefa: *Baixar atualizações no repositório do Servidor de Administração*
- Usando duas tarefas:
  - A tarefa *Baixar atualizações no repositório do Servidor de Administração*
  - A tarefa *Baixar atualizações para os repositórios de pontos de distribuição*
- Manualmente por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP
- Diretamente dos servidores de atualização da Kaspersky para o Kaspersky Endpoint Security nos dispositivos gerenciados
- Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Usando a tarefa Baixar atualizações no repositório do Servidor de Administração

Nesse esquema, o Kaspersky Security Center baixa as atualizações através da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Em redes pequenas que contêm menos de 300 dispositivos gerenciados em um segmento de rede único ou menos de 10 dispositivos gerenciados em cada segmento de rede, as atualizações são distribuídas aos dispositivos gerenciados diretamente do repositório do Servidor de Administração (veja a figura abaixo).

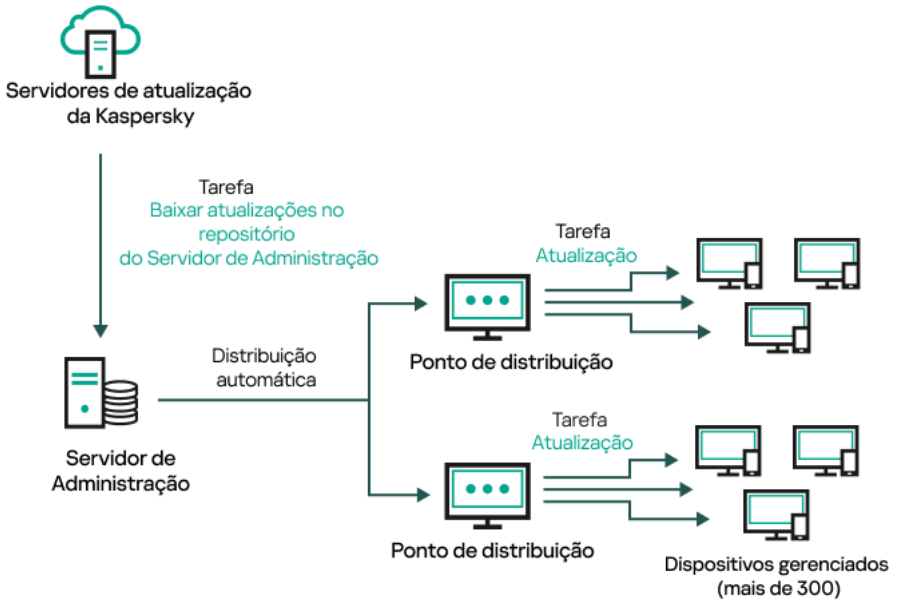


Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração sem pontos de distribuição

Por padrão, o Servidor de Administração comunica-se com os servidores de atualização Kaspersky e baixa as atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração para usar o protocolo HTTP em vez de HTTPS.

Se a rede contiver mais de 300 dispositivos gerenciados em um segmento de rede único ou se a rede consistir vários segmentos de rede com mais de 9 dispositivos gerenciados em cada segmento de rede, recomendamos o uso de pontos de distribuição para propagar as atualizações aos dispositivos gerenciados (veja a figura abaixo). Os pontos de distribuição reduzem a carga no Servidor de Administração e otimizam o tráfego entre o Servidor de Administração e os dispositivos gerenciados. Você pode calcular o número e a configuração de pontos de distribuição necessários para a rede.

Nesse esquema, as atualizações são baixadas automaticamente do repositório do Servidor de Administração para os repositórios dos pontos de distribuição. Os dispositivos gerenciados incluídos no escopo de um ponto de distribuição baixam as atualizações do repositório do ponto de distribuição em vez de do repositório do Servidor de Administração.



Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração com pontos de distribuição.

Quando a tarefa *Baixar atualizações no repositório do Servidor de Administração* for concluída, as seguintes atualizações serão baixadas no repositório do Servidor de Administração:

- Módulos de software e bancos de dados da Kaspersky para o Kaspersky Security Center

  Essas atualizações são instaladas automaticamente.

- Módulos de software e bancos de dados da Kaspersky para os aplicativos de segurança nos dispositivos gerenciados

  Essas atualizações são instaladas por meio da tarefa de Atualização para o Kaspersky Endpoint Security for Windows.

- Atualizações para o Servidor de Administração

  Essas atualizações não são instaladas automaticamente. O administrador deve explicitamente aprovar e executar a instalação das atualizações.

  > É necessário ter direitos de administrador local para a instalação de patches no Servidor de Administração.

- Atualizações dos componentes do Kaspersky Security Center

  Por padrão, essas atualizações são instaladas automaticamente. Você pode alterar as configurações na política do Agente de rede.

- Atualizações dos aplicativos de segurança

  Por padrão, o Kaspersky Endpoint Security for Windows instala apenas as atualizações aprovadas por você. (Você pode aprovar atualizações pelo Console de Administração ou pelo Kaspersky Security Center Web Console). As atualizações são instaladas pela tarefa de *Atualização* e podem ser configuradas nas propriedades desta tarefa.

> A tarefa *Baixar atualizações para o repositório do Servidor de Administração* não está disponível nos Servidores de Administração virtuais. O repositório do Servidor de Administração virtual exibe as atualizações baixadas para o Servidor de Administração principal.

Você pode configurar as atualizações a serem verificadas quanto a operabilidade e erros em um conjunto de dispositivos de teste. Se a verificação for bem-sucedida, as atualizações serão distribuídas para outros dispositivos gerenciados.

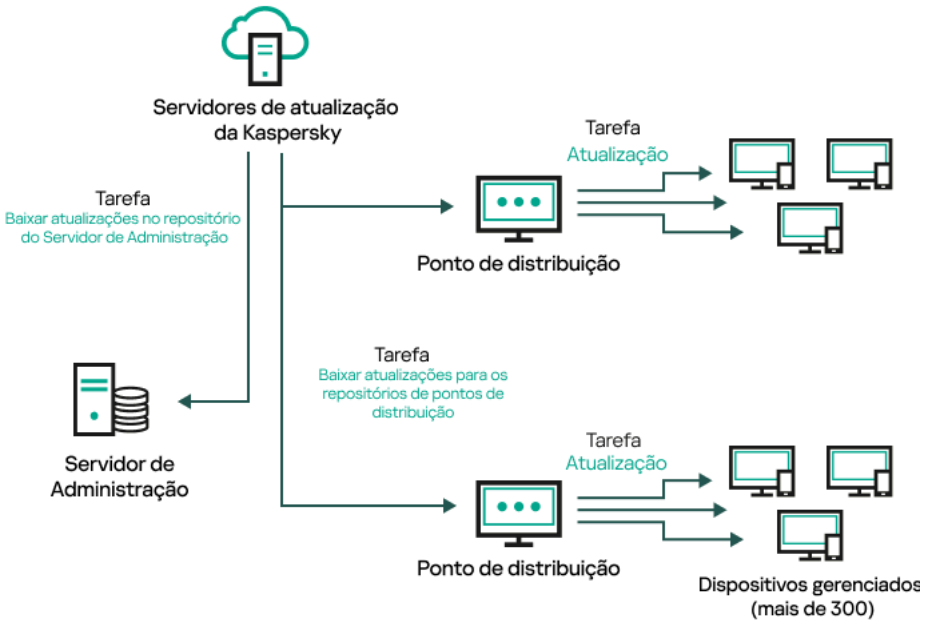
Cada aplicativo da Kaspersky solicita as atualizações necessárias do Servidor de Administração. O Servidor de Administração agrega essas solicitações e baixa somente as que são solicitadas por qualquer aplicativo. Isso garante que as mesmas atualizações não sejam baixadas várias vezes e impede que as atualizações desnecessárias sejam baixadas. Ao executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, o Servidor de Administração envia automaticamente as seguintes informações para os servidores de atualização da Kaspersky para assegurar o download das versões relevantes dos bancos de dados e dos módulos de software da Kaspersky:

- ID e versão do aplicativo
- ID de instalação do aplicativo
- ID da chave ativa
- ID de execução da tarefa *Baixar atualizações para o repositório do Servidor de Administração*

Nenhuma das informações transmitidas contém informações pessoais ou outros dados confidenciais. A AO Kaspersky Lab protege as informações de acordo com os requisitos estabelecidos por lei.

Usando duas tarefas: a tarefa Baixar atualizações no repositório do Servidor de Administração e a tarefa Baixar atualizações para os repositórios de pontos de distribuição

Você pode baixar atualizações para os repositórios de pontos de distribuição diretamente dos servidores de atualização Kaspersky em vez de do repositório do Servidor de Administração e distribuir as atualizações para os dispositivos gerenciados (veja a figura abaixo). Faça o download para os repositórios dos pontos de distribuição se o tráfego entre o Servidor de Administração e os pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.



Atualizando usando a tarefa Baixar atualizações no repositório do Servidor de Administração e a tarefa Baixar atualizações para os repositórios de pontos de distribuição

Por padrão, o Servidor de Administração e os pontos de distribuição comunicam-se com Servidores de atualização Kaspersky e baixam de atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração e/ou os pontos de distribuição para usar o protocolo HTTP em vez de HTTPS.

Para implementar esse esquema, crie a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* além da tarefa *Baixar atualizações no repositório do Servidor de Administração*. Depois disso, os pontos de distribuição baixarão atualizações dos servidores de atualização Kaspersky e não do repositório do Servidor de Administração.

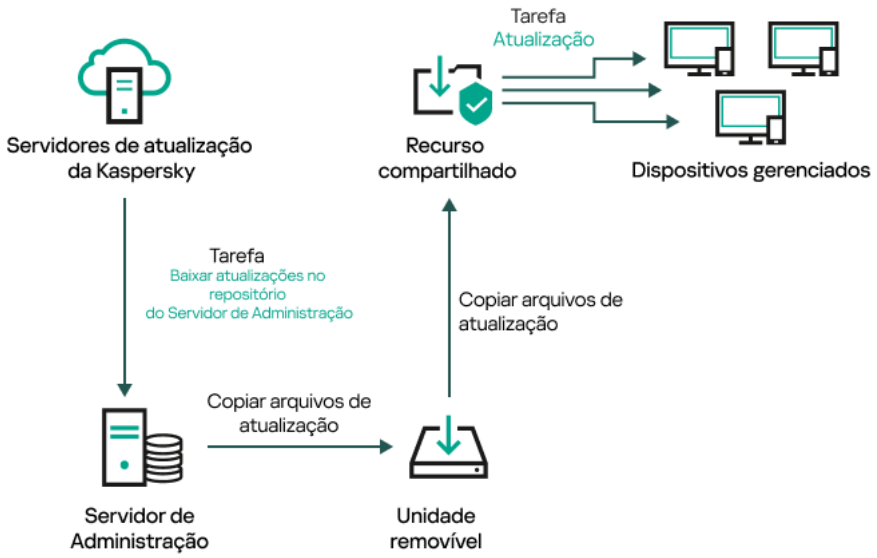
Os dispositivos de ponto de distribuição executando macOS não podem baixar atualizações dos servidores de atualização da Kaspersky.

Se um ou mais dispositivos executando macOS estiverem dentro do escopo da tarefa *Baixar atualizações para os repositórios de pontos de distribuição*, a tarefa será concluída com o status *Falha*, mesmo se for concluída com êxito em todos os dispositivos Windows.

A tarefa *Baixar atualizações no repositório do Servidor de Administração* também é necessária para esse esquema, porque essa tarefa é usada para baixar módulos de software e bancos de dados da Kaspersky para o Kaspersky Security Center.

Manualmente por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

Se os dispositivos cliente não tiverem uma conexão com o Servidor de Administração, você poderá usar uma pasta local ou um recurso compartilhado como uma origem para atualizar bancos de dados, módulos de software e aplicativos Kaspersky. Nesse esquema, você precisa copiar as atualizações necessárias do repositório do Servidor de Administração para uma unidade removível e depois copiar as atualizações para a pasta local ou o recurso compartilhado especificado como uma fonte de atualização nas configurações do Kaspersky Endpoint Security (veja a figura abaixo).



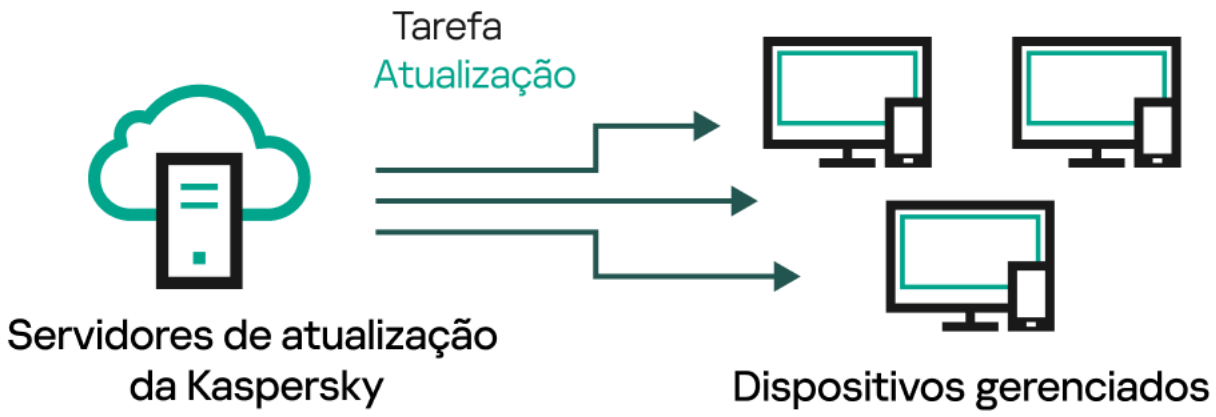
Atualização por meio de uma pasta local, uma pasta compartilhada ou um servidor FTP

Para obter mais informações sobre fontes de atualizações no Kaspersky Endpoint Security, consulte a seguinte ajuda:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux

Diretamente dos servidores de atualização da Kaspersky para o Kaspersky Endpoint Security nos dispositivos gerenciados

Nos dispositivos gerenciados, você pode configurar o Kaspersky Endpoint Security para receber atualizações diretamente dos servidores de atualização da Kaspersky (veja a figura abaixo).



Atualização de aplicativos de segurança diretamente dos servidores de atualização da Kaspersky

Nesse esquema, o aplicativo de segurança não usa os repositórios fornecidos pelo Kaspersky Security Center. Para receber atualizações diretamente dos servidores de atualização da Kaspersky, especifique os servidores de atualização da Kaspersky como uma fonte de atualização na interface do aplicativo de segurança. Para obter mais informações sobre essas configurações, consulte as seguintes ajudas:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux

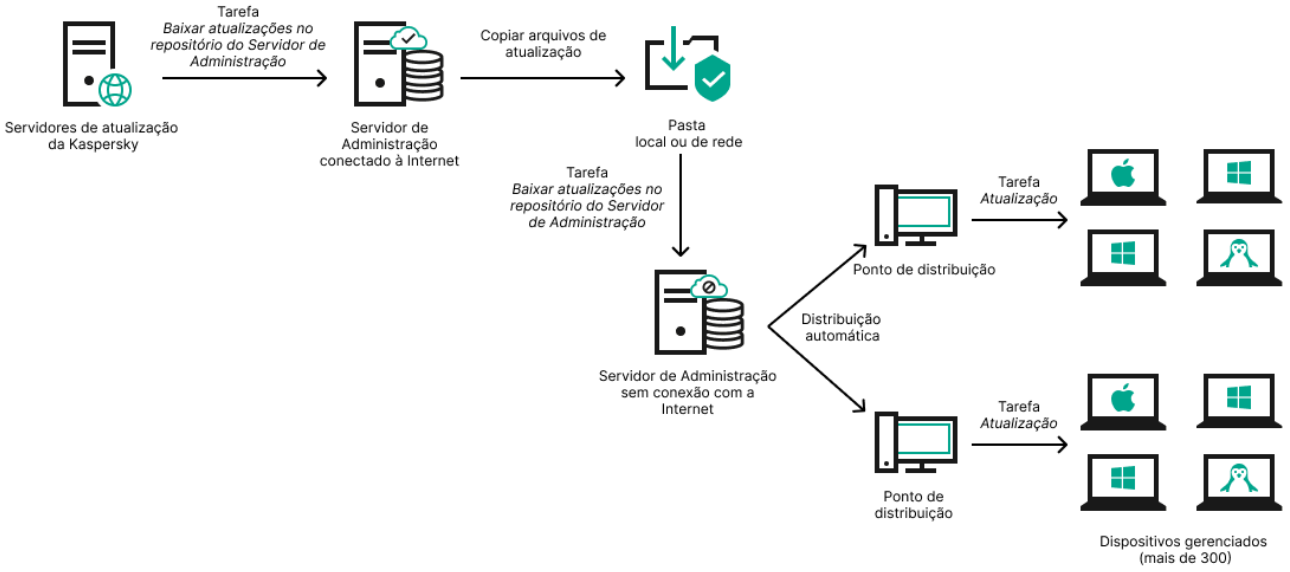
Por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

Se o Servidor de Administração não tiver conexão com a Internet, você poderá configurar a tarefa *Baixar atualizações no repositório do Servidor de Administração* para baixar atualizações de uma pasta local ou de rede. Nesse caso, você deve copiar os arquivos de atualização necessários para a pasta especificada de tempos em tempos. Por exemplo, você pode copiar os arquivos de atualização necessários de uma das seguintes fontes:

- Servidor de Administração que possui conexão com a Internet (veja a figura abaixo)

  Como um Servidor de Administração baixa apenas as atualizações solicitadas pelos aplicativos de segurança, os conjuntos de aplicativos de segurança gerenciados pelos Servidores de Administração (o que tem conexão com a Internet e o que não tem) devem corresponder.

Se o Servidor de Administração que você usa para baixar atualizações tiver a versão 13.2 ou anterior, abra as propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e, em seguida, ative a opção **Baixar atualizações usando o esquema antigo**.



Atualização por meio de uma pasta local ou de rede se o Servidor de Administração não tiver conexão com a Internet

- Utilitário de atualização da Kaspersky

  Como este utilitário usa o esquema antigo para baixar atualizações, abra as propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração* e, em seguida, ative a opção **Baixar atualizações usando o esquema antigo**.

Criação da tarefa baixar atualizações no repositório do Servidor de Administração

A tarefa *Baixar atualizações no repositório do Servidor de Administração* do Servidor de Administração é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. É possível criar apenas uma tarefa de *Baixar atualizações no repositório do Servidor de Administração*. Portanto, é possível criar uma tarefa *Baixar atualizações no repositório do Servidor de Administração* somente se essa tarefa tiver sido removida da lista de tarefas do Servidor de Administração.

Essa tarefa deve baixar atualizações dos servidores de atualização Kaspersky para o repositório do Servidor de Administração. A lista de atualizações inclui:

- Atualizações para bancos de dados e módulos do software do Servidor de Administração
- Atualizações para bancos de dados e módulos do software de aplicativos de segurança Kaspersky
- Atualizações para componentes do Kaspersky Security Center
- Atualizações para aplicativos de segurança Kaspersky

Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

Antes de distribuir as atualizações para os dispositivos gerenciados, é possível executar a tarefa de *Verificação de atualizações*. Isso permite ter a certeza de que o Servidor de Administração instalará as atualizações baixadas corretamente e que um nível de segurança não diminuirá devido às atualizações. Para verificá-las antes de distribuir, configure a opção **Executar verificação de atualizações** nas configurações de tarefas *Baixar atualizações no repositório do Servidor de Administração*.

*Para criar uma tarefa **Baixar atualizações no repositório do Servidor de Administração**:*

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Baixar atualizações no repositório do Servidor de Administração**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
6. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.
7. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

8. Na janela de propriedades da tarefa, na guia **Configurações do aplicativo**, especifique as seguintes configurações:

- Fontes de atualizações

  Os seguintes recursos podem ser utilizados como uma origem das atualizações do Servidor de Administração:

  - Servidores de atualização da Kaspersky

    Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo. Por padrão, o Servidor de Administração comunica-se com os servidores de atualização Kaspersky e baixa as atualizações usando o protocolo HTTPS. Você pode configurar o Servidor de Administração para usar o protocolo HTTP em vez de HTTPS.

    Selecionado por padrão.

  - Servidor de Administração Principal

    Este recurso é aplicado a tarefas criadas para um Servidor de Administração virtual ou secundário.

  - Pasta local ou de rede

    Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Uma pasta de rede pode ser um servidor FTP ou HTTP, ou um compartilhamento SMB. Se uma pasta de rede exigir autenticação, apenas o protocolo SMB será compatível. Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado.

    > Um servidor FTP ou HTTP ou pasta de rede utilizados por uma fonte de atualização devem conter uma estrutura de pastas (com atualizações) que corresponda à estrutura criada ao usar servidores de atualização Kaspersky.

  Caso uma pasta compartilhada que contenha atualizações seja protegida por senha, ative a opção **Especificar conta para acesso à pasta compartilhada da fonte de atualização (se houver)** e insira as credenciais da conta necessárias para o acesso.

- Pasta para armazenar atualizações

  O caminho para a pasta especificada para armazenar atualizações salvas. É possível copiar o caminho da pasta especificada para uma área de transferência. Não é possível alterar o caminho para uma pasta especificada para uma tarefa de grupo.

- Outras configurações:

  - Forçar a atualização de Servidores de Administração secundários

    Caso esta opção esteja ativada, o Servidor de Administração inicia as tarefas de atualização nos Servidores de Administração secundários assim que as novas atualizações são baixadas. As tarefas de atualização são iniciadas usando a fonte de atualização configurada nas propriedades da tarefa nos Servidores de Administração secundários.

    Caso esta opção esteja desativada, as tarefas de atualização nos Servidores de Administração secundários serão iniciadas de acordo com seus agendamentos.

    Por padrão, esta opção está desativada.

  - Copiar as atualizações baixadas em pastas adicionais

Após recepção das atualizações pelo Servidor de Administração, estas são copiadas para as pastas especificadas. Use esta opção se você deseja gerenciar manualmente a distribuição das atualizações na rede.

Por exemplo, você pode desejar usar esta opção na seguinte situação: a rede de sua organização consiste em várias sub-redes independentes e os dispositivos de cada uma das sub redes não têm acesso a outras sub-redes. Entretanto, os dispositivos em todas das sub-redes têm acesso a um compartilhamento de rede comum. Neste caso, você define o Servidor de Administração em uma das sub-redes para baixar atualizações dos Servidores de Atualização Kaspersky, ativar essa opção e especificar esse compartilhamento de rede. Nas atualizações baixadas para as tarefas de repositório de outros Servidores de Administração, especifique o mesmo compartilhamento de rede como a origem da atualização.

Por padrão, esta opção está desativada.

- **Não forçar a atualização de dispositivos e Servidores de Administração secundários a não ser que a cópia tenha sido concluída**

  As tarefas de download das atualizações nos dispositivos cliente e no Servidor de Administração secundário somente inicia depois das atualizações serem copiadas da pasta principal das atualizações para as pastas de atualização adicionais.

  Essa opção deve ser ativada se os de dispositivos cliente e os Servidores de Administração secundários baixam atualizações de pastas adicionais da rede.

  Por padrão, esta opção está desativada.

- **Conteúdo das atualizações**:

  - **Baixar arquivos diff**

    Esta opção ativa o recurso de download dos arquivos diff.

    Por padrão, esta opção está desativada.

- **Baixar atualizações usando o esquema antigo**

A partir da versão 14, o Kaspersky Security Center baixa as atualizações de bancos de dados e os módulos de software usando o novo esquema. Para que o aplicativo baixe atualizações usando o novo esquema, a fonte de atualização deve conter os arquivos de atualização com os metadados compatíveis com o novo esquema. Caso a fonte de atualização contenha os arquivos de atualização com os metadados compatíveis apenas com o esquema antigo, ative a opção **Baixar atualizações usando o esquema antigo**. Caso contrário, a tarefa de download de atualizações falhará.

Por exemplo, é preciso habilitar essa opção quando uma pasta local ou de rede for especificada como fonte de atualização, e os arquivos de atualização nesta pasta tiverem sido baixados por um dos seguintes aplicativos:

- Utilitário de atualização da Kaspersky

  Esse utilitário baixa as atualizações usando o esquema antigo.

- Kaspersky Security Center 13.2 ou versão anterior

  Por exemplo, o Servidor de Administração 1 não possui uma conexão com a Internet. Nesse caso, é possível baixar as atualizações usando o Servidor de Administração 2, desde que ele tenha conexão com a Internet e, em seguida, colocar as atualizações em uma pasta local ou de rede para usá-la como fonte de atualização para o Servidor de Administração 1. Caso o Servidor de Administração 2 tenha a versão 13.2 ou anterior, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa para o Servidor de Administração 1.

Por padrão, esta opção está desativada.

- **Executar verificação de atualizações**

  O Servidor de Administração baixa as atualizações da fonte, salva-as num repositório temporário e executa a tarefa definida no campo **Tarefa de verificação de atualizações**. Se a tarefa for concluída com êxito, as atualizações serão copiadas do repositório temporário para uma pasta compartilhada no Servidor de Administração e distribuídas a todos os dispositivos para os quais o Servidor de Administração atua como a fonte de atualizações (tarefas com o agendamento de **Quando novas atualizações são baixadas no repositório** forem iniciadas). A tarefa de download de atualizações para o repositório é concluída somente após o término da *Tarefa de verificação de atualizações*.

  Por padrão, esta opção está desativada.

9. Na janela de propriedades da tarefa, na guia **Agendamento**, crie uma programação para o início da tarefa. Se necessário, especifique as seguintes configurações:

- Início agendado:

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - Manualmente

    A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

    Por padrão, esta opção está selecionada.

  - A cada N minutos

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - A cada N horas

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - A cada N dias

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - A cada N semanas

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - Diariamente (não é compatível com horário de verão)

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

- **Semanalmente**

  A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Todos os meses em dias especificados das semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- **Usar atraso randomizado automaticamente para início da tarefas**

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- **Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)**

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

- **Parar a tarefa se ela for executada por mais que (min.)**

  Após o final do período especificado, a tarefa é interrompida automaticamente, quer tenha sido concluída ou não.

  Ative esta opção se você quiser interromper (ou parar) tarefas que levam muito tempo para serem executadas.

  Por padrão, esta opção está desativada. O tempo predefinido de execução da tarefa é de 120 minutos.

10. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

Quando o Servidor de Administração executa a tarefa *Baixar atualizações no repositório do Servidor de Administração*, as atualizações de bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada do Servidor de Administração. Se você criar esta tarefa para um grupo de administração, ela somente será aplicada aos Agentes de Rede incluídos no grupo de administração especificado.

As atualizações são distribuídas aos dispositivos clientes e aos Servidores de Administração secundários da pasta compartilhada do Servidor de Administração.

Verificação das atualizações baixadas

Antes de instalar as atualizações nos dispositivos gerenciados, é possível verificar primeiro as atualizações sobre operabilidade e erros por meio da tarefa de *Verificação de atualizações*. A tarefa de *Verificação de atualizações* é executada automaticamente como parte da tarefa *Baixar atualizações no repositório do Servidor de Administração*. O Servidor de Administração baixa as atualizações da origem, salva-as no armazenamento temporário e executa a tarefa de *Verificação de atualizações*. Caso a tarefa seja concluída com êxito, as atualizações são copiadas do repositório temporário para a pasta compartilhada do Servidor de Administração. Elas são distribuídas à todos os dispositivos clientes para os quais o Servidor de Administração for a fonte de atualizações.

Caso os resultados da tarefa de *Verificação de atualizações* demostrarem que as atualizações localizadas no repositório temporário estão incorretas ou se a tarefa de *Verificação de atualizações* concluir com erro, as atualizações não serão copiadas para a pasta compartilhada. O Servidor de Administração retém o conjunto anterior de atualizações. Além disso, as tarefas que têm o tipo de agendamento **Quando novas atualizações são baixadas no repositório** não são iniciadas. Essas operações são realizadas no próximo início da tarefa *Baixar atualizações no repositório do Servidor de Administração* se a verificação das novas atualizações for concluída com êxito.

Um conjunto de atualizações é considerado inválido se uma das seguintes condições for atendida em pelo menos um dispositivo de teste:

- Ocorreu um erro na tarefa de atualização.
- O status da proteção em tempo real do aplicativo de segurança foi modificado após a aplicação das atualizações.
- Um objeto infectado foi detectado durante a execução da tarefa de verificação sob demanda.
- Ocorreu um erro de tempo de execução de um aplicativo da Kaspersky.

Caso nenhuma das condições listadas sejam verdadeiras em nenhum dispositivo de teste, o conjunto de atualizações é considerado como válido, e a tarefa de *Verificação de atualizações* será considerada com êxito na conclusão.

Antes de começar a criar a tarefa de *Verificação de atualizações*, execute os pré-requisitos:

1. Criar um grupo de administração com vários dispositivos de teste. Esse grupo será necessário para verificar as atualizações.

   Recomenda-se usar os dispositivos com a proteção mais confiável e com a configuração de aplicativo mais popular na rede. Essa abordagem aumenta a qualidade e a probabilidade de detecção de vírus durante as verificações e minimiza o risco de falsos positivos. Caso sejam detectados vírus nos dispositivos de teste, a tarefa de *Verificação de atualizações* será considerada malsucedida.

2. Crie as tarefas de atualização e verificação de malwares para um aplicativo compatível com o Kaspersky Security Center, por exemplo, Kaspersky Endpoint Security for Windows ou Kaspersky Security for Windows Server. Ao criar as tarefas de atualização e verificação de malwares, especifique o grupo de administração com os dispositivos de teste.

   A tarefa de *verificação de atualizações* executa sequencialmente as tarefas de atualização e verificação de malwares em dispositivos de teste para verificar se todas as atualizações são válidas. Além disso, ao criar a tarefa de *Verificação de atualizações*, será necessário especificar as tarefas de atualização e verificação de malwares.

3. Crie a tarefa *Baixar atualizações no repositório do Servidor de Administração*.

Para que o Kaspersky Security Center verifique as atualizações baixadas antes de distribuí-las para os dispositivos cliente:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Clique na tarefa **Baixar atualizações no repositório do Servidor de Administração**.

3. Na janela de propriedades do aplicativo que se abre, acesse a guia **Configurações do aplicativo** e, então, habilite a opção **Executar verificação de atualizações**.

4. Caso a tarefa *Verificação de atualizações* exista, clique no botão **Selecionar tarefa**. Na janela aberta, selecione a tarefa de *Verificação de atualizações* no grupo de administração com dispositivos de teste.

5. Caso não tenha criado a tarefa de *Verificação de atualizações* anteriormente, faça o seguinte:

   a. Clique no botão **Nova tarefa**.

   b. No Assistente para novas tarefas aberto, especifique o nome da tarefa caso queira alterar o nome da predefinição.

   c. Selecione o grupo de administração com os dispositivos de teste criado anteriormente.

   d. Primeiro, selecione a tarefa de atualização de um aplicativo necessário e compatível com o Kaspersky Security Center, em seguida, selecione a tarefa de verificação de malwares.

   Depois disso, as seguintes opções aparecem. Recomendamos deixá-las ativadas:

   - **Reiniciar o dispositivo após a atualização do banco de dados**

     Depois que os bancos de dados antivírus forem atualizados em um dispositivo, recomendamos reinicializar o dispositivo.

     Por padrão, a opção está ativada.

   - **Verificar o status de proteção em tempo real após atualização do banco de dados e o reinício do dispositivo**

     Caso esta opção esteja habilitada, a tarefa de *Verificação de atualizações* verifica se as atualizações baixadas para o repositório do Servidor de Administração são válidas e se o nível de proteção diminuiu após a atualização do banco de dados antivírus e a reinicialização do dispositivo.

     Por padrão, esta opção está ativada.

   e. Especifique uma conta a partir da qual a tarefa de *Verificação de atualizações* será executada. É possível usar a conta e deixar a opção **Conta padrão** habilitada. Como alternativa, é possível especificar que a tarefa seja executada em outra conta com os direitos de acesso necessários. Para isso, selecione a opção **Especificar conta** e, em seguida, insira as credenciais dessa conta.

6. Clique em **Salvar** para fechar a janela de propriedades da tarefa *Baixar atualizações no repositório do Servidor de Administração*.

A verificação de atualizações automática é ativada. Agora, é possível executar a tarefa *Baixar atualizações no repositório do Servidor de Administração*, e ela começará a partir da verificação de atualização.

Criar as atualizações de download para a tarefa dos repositórios dos pontos de distribuição

A tarefa *Download de atualizações nos repositórios de pontos de distribuição* somente funciona em dispositivos de ponto de distribuição que executam o Windows. Os dispositivos do ponto de distribuição executando Linux ou macOS não podem baixar atualizações dos servidores de atualização Kaspersky. Se pelo menos um dispositivo executando Linux ou macOS estiver dentro do escopo da tarefa, a tarefa terá o status *Falhou*. Mesmo se a tarefa for concluída com êxito em todos os dispositivos Windows, ela retornará um erro nos dispositivos restantes.

É possível criar a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* para um grupo de administração. Esta tarefa será executada para pontos de distribuição incluídos no grupo de administração especificado.

Você pode usar esta tarefa, por exemplo, se o tráfego entre o Servidor de Administração e pontos de distribuição for mais dispendioso do que o tráfego entre os pontos de distribuição e os servidores de atualização da Kaspersky, ou se o Servidor de Administração não tiver acesso à Internet.

Esta tarefa é necessária para baixar atualizações de servidores de atualização da Kaspersky para os repositórios de pontos de distribuição. A lista de atualizações inclui:

- Atualizações para bancos de dados e módulos do software de aplicativos de segurança Kaspersky
- Atualizações para componentes do Kaspersky Security Center
- Atualizações para aplicativos de segurança Kaspersky

Após o download das atualizações, elas podem ser propagadas aos dispositivos gerenciados.

*Para criar a tarefa **Baixar atualizações para os repositórios de pontos de distribuição**, para um grupo de administração selecionado:*

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, no campo **Tipo de tarefa**, selecione **Baixar atualizações para os repositórios de pontos de distribuição**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Selecione um botão de opção para especificar o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.
6. Na etapa **Concluir a criação da tarefa**, caso queira modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
7. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.
8. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

9. Na guia **Configurações do aplicativo** da janela de propriedades da tarefa, especifique as seguintes configurações:

- **Fontes de atualizações**

  Os seguintes recursos podem ser utilizados como uma origem das atualizações para o ponto de distribuição:

  - Servidores de atualização da Kaspersky

    Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

    Esta opção está marcada por padrão.

  - Pasta local ou de rede

    Uma pasta local ou pasta de rede que contém as atualizações mais recentes. Uma pasta de rede pode ser um servidor FTP ou HTTP, ou um compartilhamento SMB. Se uma pasta de rede exigir autenticação, apenas o protocolo SMB será compatível. Ao selecionar uma pasta local, você deve especificar uma pasta no dispositivo que tenha o Servidor de Administração instalado.

    Um servidor FTP ou HTTP ou pasta de rede utilizados por uma fonte de atualização devem conter uma estrutura de pastas (com atualizações) que corresponda à estrutura criada ao usar servidores de atualização Kaspersky.

- **Pasta para armazenar atualizações**

  O caminho para a pasta especificada para armazenar atualizações salvas. É possível copiar o caminho da pasta especificada para uma área de transferência. Não é possível alterar o caminho para uma pasta especificada para uma tarefa de grupo.

- **Baixar arquivos diff**

  Esta opção ativa o recurso de download dos arquivos diff.

  Por padrão, esta opção está desativada.

- **Baixar atualizações usando o esquema antigo**

A partir da versão 14, o Kaspersky Security Center baixa as atualizações de bancos de dados e os módulos de software usando o novo esquema. Para que o aplicativo baixe atualizações usando o novo esquema, a fonte de atualização deve conter os arquivos de atualização com os metadados compatíveis com o novo esquema. Caso a fonte de atualização contenha os arquivos de atualização com os metadados compatíveis apenas com o esquema antigo, ative a opção **Baixar atualizações usando o esquema antigo**. Caso contrário, a tarefa de download de atualizações falhará.

Por exemplo, é preciso habilitar essa opção quando uma pasta local ou de rede for especificada como fonte de atualização, e os arquivos de atualização nesta pasta tiverem sido baixados por um dos seguintes aplicativos:

- Utilitário de atualização da Kaspersky

  Esse utilitário baixa as atualizações usando o esquema antigo.

- Kaspersky Security Center 13.2 ou versão anterior

  Por exemplo, um ponto de distribuição está configurado para receber as atualizações de uma pasta local ou de rede. Nesse caso, é possível baixar as atualizações usando um Servidor de Administração que tenha uma conexão com a Internet e, em seguida, colocar as atualizações na pasta local no ponto de distribuição. Caso o Servidor de Administração tenha a versão 13.2 ou anterior, habilite a opção **Baixar atualizações usando o esquema antigo** na tarefa *Baixe atualizações para os repositórios de pontos de distribuição*.

Por padrão, esta opção está desativada.

10. Crie um agendamento para o início da tarefa. Se necessário, especifique as seguintes configurações:

- **Início agendado**

  Selecione o agendamento segundo o qual a tarefa é executada e configure o agendamento selecionado.

  - **Manualmente**

    A tarefa não executa automaticamente. Você somente pode iniciá-la manualmente.

    Por padrão, esta opção está selecionada.

  - **A cada N minutos**

    A tarefa é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada do dia em que a tarefa é criada.

    Por padrão, a tarefa é executada a cada 30 minutos, iniciando na hora atual do sistema.

  - **A cada N horas**

    A tarefa é executada regularmente, com o intervalo especificado em horas, iniciando na data e hora especificadas.

    Por padrão, a tarefa é executada a cada 6 horas, começando na data e hora atuais do sistema.

  - **A cada N dias**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Além disso, você pode especificar uma data e hora da primeira tarefa executada. Essas opções adicionais ficam disponíveis, se forem compatíveis pelo aplicativo para o qual você cria a tarefa.

    Por padrão, a tarefa é executada todos os dias, iniciando na data e hora atuais do sistema.

  - **A cada N semanas**

    A tarefa é executada regularmente, com o intervalo especificado em semanas, no dia da semana e na hora especificados.

    Por padrão, a tarefa é executada às segundas-feiras, na hora atual do sistema.

  - **Diariamente (não é compatível com horário de verão)**

    A tarefa é executada regularmente, com o intervalo especificado em dias. Esse agendamento não tem suporte à observância do horário de verão (DST, daylight saving time). Isso significa que, quando os relógios são adiantados ou atrasados em uma hora no início ou no término do DST, a hora de início real da tarefa não é alterada.

    Não recomendamos que você use esse agendamento. Ele é necessário para compatibilidade com as versões anteriores do Kaspersky Security Center.

    Por padrão, a tarefa inicia diariamente na hora atual do sistema.

- **Semanalmente**

  A tarefa é executada toda semana, no dia e na hora especificados.

- **Por dias da semana**

  A tarefa é executada regularmente, nos dias da semana e no horário especificados.

  Por padrão, a tarefa é executada todas as sextas-feiras às 18h.

- **Mensalmente**

  A tarefa é executada regularmente, no dia do mês e na hora especificados.

  Nos meses cuja data especificada não existe, a tarefa é executada no último dia.

  Por padrão, a tarefa é executada no primeiro dia do mês, na hora atual do sistema.

- **Todos os meses em dias especificados das semanas selecionadas**

  A tarefa é executada regularmente, nos dias de cada mês e na hora especificados.

  Por padrão, nenhum dia do mês é selecionado. A hora de início padrão é 18:00.

- **No surto de vírus**

  A tarefa é executada após a ocorrência de um evento de *Surto de vírus*. Selecione tipos de aplicativos que monitorem ataques de vírus. Estão disponíveis os seguintes tipos de aplicativos:

  - Antivírus para estações de trabalho e servidores de arquivo
  - Antivírus para defesa de perímetro
  - Antivírus para sistemas de correio

  Por padrão, todos os tipos de aplicativos estão selecionados.

  Talvez você queira executar tarefas diferentes dependendo do tipo de aplicativo de segurança que relata um surto de vírus. Neste caso, remova a seleção dos tipos de aplicativos de que você não precisa.

- **Na conclusão de outra tarefa**

  A tarefa atual inicia após outra tarefa ser concluída. Você pode selecionar como a tarefa anterior deve ser concluída (com êxito ou com erro) para acionar o início da tarefa atual. Por exemplo, talvez seja necessário executar a tarefa *Gerenciar dispositivos* com a opção **Ligar o dispositivo** e, após a conclusão, executar a tarefa *Verificação de vírus*. Este parâmetro só funciona se ambas as tarefas forem atribuídas aos mesmos dispositivos.

- **Executar tarefas ignoradas**

Esta opção determina o comportamento de uma tarefa se um dispositivo cliente não estiver visível na rede quando a tarefa estiver prestes a iniciar.

Se esta opção estiver ativada, o sistema tentará iniciar a tarefa da próxima vez que um aplicativo da Kaspersky for executado em um dispositivo cliente. Se o agendamento da tarefa for **Manualmente**, **Uma vez** ou **Imediatamente**, a tarefa é iniciada imediatamente após o dispositivo ficar visível na rede, ou imediatamente após o dispositivo ser incluído no escopo da tarefa.

Se esta opção estiver desativada, somente as tarefas agendadas serão executadas em dispositivos clientes. Para os tipos de agendamento **Manualmente**, **Uma vez** e **Imediatamente**, as tarefas são executadas somente nos dispositivos clientes que estão visíveis na rede. Por exemplo, você pode querer desativar esta opção para uma tarefa que consome recursos e que você deseja executar somente fora do horário comercial.

Por padrão, esta opção está desativada.

- Usar retardo aleatório automaticamente para início da tarefa

  Se esta opção for ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro de um intervalo de tempo especificado, ou seja, no *início da tarefa distribuída*. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos clientes ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  A hora inicial distribuída é calculada automaticamente quando a tarefa é criada, dependendo do número de dispositivos clientes aos quais a tarefa foi atribuída. Posteriormente, a tarefa sempre será iniciada na hora de início calculada. Entretanto, quando as configurações da tarefa são editadas ou a tarefa é iniciada manualmente, o valor calculado da hora de início da tarefa muda.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos clientes apenas de acordo com o agendamento.

- Usar retardo aleatório para inícios de tarefa em um intervalo de (min.)

  Se esta opção estiver ativada, a tarefa é iniciada nos dispositivos clientes aleatoriamente dentro do intervalo de tempo especificado. O início da tarefa distribuída ajuda a evitar um grande número de solicitações simultâneas pelos dispositivos cliente ao Servidor de Administração, quando uma tarefa agendada estiver em execução.

  Se essa opção estiver desativada, a tarefa inicia em dispositivos cliente apenas de acordo com o agendamento.

  Por padrão, esta opção está desativada. O intervalo de tempo predefinido é de um minuto.

11. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

    Além das configurações que você especificar durante a criação da tarefa, você pode alterar outras propriedades de uma tarefa criada.

Quando a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* for executada, as atualizações para bancos de dados e módulos de software são baixadas da fonte de atualização e armazenadas na pasta compartilhada. As atualizações baixadas somente serão usadas por pontos de distribuição que estão incluídos no grupo de administração especificado e que não têm nenhuma tarefa de download de atualização explicitamente definida para eles.

Ativar e desativar a atualização automática e a correção para componentes do Kaspersky Security Center

As atualizações e as correções do Servidor de Administração podem ser instaladas apenas manualmente, depois da obtenção da aprovação explícita do administrador.

A instalação automática de atualizações e patches para componentes do Kaspersky Security Center é ativada por padrão durante a instalação do Agente de Rede no dispositivo. Você pode desativá-lo durante a instalação do Agente de Rede ou desativá-lo em outro momento usando uma política.

Para desativar a atualização automática e a correção para componentes do Kaspersky Security Center durante a instalação local do Agente de Rede em um dispositivo:

1. Inicie a instalação local do Agente de Rede no dispositivo.
2. Na etapa **Configurações avançadas**, desmarque a caixa de seleção **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**.
3. Siga as instruções do Assistente.

O Agente de Rede com a atualização e correção automática desativada para os componentes do Kaspersky Security Center será instalado no dispositivo. É possível ativar a atualização e a aplicação de patches automáticas mais tarde usando uma política.

Para desativar a atualização e a correção automática dos componentes do Kaspersky Security Center durante a instalação do Agente de Rede no dispositivo através de um pacote de instalação:

1. No menu principal, acesse **Operações → Repositórios → Pacotes de instalação**.
2. Clique no pacote **Agente de Rede do Kaspersky Security Center <número da versão>**.
3. Na janela de propriedades, abra a guia **Configurações**.
4. Desligue o botão de alternância **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido**.

O Agente de Rede com a atualização e correção automática desativado para os componentes do Kaspersky Security Center será instalado a partir deste pacote. É possível ativar a atualização e a aplicação de patches automáticas mais tarde usando uma política.

Se esta caixa de seleção estiver marcada (ou desmarcada) durante a instalação do Agente de Rede no dispositivo, você pode subsequentemente ativar (ou desativar) a atualização automática usando a política de Agente de Rede.

Para ativar ou desativar a atualização e a correção automática para os componentes do Kaspersky Security Center usando a política de Agente de Rede:

1. No menu principal, vá para **Dispositivos → Políticas e perfis**.
2. Clique na política do Agente de Rede.

3. Na janela de propriedades da política, abra a guia **Configurações do aplicativo**.

4. Na seção **Gerenciar patches e atualizações**, ative ou desative o botão de alternância **Instalar automaticamente as atualizações e patches aplicáveis para os componentes com status Indefinido** para ativar ou desativar, respectivamente, a atualização e a aplicação de patches automáticas.

5. Defina o bloqueio (🔒) para este botão de alternância.

A política será aplicada aos dispositivos selecionados, e a atualização e a correção automática para componentes do Kaspersky Security Center será ativada (ou desativada) nestes dispositivos.

Instalação automática de atualizações para o Kaspersky Endpoint Security for Windows

Você pode configurar as atualizações automáticas dos bancos de dados e módulos de software do Kaspersky Endpoint Security for Windows nos dispositivos clientes.

Para configurar o download e a instalação automática das atualizações do Kaspersky Endpoint Security for Windows nos dispositivos:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

2. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

3. Para o aplicativo da Kaspersky Endpoint Security for Windows, selecione **Atualização** como o subtipo de tarefa.

4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).

5. Selecione o escopo da tarefa.

6. Especifique o grupo de administração, a seleção de dispositivos ou os dispositivos aos quais a tarefa se aplica.

7. Na etapa **Concluir a criação da tarefa**, caso queira modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

8. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.

9. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

10. Na guia **Configurações do aplicativo** da janela de propriedades de tarefa, defina as configurações da tarefa de atualização no modo local ou de dispositivos móveis:

    - **Modo local**: a conexão é estabelecida entre o dispositivo e o Servidor de Administração.

    - **Modo móvel**: nenhuma conexão é estabelecida entre o Kaspersky Security Center e o dispositivo (por exemplo, quando o dispositivo não está conectado à Internet).

11. Ative as fontes de atualização que deseja usar para atualizar bancos de dados e módulos de aplicativo do Kaspersky Endpoint Security for Windows. Se necessário, altere as posições das fontes na lista usando os botões **Para cima** e **Para baixo**. Se várias fontes de atualizações forem ativadas, o Kaspersky Endpoint Security for Windows tentará se conectar a elas uma após a outra, começando pelo topo da lista, e executará a tarefa de atualização recuperando o pacote de atualização da primeira fonte disponível.

12. Ative a opção **Instalar apenas atualizações aprovadas** para baixar e instalar atualizações dos módulos de software junto com bancos de dados do aplicativo.

    Se a opção estiver ativada, o Kaspersky Endpoint Security for Windows notifica o usuário sobre as atualizações dos módulos de software disponíveis e inclui atualizações nos módulos de software no pacote de atualização ao executar a tarefa de atualização. O Kaspersky Endpoint Security for Windows instala somente as atualizações para as quais você definiu o status *Aprovado*; elas serão instaladas localmente por meio da interface do aplicativo ou do Kaspersky Security Center.

    Você também pode ativar a opção **Instalar atualizações críticas do módulo de aplicativo automaticamente**. Se quaisquer atualizações do módulo de software estiverem disponíveis, o Kaspersky Endpoint Security for Windows as instala com o status *Crítico*; as atualizações remanescentes serão instaladas após a sua aprovação.

    Se a atualização do módulo de software requerer a revisão e aceitação dos termos do Contrato de Licença e da Política de Privacidade, o aplicativo instala as atualizações após os termos do Contrato de Licença e da Política de Privacidade terem sido aceitos pelo usuário.

13. Marque a caixa de seleção **Copiar atualizações para uma pasta** para que o aplicativo salve as atualizações baixadas em uma pasta e especifique o caminho da pasta.

14. Agende a tarefa. Para assegurar atualizações oportunas, recomendamos selecionar a opção **Quando novas atualizações são baixadas no repositório**.

15. Clique em **Salvar**.

Ao executar a tarefa de **Atualização**, o aplicativo envia solicitações aos servidores de atualização Kaspersky.

Algumas atualizações necessitam da instalação das versões mais recentes dos plug-ins de gerenciamento.

Aprovar e recusar atualizações de software

As configurações de uma tarefa de instalação de atualização podem necessitar da aprovação de atualizações que devem ser instaladas. Você pode aprovar atualizações que devem ser instaladas e recusar as atualizações que não devem ser instaladas.

Por exemplo, pode ser necessário verificar primeiro a instalação das atualizações em um ambiente de teste, assegurar-se de que elas não interferem na operação dos dispositivos e, só então, permitir a instalação dessas atualizações nos dispositivos cliente.

Para aprovar ou recusar uma ou várias atualizações:

1. No menu principal, vá para **Operações → Aplicativos Kaspersky → Atualizações contínuas**.

   Aparece uma lista das atualizações disponíveis.

   As atualizações de aplicativos gerenciados podem exigir a instalação de uma versão mínima específica do Kaspersky Security Center. Se esta versão for posterior à versão atual, essas atualizações serão exibidas, mas não poderão ser aprovadas. Além disso, nenhum pacote de instalação pode ser criado a partir dessas atualizações até que você atualize o Kaspersky Security Center. Você receberá uma solicitação para atualizar sua instância do Kaspersky Security Center para a versão mínima necessária.

2. Selecione as atualizações que deseja aprovar ou recusar.

3. Clique em **Aprovar** para aprovar as atualizações selecionadas ou **Recusar** para recusar as atualizações selecionadas.

   O valor padrão é *Indefinido*.

   As atualizações às quais você atribui o status *Aprovado* são colocadas em uma fila para instalação.

   As atualizações às quais você atribui o status *Negado* são desinstaladas (se possível) de todos os dispositivos nos quais elas foram anteriormente instaladas. Além disso, elas não serão instaladas em outros dispositivos no futuro.

Algumas atualizações para aplicativos da Kaspersky não podem ser desinstaladas. Se você definir o status *Negado* para elas, o Kaspersky Security Center não desinstalará estas atualizações dos dispositivos nos quais elas foram anteriormente instaladas. No entanto, essas atualizações nunca serão instaladas em outros dispositivos no futuro.

Se você definir o status *Negado* para atualizações de software de terceiros, estas atualizações não serão instaladas em dispositivos para os quais elas foram planejadas, mas que ainda não foram instaladas. As atualizações permanecerão nos dispositivos nos quais elas já foram instaladas. Se você tiver as atualizações, poderá exclui-las de forma manual localmente.

Atualizando o Servidor de Administração

Você pode instalar as atualizações do Servidor de Administração usando o Assistente de atualização do Servidor de Administração.

Para instalar uma atualização do Servidor de Administração:

1. No menu principal, vá para **Operações** → **Aplicativos Kaspersky** → **Atualizações contínuas**.
2. Execute o Assistente de atualização do Servidor de Administração de uma das seguintes maneiras:
   - Clique no nome de uma atualização do Servidor de Administração na lista de atualizações e, na janela que é aberta, clique no link **Executar o assistente de atualização do Servidor de Administração**.
   - Clique no link **Executar o assistente de atualização do Servidor de Administração** no campo de notificação na parte superior da janela.
3. Na janela Assistente de atualização do Servidor de Administração, selecione uma das seguintes opções para especificar quando instalar uma atualização:
   - **Instalar agora**. Selecione esta opção se deseja instalar a atualização agora.
   - **Adiar instalação**. Selecione esta opção se deseja instalar a opção mais tarde. Nesse caso, uma notificação sobre esta atualização será exibida.
   - **Ignorar atualização**. Selecione esta opção se não deseja instalar uma atualização e não deseja receber notificações sobre esta atualização.
4. Selecione a opção **Criar cópia backup do Servidor de Administração antes da instalação da atualização** se deseja criar um backup do Servidor de Administração antes de instalar a atualização.
5. Clique no botão **OK** para encerrar o Assistente.

Se um processo de backup é interrompido, o processo de instalação da atualização também é interrompido.

Ativar e desativar o modelo offline de download da atualização

Recomendamos que você evite desativar o modelo offline de download da atualização. Sua desativação pode causar falhas na entrega da atualização aos dispositivos. Em determinados casos, o especialista de Suporte Técnico da Kaspersky pode recomendar que você desabilite a opção **Baixar atualizações e bancos de dados de antivírus do Servidor de Administração com antecedência**. Então, você terá que assegurar-se de que a tarefa para receber atualizações para aplicativos Kaspersky foi configurada.

Para ativar ou desativar o modelo offline de download da atualização para um grupo de administração:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique em **Grupos**.
3. Na estrutura de grupos de administração, selecione o grupo de administração para o qual você precisa ativar o modelo off-line para o download das atualizações.

4. Clique na política do Agente de Rede.

   A janela de propriedades da política do Agente de Rede se abre.

   Por padrão, as configurações de políticas secundárias são herdadas das políticas principais e não podem ser modificadas. Se a política que você deseja modificar for herdada, primeiro será necessário criar uma nova política para o Agente de Rede no grupo de administração necessário. Na política recém-criada, você pode modificar as configurações que não estão bloqueadas na política principal.

5. Na guia **Configurações do aplicativo**, selecione a seção **Gerenciar patches e atualizações**.

6. Ative ou desative a opção **Fazer antecipadamente o download das atualizações e dos bancos de dados de antivírus via Servidor de Administração (recomendado)** para ativar ou desativar, respectivamente, o modelo offline de download da atualização.

   Por padrão, o modelo offline para download das atualizações está ativado.

O modelo offline de download da atualização será ativado ou desativado.

Atualização de bancos de dados e módulos de software da Kaspersky em dispositivos offline

A atualização dos bancos de dados e dos módulos de software da Kaspersky em dispositivos gerenciados é uma tarefa importante para manter a proteção dos dispositivos contra vírus e outras ameaças. Os administradores normalmente configuram atualizações regulares por meio do uso do repositório do Servidor de Administração ou repositórios de pontos de distribuição.

Quando for preciso atualizar bancos de dados e módulos do software em um dispositivo (ou um grupo de dispositivos) que não está conectado ao Servidor de Administração (principal ou secundário), a um ponto de distribuição ou à Internet, você terá de usar fontes alternativas de atualizações, como um servidor FTP ou uma pasta local. Nesse caso, você precisa entregar os arquivos das atualizações necessárias usando um dispositivo de armazenamento em massa, como um pen drive ou um disco rígido externo.

Você pode copiar as atualizações necessárias de:

- O Servidor de Administração.

  Para ter certeza de que o repositório do Servidor de Administração contém as atualizações necessárias para o aplicativo de segurança instalado em um dispositivo offline, pelo menos um dos dispositivos online gerenciados deve ter o mesmo aplicativo de segurança instalado. Esse aplicativo deve ser configurado para receber as atualizações do repositório do Servidor de administração através da tarefa Baixar atualizações no repositório do Servidor de Administração.

- Qualquer dispositivo que tem o mesmo aplicativo de segurança instalado e configurado para receber as atualizações do repositório do Servidor de Administração, um repositório de ponto de distribuição ou diretamente dos servidores de atualização Kaspersky.

Abaixo há um exemplo de configuração de atualizações de bancos de dados e módulos de software copiando-os do repositório do Servidor de Administração.

Para atualizar os bancos de dados e módulos de software da Kaspersky em dispositivos offline:

1. Conecte a unidade removível ao dispositivo onde o Servidor de Administração está instalado.

2. Copie os arquivos de atualizações para a unidade removível.

   Por padrão, as atualizações estão localizadas em: \\<nome do servidor>\KLSHARE\Updates.

   Como alternativa, você pode configurar o Kaspersky Security Center para copiar regularmente as atualizações para a pasta selecionada. Para isso, use a opção **Copiar as atualizações baixadas em pastas adicionais** nas propriedades da tarefa Baixar atualizações no repositório do Servidor de Administração. Se você especificar uma pasta localizada em um pendrive ou um disco rígido externo como uma pasta de destino dessa opção, esse dispositivo de armazenamento em massa sempre conterá a versão mais recente das atualizações.

3. Em dispositivos offline, configure o aplicativo de segurança (por exemplo, Kaspersky Endpoint Security for Windows) para receber atualizações de uma pasta local ou um recurso compartilhado, como um Servidor FTP ou uma pasta compartilhada.

4. Copie os arquivos de atualizações da unidade removível para a pasta local ou o recurso compartilhado que deseja usar como uma fonte de atualização.

5. No dispositivo offline que requer a instalação de atualização, inicie a tarefa de atualização do Kaspersky Endpoint Security for Windows.

Depois que a tarefa de atualização for concluída, os bancos de dados e os módulos de software da Kaspersky serão atualizados no dispositivo.

Fazendo backup e restaurando plug-ins da web

O Kaspersky Security Center Web Console permite fazer backup do estado atual de um plug-in da web para poder restaurar o estado salvo posteriormente. Por exemplo, é possível fazer backup de um plug-in da web antes de atualizá-lo para uma versão mais recente. Após a atualização, caso a versão mais recente não atenda aos requisitos ou expectativas, será possível restaurar a versão anterior do plug-in da web a partir do backup.

Para fazer backup de plug-ins da web:

1. No menu principal, vá para **Configurações do console** → **Plug-ins da web**.

   A janela **Configurações do console** se abre.

2. Na guia **Plug-ins da web**, selecione os plug-ins da web que deseja fazer backup e clique no botão **Criar cópia backup**.

Os plug-ins da web selecionados são submetidos a backup. É possível visualizar os backups criados na aba **Backups**.

Para restaurar um plug-in da web a partir de um backup:

1. No menu principal, vá para **Configurações do console** → **Backups**.

   A janela **Configurações do console** se abre.

2. Na guia **Backups**, selecione o backup do plug-in da web que deseja restaurar e clique no botão **Restaurar do backup**.

O plug-in da web é restaurado a partir do backup selecionado.

Ajuste de pontos de distribuição e gateways de conexão

Uma estrutura de grupos de administração no Kaspersky Security Center executa as seguintes funções:

- Define o escopo das políticas

  Há um modo alternativo para aplicar configurações relevantes nos dispositivos, usando *perfis de política*. Neste caso, defina o escopo das políticas com tags, localizações de dispositivos nas unidades organizacionais do Active Directory ou associação nos grupos de segurança do Active Directory.

- Define o escopo da tarefas de grupo

  Há uma abordagem para definir o escopo da tarefas de grupo que não tem base em uma hierarquia de grupos de administração: uso de tarefas para seleções de dispositivos e tarefas para dispositivos específicos.

- Define os direitos de acesso aos dispositivos, Servidores de Administração virtuais e Servidores de Administração secundários

- Atribui os pontos de distribuição

Ao criar a estrutura de grupos de administração, você deve levar em conta a topologia da rede da organização para a atribuição ótima de pontos de distribuição. A distribuição ótima dos pontos de distribuição permite poupar tráfego na rede da organização.

Dependendo do esquema da organização e da topologia da rede, as seguintes configurações padrão podem ser aplicadas à estrutura de grupos de administração:

- Escritório único

- Múltiplos pequenos escritórios remotos

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Configuração padrão de pontos de distribuição: escritório único

Em uma configuração de "escritório único" padrão, todos os dispositivos estão dentro da rede da organização, portanto eles podem se "ver" mutuamente. A rede da organização pode consistir em algumas partes separadas (redes ou segmentos de rede) vinculadas por canais estreitos.

Os seguintes métodos de criar a estrutura de grupos de administração são possíveis:

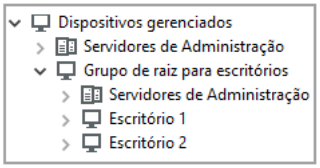
- Criar uma estrutura de grupos de administração levando em consideração a topologia da rede. A estrutura de grupos de administração pode não refletir a topologia da rede com uma precisão absoluta. Uma coincidência entre as partes separadas da rede e determinados grupos de administração seria suficiente. Você pode usar a atribuição automática de pontos de distribuição ou atribui-los manualmente.

- Criar uma estrutura de grupos de administração não levando em consideração a topologia da rede. Nesse caso, é necessário desativar a atribuição automática de pontos de distribuição e, a seguir, atribuir um ou diversos dispositivos para atuar como pontos de distribuição de um grupo de administração raiz em cada uma das partes separadas da rede, por exemplo, para o grupo **Dispositivos gerenciados**. Todos os pontos de distribuição estarão no mesmo nível e apresentarão a mesma expansão de escopo para todos os dispositivos na rede da organização. Nesse caso, cada Agente de Rede se conectará ao ponto de distribuição que tenha a rota mais curta. A rota para um ponto de distribuição pode ser traçada com o utilitário tracert.

Configuração padrão de pontos de distribuição: múltiplos pequenos escritórios remotos

Esta configuração padrão proporciona uma série de pequenos escritórios remotos, que podem se comunicar com a sede através da Internet. Cada escritório remoto é localizado além da NAT, ou seja, a conexão de um escritório remoto ao outro não é possível porque os escritórios estão isolados entre si.

A configuração deve ser refletida na estrutura de grupos de administração: um grupo de administração separado deve ser criado para cada escritório remoto (grupos **Escritório 1** e **Escritório 2** na figura abaixo).



Os escritórios remotos estão incluídos na estrutura do grupo de administração

Um ou vários pontos de distribuição devem ser atribuídos à cada grupo de administração que corresponda a um escritório. Os pontos de distribuição devem ser dispositivos nos escritórios remotos que têm espaço livre suficiente em disco. Os dispositivos implementados no grupo **Escritório 1**, por exemplo, acessarão os pontos de distribuição atribuídos ao grupo de administração **Escritório 1**.

Se alguns usuários se moverem entre escritórios fisicamente, com os seus computadores portáteis, você deve selecionar dois ou mais dispositivos (além dos pontos de distribuição existentes) em cada escritório remoto e atribui-los para atuar como pontos de distribuição para um grupo de administração de nível superior (**Grupo de raiz para escritórios** na figura acima).

Exemplo: Um computador portátil é implementado no grupo de administração **Escritório 1** e então é movido fisicamente para o escritório que corresponde ao grupo de administração **Escritório 2**. Após o computador portátil ter sido movido, o Agente de Rede tenta acessar os pontos de distribuição atribuídos ao grupo **Escritório 1**, mas aqueles pontos de distribuição estão indisponíveis. Então, O Agente de Rede começa a tentar acessar os pontos de distribuição que foram atribuídos ao **Grupo de raiz para escritórios**. Como os escritórios remotos estão isolados entre si, as tentativas de acessar os pontos de distribuição atribuídos ao grupo de administração **Grupo raiz para escritórios** somente terão êxito quando o Agente de Rede tentar acessar os pontos de distribuição no grupo **Escritório 2**. Ou seja, o computador portátil permanecerá no grupo de administração que corresponde ao escritório inicial, mas o computador portátil usará o ponto de distribuição do escritório onde estiver fisicamente localizado no momento.

Sobre os pontos de distribuição atribuídos

É possível atribuir um dispositivo gerenciado como um ponto de distribuição manualmente ou automaticamente.

Caso um dispositivo gerenciado como um ponto de distribuição seja atribuído manualmente, será possível selecionar qualquer dispositivo na rede.

Caso os pontos de distribuição sejam atribuídos automaticamente, o Kaspersky Security Center poderá selecionar apenas o dispositivo gerenciado que atenda às seguintes condições:

- O dispositivo tem ao menos 50 GB de espaço livre no disco.
- O dispositivo gerenciado é conectado diretamente ao Kaspersky Security Center (não pelo gateway).
- O dispositivo gerenciado não é um laptop.

> Caso a rede não tenha dispositivos que atendam às condições especificadas, o Kaspersky Security Center não atribuirá nenhum dispositivo como ponto de distribuição automaticamente.

Atribuir os pontos de distribuição automaticamente

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos.

Para atribuir os pontos de distribuição automaticamente:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Selecione a opção **Atribuir automaticamente os pontos de distribuição**.

   > Se a atribuição automática dos dispositivos para agirem como pontos de distribuição estiver ativada, você não pode configurar manualmente os pontos de distribuição nem editar a lista de pontos de distribuição.

4. Clique no botão **Salvar**.

O Servidor de Administração atribui e configura automaticamente os pontos de distribuição.

Atribuir os pontos de distribuição manualmente

O Kaspersky Security Center permite que você atribua dispositivos manualmente para agirem como pontos de distribuição.

Recomendamos que você atribua pontos de distribuição automaticamente. Neste caso, o Kaspersky Security Center selecionará por si só quais dispositivos devem ser pontos de distribuição atribuídos. No entanto, se você tiver de optar por não atribuir pontos de distribuição automaticamente por algum motivo (por exemplo, se você quiser usar servidores exclusivamente atribuídos), poderá atribuir manualmente os pontos de distribuição após calcular seu número e configuração.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Para atribuir manualmente os dispositivos para agir como ponto de distribuição:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Selecione a opção **Atribuir manualmente os pontos de distribuição**.

4. Clique no botão **Atribuir**.

5. Selecione o dispositivo que você quer atribuir como ponto de distribuição.

   Ao selecionar um dispositivo, tenha em mente os recursos da operação de pontos de distribuição e os requisitos definidos para o dispositivo que age como ponto de distribuição.

6. Selecione o grupo de administração que você quer incluir no escopo do ponto de distribuição selecionado.

7. Clique no botão **OK**.

   O pontos de distribuição que você adicionou será exibido na lista de pontos de distribuição na seção **Pontos de distribuição**.

8. Clique no ponto de distribuição recém-adicionado na lista para abrir sua janela de propriedades.

9. Configure o ponto de distribuição na janela de propriedades:

- A seção **Geral** contém a configuração de interação entre o ponto de distribuição e os dispositivos clientes:
  - **Porta SSL**

    O número da porta SSL para a conexão criptografada entre dispositivos clientes e o ponto de distribuição usando SSL.

    Por padrão, a porta 13000 é usada.

  - **Usar multicast**

    Se esta opção estiver ativada, o IP multicasting será usado para distribuição automática de pacotes de instalação para dispositivos clientes dentro do grupo.

    O multicast de IP diminui o tempo necessário para instalar um aplicativo de um pacote de instalação em um grupo de dispositivos clientes, mas aumenta o tempo de instalação quando você instala um aplicativo em um único dispositivo cliente.

  - **Endereço IP multicast**

    O endereço IP que será usado para multicasting. Você pode definir um endereço IP no conjunto de 224.0.0.0 – 239.255.255.255

    Por padrão, o Kaspersky Security Center atribui automaticamente um endereço IP multicast exclusivo dentro do conjunto especificado.

  - **Número da porta de IP multicast**

    Número da porta para multicasting de IP.

    Por padrão, o número de porta é 15001. Se o dispositivo com o Servidor de Administração instalado for especificado como o ponto de distribuição, por padrão a porta 13001 é usada para conexão SSL.

  - **Endereço do ponto de distribuição para dispositivos remotos**

    O endereço IPv4 por meio do qual os dispositivos remotos estabelecem conexão com o ponto de distribuição.

  - **Implementar atualizações**

As atualizações são distribuídas para dispositivos gerenciados a partir das seguintes fontes:

- Este ponto de distribuição, caso esta opção esteja ativada.
- Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

Caso utilize os pontos de distribuição para implantar atualizações, será possível economizar tráfego, pois o número de downloads será reduzido. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. É possível calcular o número de pontos de distribuição para a rede e otimizar o tráfego e a carga.

Caso essa opção seja desativada, o número de downloads de atualização e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

- **Implementar pacotes de instalação**

Os pacotes de instalação são distribuídos para dispositivos gerenciados a partir das seguintes fontes:

- Este ponto de distribuição, caso esta opção esteja ativada.
- Outros pontos de distribuição, o Servidor de Administração ou os servidores de atualização da Kaspersky, caso esta opção esteja desativada.

Se você usar pontos de distribuição para implementar pacotes de instalação, poderá economizar tráfego porque reduz o número de downloads. Além disso, é possível aliviar a carga no Servidor de Administração e realocar a carga entre os pontos de distribuição. É possível calcular o número de pontos de distribuição para a rede e otimizar o tráfego e a carga.

Caso essa opção seja desativada, o número de downloads de pacotes de instalação e a carga no Servidor de Administração podem aumentar. Por padrão, esta opção está ativada.

- **Executar servidor push**

No Kaspersky Security Center, um ponto de distribuição pode funcionar como um servidor push para os dispositivos gerenciados por meio do protocolo móvel e para os dispositivos gerenciados pelo Agente de Rede. Por exemplo, um servidor push deve ser ativado se você quiser forçar a sincronização dos dispositivos KasperskyOS com o Servidor de Administração. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Se você tiver vários pontos de distribuição atribuídos ao mesmo grupo de administração, poderá ativar o servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

- **Porta do servidor push**

O número da porta para o servidor push. É possível especificar o número de qualquer porta livre.

- Na seção **Escopo**, especifique o escopo ao qual o ponto de distribuição distribuirá as atualizações (grupos de administração e/ou um local de rede).

Somente os dispositivos sendo executados no sistema operacional Windows podem determinar a sua localização na rede. A localização da rede não pode ser determinada para dispositivos que executam outros sistemas operacionais.

- Caso o ponto de distribuição funcione em uma máquina diferente do Servidor de Administração, na seção **Fonte de atualizações**, é possível selecionar uma fonte de atualizações para o ponto de distribuição:

  - **Fonte de atualizações**

    Selecione uma fonte de atualizações para o ponto de distribuição:

    - Para permitir que o ponto de distribuição receba atualizações do Servidor de Administração, selecione **Obter do Servidor de Administração**.
    - Para permitir que o ponto de distribuição receba atualizações usando uma tarefa, selecione **Usar tarefa de download de atualizações** e, em seguida, especifique a tarefa *Baixar atualizações para os repositórios de pontos de distribuição*:
      - Se essa tarefa já existir no dispositivo, selecione a tarefa na lista.
      - Se ainda não existir tal tarefa no dispositivo, clique no link **Criar tarefa** para criar uma tarefa. O Assistente para novas tarefas inicia. Siga as instruções do Assistente.

  - **Baixar arquivos diff**

    Esta opção ativa o recurso de download dos arquivos diff.

    Por padrão, esta opção está ativada.

- Caso seus pontos de distribuição usem o servidor proxy para se conectar à internet, na subseção **Configurações de conexão com a internet**, você poderá especificar as seguintes configurações:

  - **Usar o servidor proxy**

    Se esta caixa de seleção estiver selecionada, você pode configurar nos campos de entrada a conexão ao servidor proxy.

    Por padrão, esta caixa de seleção está desmarcada.

  - **Endereço do servidor proxy**

    Endereço do servidor proxy.

  - **Número da porta**

    O número da porta que é usada para conexão.

  - **Ignorar servidor proxy para endereços locais**

    Se esta opção estiver ativada, nenhum servidor proxy será usado para se conectar aos dispositivos na rede local.

    Por padrão, esta opção está desativada.

  - **Autenticação do servidor proxy**

Se esta caixa de seleção estiver selecionada, você poderá especificar os credenciais para a autenticação do servidor proxy.

Por padrão, esta caixa de seleção está desmarcada.

- **Nome do usuário**

  Conta do usuário sob a qual a conexão ao servidor proxy é estabelecida.

- **Senha**

  Senha da conta sob a qual a tarefa será executada.

- Na seção **Proxy da KSN**, você pode configurar o aplicativo para usar o ponto de distribuição para encaminhar solicitações do KSN a partir dos dispositivos gerenciados:

  - **Ativar Proxy KSN no lado do ponto de distribuição**

    O serviço Proxy da KSN é executado no dispositivo que é usado como um ponto de distribuição. Use este recurso para redistribuir e otimizar o tráfego na rede.

    O ponto de distribuição envia as estatísticas da KSN, que são listadas na Declaração da Kaspersky Security Network, à Kaspersky. Por padrão, a Declaração da KSN está localizada em %ProgramFiles%\Kaspersky Lab\Kaspersky Security Center\ksneula.

    Por padrão, esta opção está desativada. A ativação desta opção somente terá efeito se as opções **Usar Servidor de Administração como um servidor proxy** e **Concordo em usar a Kaspersky Security Network** estiverem ativadas na janela de propriedades do Servidor de Administração.

    É possível atribuir um nó de um cluster ativo-passivo a um ponto de distribuição e habilitar o servidor proxy da KSN nesse nó.

  - **Encaminhar solicitações da KSN para o Servidor de Administração**

    O ponto de distribuição encaminha solicitações do KSN dos dispositivos gerenciados para o Servidor de Administração.

    Por padrão, esta opção está ativada.

  - **Acessar a KSN Cloud/KSN Privada diretamente pela internet**

    O ponto de distribuição encaminha solicitações à KSN dos dispositivos gerenciados para a KSN Cloud ou KSN Privada. As solicitações KSN geradas no próprio ponto de distribuição também são enviadas diretamente à KSN Cloud ou à KSN Privada.

    Os pontos de distribuição com o Agente de Rede versão 11 (ou anterior) instalado não podem acessar diretamente a KSN Privada. Se você deseja reconfigurar os pontos de distribuição para enviar solicitações à KSN à KSN Privada, ative a opção **Encaminhar solicitações da KSN para o Servidor de Administração** para cada ponto de distribuição.

    Os pontos de distribuição com o Agente de Rede versão 12 (ou posterior) instalado podem acessar diretamente a KSN Privada.

  - **Ignorar configurações do Servidor Proxy ao conectar à KSN Privada**

Ative esta opção, se tiver as configurações do servidor proxy definidas nas propriedades do ponto de distribuição ou na política do Agente de Rede, mas sua arquitetura de rede requer o uso direto da KSN Privada. Caso contrário, as solicitações dos aplicativos gerenciados não alcançarão a KSN Privada.

Esta alternativa estará disponível caso a opção **Acessar a KSN Cloud/KSN Privada diretamente pela internet** seja selecionada.

- **Porta**

  O número da porta TCP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. O número da porta padrão é 13111.

- **Usar porta UDP**

  Se você desejar que os dispositivos gerenciados sejam conectados ao proxy da KSN através de uma porta UDP, ative a opção **Usar porta UDP** e especifique um número de Porta UDP. Por padrão, esta opção está ativada.

- **Porta UDP**

  O número da porta UDP que os dispositivos gerenciados utilizarão para conectarem-se ao servidor proxy KSN. A porta UDP padrão para se conectar ao servidor proxy KSN é 15111.

- Caso o ponto de distribuição funcione em uma máquina diferente do Servidor de Administração, na seção **Gateway de conexão**, será possível configurar o ponto de distribuição para atuar como um gateway para conexão entre as instâncias do Agente de Rede e o Servidor de Administração:

  - **Gateway de conexão**

    Caso uma conexão direta entre o Servidor de Administração e os Agentes de Rede não possa ser estabelecida em função da organização de sua rede, será possível usar o ponto de distribuição para atuar como o gateway de conexão entre o Servidor de Administração e os Agentes de Rede.

    Ative essa opção caso você precise que o ponto de distribuição atue como um gateway de conexão entre os Agentes de Rede e o Servidor de Administração. Por padrão, esta opção está desativada.

  - **Estabelecer conexão com o gateway a partir do Servidor de Administração (se o gateway estiver na DMZ)**

    Caso o Servidor de Administração esteja localizado fora da zona desmilitarizada (DMZ), na rede local, os Agentes de Rede instalados em dispositivos remotos não poderão se conectar com o Servidor de Administração. É possível usar um ponto de distribuição como o gateway de conexão com conectividade reversa (o Servidor de Administração estabelece uma conexão com o ponto de distribuição).

    Ative essa opção caso seja necessário conectar o Servidor de Administração ao gateway de conexão na DMZ.

  - **Abrir porta local do Kaspersky Security Center 14 Web Console**

Ative essa opção caso seja necessário que o gateway de conexão na DMZ abra uma porta para o Web Console que esteja na DMZ ou na Internet. Especifique o número da porta que será usada para conexão do Web Console com o ponto de distribuição. O número da porta padrão é 13299.

Essa opção estará disponível caso a opção **Estabelecer conexão com o gateway a partir do Servidor de Administração (se o gateway estiver na DMZ)** seja ativada.

Ao conectar os dispositivos móveis com o Servidor de Administração por meio do ponto de distribuição que atua como gateway de conexão, é possível ativar as seguintes opções:

- **Abrir porta para dispositivos móveis (apenas autenticação SSL do Servidor de Administração)**

  Ative essa opção caso seja necessário que o gateway de conexão abra uma porta para dispositivos móveis e especifique o número da porta que os dispositivos móveis usarão para estabelecer conexão com o ponto de distribuição. O número da porta padrão é 13292. O dispositivo móvel verificará o certificado do Servidor de Administração. Ao estabelecer a conexão, somente o Servidor de Administração será autenticado.

- **Abrir porta para dispositivos móveis (autenticação SSL bidirecional)**

  Ative essa opção caso seja necessário que o gateway de conexão abra uma porta que será usada para autenticação bidirecional do Servidor de Administração e dispositivos móveis. O dispositivo móvel verificará o certificado do Servidor de Administração e o Servidor de Administração verificará o certificado de dispositivos móveis. Especifique os seguintes parâmetros:

  - Número da porta que os dispositivos móveis usarão para conexão com o ponto de distribuição. O número da porta padrão é 13293.
  - Nomes de domínio DNS do gateway de conexão que serão usados por dispositivos móveis. Separe os nomes de domínio com vírgulas. Os nomes de domínio especificados serão incluídos no certificado do ponto de distribuição. Caso os nomes de domínio usados pelos dispositivos móveis não correspondam ao nome comum no certificado do ponto de distribuição, os dispositivos móveis não se conectarão com ponto de distribuição.

    O nome de domínio DNS padrão é o nome FQDN do gateway de conexão.

Em ambos os casos, os certificados serão verificados durante o estabelecimento da sessão TLS somente no ponto de distribuição. Os certificados não são encaminhados para serem verificados pelo Servidor de Administração. Depois que uma sessão TLS é estabelecida com o dispositivo móvel, o ponto de distribuição usa o certificado do Servidor de Administração para criar um túnel para sincronização entre o dispositivo móvel e o Servidor de Administração. Caso a porta para autenticação SSL bidirecional seja aberta, a única maneira de distribuir o certificado de dispositivos móveis é por meio de um pacote de instalação.

- Configure a amostragem de domínios do Windows, Active Directory e faixas IP pelo ponto de distribuição:

  - **Domínios do Windows**

    Você pode ativar a descoberta de dispositivos para domínios do Windows e definir o agendamento para a localização.

  - **Active Directory**

Você pode ativar a sondagem da rede para o Active Directory e definir o agendamento da sondagem.

Se você usar um ponto de distribuição do Windows, poderá selecionar uma das seguintes opções:

- **Sondar o domínio atual do Active Directory**.
- **Sondar a floresta de domínios do Active Directory**.
- **Criar sondagem apenas de domínios selecionados do Active Directory**. Se você selecionar esta opção, adicione um ou mais domínios do Active Directory à lista.

Se você usar um ponto de distribuição do Linux com o Agente de Rede versão 15 instalado, poderá sondar somente domínios do Active Directory para os quais o endereço e as credenciais do usuário foram especificados. A sondagem do domínio atual do Active Directory e da floresta de domínios do Active Directory não está disponível.

- Intervalos de IP

  Você pode ativar a descoberta de dispositivos para conjuntos IPv4 e redes IPv6.

  Ao ativar a opção **Ativar sondagem de conjuntos**, você poderá adicionar conjuntos verificados e definir seu agendamento. Você pode adicionar conjuntos de IPs à lista de conjuntos verificados.

  Ao ativar a opção **Usar Zeroconf para sondar redes IPv6**, o ponto de distribuição sonda automaticamente a rede IPv6 usando rede zero configuração (também referida como *Zeroconf*). Nesse caso, os conjuntos IP especificados são ignorados, pois o ponto de distribuição sonda toda a rede. A opção **Usar Zeroconf para sondar redes IPv6** estará disponível caso o ponto de distribuição execute Linux. Para usar a sondagem do Zeroconf IPv6, é necessário instalar o utilitário avahi-browse no ponto de distribuição.

- Na seção **Avançado**, especifique a pasta que o ponto de distribuição deverá usar para armazenar dados distribuídos:

  - Usar pasta padrão

    Se você selecionar esta opção, o aplicativo usa a pasta de Instalação do Agente de Rede no ponto de distribuição.

  - Usar pasta especificada

    Se selecionar esta opção, você pode, no campo abaixo, especificar o caminho até a pasta. Pode ser uma pasta local no ponto de distribuição ou pode ser uma pasta em qualquer dispositivo na rede corporativa.

    A conta do usuário usada no ponto de distribuição para executar o Agente de Rede deve ter acesso de leitura/gravação à pasta especificada.

10. Clique no botão **OK**.

Os dispositivos selecionados agirão como pontos de distribuição.

Modificar a lista de pontos de distribuição para um grupo de administração

Você pode visualizar a lista de pontos de distribuição atribuídos a um grupo de administração específico e modificá-la adicionando ou removendo pontos de distribuição.

Para visualizar e modificar a lista de pontos de distribuição atribuídos a um grupo de administração:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. No campo **Caminho atual**, acima da lista de dispositivos gerenciados, clique no link do caminho.
3. No painel aberto à esquerda, selecione o grupo de administração para o qual deseja visualizar os pontos de distribuição atribuídos.

   Isso ativa o item de menu **Pontos de distribuição**.
4. No menu principal, vá para **Dispositivos** → **Pontos de distribuição**.
5. Para adicionar novos pontos de distribuição para o grupo de administração, clique no botão **Atribuir** acima da lista de dispositivos gerenciados e selecione os dispositivos no painel que se abre.
6. Para remover os pontos de distribuição atribuídos, selecione os dispositivos na lista e clique no botão **Desatribuir**.

Dependendo das suas modificações, os novos pontos de distribuição serão adicionados à lista ou os pontos de distribuição existentes serão removidos da lista.

Sincronização forçada

Embora o Kaspersky Security Center sincronize automaticamente status, configurações, tarefas e políticas dos dispositivos gerenciados, em alguns casos você pode querer forçar a sincronização para um dispositivo especificado. Você pode executar a sincronização forçada para os seguintes dispositivos:

- Dispositivos com Agente de Rede instalado
- Dispositivos executando o KasperskyOS

  Antes de executar a sincronização forçada para um dispositivo KasperskyOS, certifique-se de que o dispositivo está incluído em um escopo de ponto de distribuição e que um servidor push está ativado no ponto de distribuição.
- Dispositivos iOS
- Dispositivos Android

  Antes de executar a sincronização forçada para um dispositivo Android, você deve configurar o Firebase Cloud Messaging.

Sincronizar um único dispositivo

Para forçar a sincronização entre o Servidor de Administração e um dispositivo gerenciado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo que deseja sincronizar com o Servidor de Administração.

   Uma janela de propriedades é exibida com a seção **Geral** selecionada.
3. Clique no botão **Forçar a sincronização**.

O aplicativo sincroniza o dispositivo selecionado com o Servidor de Administração.

Sincronizar vários dispositivos

Para forçar a sincronização entre o Servidor de Administração e vários dispositivos gerenciados:

1. Abra a lista de dispositivos de um grupo de administração ou uma seleção de dispositivos:
   - No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**, clique no link do caminho no campo **Caminho atual** acima da lista de dispositivos gerenciados e, a seguir, selecione o grupo de administração que contém os dispositivos a serem sincronizados.
   - Execute uma seleção de dispositivos para visualizar a lista de dispositivos.
2. Marque as caixas de seleção ao lado dos dispositivos que deseja sincronizar com o Servidor de Administração.
3. Acima da lista de dispositivos gerenciados, clique no botão de reticências (**...**) e, a seguir, clique no botão **Forçar a sincronização**.

   O aplicativo sincroniza os dispositivos selecionados com o Servidor de Administração.
4. Na lista de dispositivos, verifique se a hora da última conexão com o Servidor de Administração foi alterada para os dispositivos selecionados para a hora atual. Se a hora não tiver sido alterada, atualize o conteúdo da página clicando no botão **Atualizar**.

Os dispositivos selecionados são sincronizados com o Servidor de Administração.

Visualização da hora da entrega de uma política

Após alterar uma política de um aplicativo da Kaspersky no Servidor de Administração, o administrador pode verificar se a política alterada foi entregue a um dispositivo gerenciado específico. Uma política pode ser entregue durante uma sincronização normal ou uma sincronização forçada.

Para visualizar a data e a hora que uma política de aplicativo foi fornecida a um dispositivo gerenciado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo que deseja sincronizar com o Servidor de Administração.

   Uma janela de propriedades é exibida com a seção **Geral** selecionada.

3. Selecione a guia **Aplicativos**.

4. Selecione o aplicativo do qual do qual deseja visualizar a data de sincronização da política.

   A janela de política do aplicativo é exibida com a seção **Geral** selecionada e a data e a hora de entrega da política exibidas.

Ativando um servidor push

No Kaspersky Security Center, um ponto de distribuição pode funcionar como um servidor push para os dispositivos gerenciados por meio do protocolo móvel e para os dispositivos gerenciados pelo Agente de Rede. Por exemplo, um servidor push deve ser ativado se você quiser forçar a sincronização dos dispositivos KasperskyOS com o Servidor de Administração. Um servidor push tem o mesmo escopo de dispositivos gerenciados que o ponto de distribuição no qual o servidor push está ativado. Se você tiver vários pontos de distribuição atribuídos ao mesmo grupo de administração, poderá ativar o servidor push em cada um dos pontos de distribuição. Nesse caso, o Servidor de Administração equilibra a carga entre os pontos de distribuição.

É possível querer usar pontos de distribuição como servidores push para garantir que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração. A conectividade contínua é necessária para algumas operações, como executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado ou criar um túnel. Caso um ponto de distribuição seja usado como servidor push, não será necessário usar a opção **Não desconecte do Servidor de Administração** nos dispositivos gerenciados ou enviar pacotes para a porta UDP do agente de rede.

Um servidor push suporta a carga de até 50.000 conexões simultâneas.

Para ativar o servidor push em um ponto de distribuição:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Pontos de distribuição**.

3. Clique no nome do ponto de distribuição no qual deseja ativar o servidor push.

   A janela Propriedades do ponto de distribuição é aberta.

4. Na seção **Geral**, selecione a opção **Executar servidor push**.

5. No campo **Porta do servidor push**, digite o número da porta. Você pode especificar o número de qualquer porta livre.

6. No campo **Endereço para hosts remotos**, especifique o endereço IP ou o nome do dispositivo do ponto de distribuição.

7. Clique no botão **OK**.

O servidor push é ativado no ponto de distribuição selecionado.

Gerenciar aplicativos de terceiros em dispositivos cliente

Esta seção descreve os recursos do Kaspersky Security Center relacionados ao gerenciamento de aplicativos de terceiros instalados nos dispositivos cliente.

Sobre aplicativos de terceiros

O Kaspersky Security Center pode ajudar a atualizar o software de terceiros instalado em dispositivos clientes e corrigir as vulnerabilidades desse software. O Kaspersky Security Center pode atualizar o software de terceiros apenas da versão atual para a versão mais recente.

A lista de software de terceiros pode ser alterada e é atualizada dinamicamente. Você pode verificar se é possível atualizar o software de terceiros (instalado nos dispositivos dos usuários) com o Kaspersky Security Center visualizando a lista de atualizações disponíveis no Console de Administração baseado em MMC e no Kaspersky Security Center Web Console.

O procedimento descrito abaixo tem o único propósito de exibir a lista de softwares de terceiros que podem ser atualizados com o Kaspersky Security Center. As etapas são seguidas para acessar as informações relevantes sem ter de iniciar nenhuma tarefa.

Para visualizar a lista de software de terceiros que podem ser atualizados com o Kaspersky Security Center no Kaspersky Security Center Web Console:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Na etapa **Nova tarefa** do assistente, especifique as seguintes configurações:
   a. Na lista suspensa **Aplicativo**, selecione **Kaspersky Security Center**.
   b. No campo **Tipo de tarefa**, selecione **Instalar as atualizações necessárias e corrigir vulnerabilidades**.
4. Na etapa **Escopo da tarefa** do assistente, selecione a opção **Dispositivos gerenciados**.
5. Na etapa **Especificar regras para a instalação de atualizações** do assistente, clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
6. Na etapa **Selecionar o tipo de regra** do assistente, selecione a opção **Regra para atualizações de terceiros**.
7. Na etapa **Critérios gerais** do assistente, selecione a opção **Instalar todas as atualizações (exceto as recusadas)** e clique em **Avançar**.

A lista de softwares de terceiros será exibida.

Para visualizar a lista de software de terceiros que você pode atualizar com o Kaspersky Security Center no console baseado em MMC, você precisa da Licença de gerenciamento de patches e vulnerabilidades. Caso contrário, a tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades** não estará disponível.

1. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.
2. No espaço de trabalho, selecione a guia **Tarefas**.
3. Clique no botão **Criar uma tarefa** para executar o Assistente para novas tarefas. Siga as etapas do Assistente.
4. Na página **Selecionar o tipo de tarefa** do assistente, selecione **Instalar as atualizações necessárias e corrigir vulnerabilidades**.
5. Na etapa **Especificar regras para a instalação de atualizações** do assistente, clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
6. Na etapa **Selecionar o tipo de regra** do assistente, selecione a opção **Regra para atualizações de terceiros**.
7. Na etapa **Critérios gerais** do assistente, selecione a opção **Instalar todas as atualizações (exceto as recusadas)** e clique em **Avançar**.

A lista de softwares de terceiros será exibida.

Instalar atualizações de software de terceiros

O Kaspersky Security Center permite gerenciar as atualizações do software de terceiros instalado em dispositivos gerenciados e corrigir vulnerabilidade em aplicativos da Microsoft e de produtos de outros fornecedores através da instalação das atualizações necessárias.

O Kaspersky Security Center procura atualizações por meio da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Servidor de Administração recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa. Após visualizar as informações sobre as atualizações disponíveis, você pode instalar as mesmas nos dispositivos.

O Kaspersky Security Center atualiza alguns aplicativos ao remover a versão anterior do aplicativo e ao instalar uma nova versão.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Por motivos de segurança, todas as atualizações de softwares de terceiros instaladas usando o recurso Gerenciamento de patches e vulnerabilidades são verificadas automaticamente pelas tecnologias da Kaspersky em busca de malwares. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

Tarefas para instalação das atualizações de software de terceiros

Quando os metadados das atualizações de software de terceiros são baixados para o repositório, você pode instalar as atualizações nos dispositivos clientes usando as seguintes tarefas:

- A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*

  A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para instalar atualizações para aplicativos da Microsoft, incluindo as atualizações fornecidas pelo serviço Windows Update e atualizações de software de outros fornecedores. Observe que esta tarefa pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades.

  Quando essa tarefa é concluída, as atualizações são instaladas nos dispositivos gerenciados automaticamente. Quando os metadados das novas atualizações são baixados no repositório do Servidor de Administração, o Kaspersky Security Center verifica se as atualizações atendem aos critérios especificados nas regras de atualização. Todas as novas atualizações que atendem aos critérios serão baixadas e instaladas automaticamente na próxima tarefa executada.

- A tarefa *Instalar as atualizações do Windows Update*

  A tarefa *Instalar as atualizações do Windows Update* não requer uma licença, mas pode ser usada para instalar apenas atualizações do Windows Update.

  Quando esta tarefa é concluída, apenas as atualizações especificadas nas propriedades da tarefa são instaladas. No futuro, caso deseje instalar novas atualizações baixadas no repositório do Servidor de Administração, será preciso adicionar as atualizações necessárias à lista de atualizações da tarefa existente ou criar uma nova tarefa Instalar atualizações do Windows Update.

Usar Servidor de Administração como servidor WSUS

As informações sobre atualizações disponíveis são fornecidas pelo serviço do Windows Update. O Servidor de Administração pode ser usado como um servidor Windows Server Update Services (WSUS). Para usar o Servidor de Administração como o servidor WSUS, crie a tarefa de sincronização Executar a sincronização do Windows Update e selecione a opção **Usar o Servidor de Administração como servidor WSUS** na política do Agente de Rede. Após ter configurado a sincronização dos dados com o Windows Update, o Servidor de Administração fornece atualizações de serviços do Windows Update nos dispositivos no modo centralizado e com a frequência definida.

Instalar atualizações de software de terceiros

É possível instalar atualizações de softwares de terceiros em dispositivos gerenciados criando e executando uma das seguintes tarefas:

- *Instalar as atualizações necessárias e corrigir vulnerabilidades*

  A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades. Você pode usar esta tarefa para instalar atualizações do Windows Update fornecidas pela Microsoft e atualizações de software de outros fornecedores.

- *Instalar as atualizações do Windows Update*

  Você pode usar a tarefa *Instalar as atualizações do Windows Update* para instalar apenas atualizações do Windows Update.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Como opção, é possível criar uma tarefa para instalar as atualizações necessárias das seguintes maneiras:

- Abrindo a lista de atualizações e especificando quais atualizações instalar.

  Como resultado, é criada uma nova tarefa para instalar as atualizações selecionadas. Como opção, você pode adicionar as atualizações selecionadas a uma tarefa existente.

- Executando o assistente de Instalação de atualizações.

  O Assistente de instalação das Atualizações só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

  O assistente simplifica a criação e a configuração de uma tarefa de instalação de atualização e permite eliminar a criação de tarefas redundantes que contenham as mesmas atualizações para instalação.

Instalar atualizações de softwares de terceiros usando a lista de atualizações

Para instalar atualizações de software de terceiros usando a lista de atualizações:

1. Abra uma das listas de atualizações:

   - Para abrir a lista geral de atualização, No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

   - Para abrir a lista de atualização para um dispositivo gerenciado, No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados** → <nome do dispositivo> → **Avançado** → **Atualizações disponíveis**.

   - Para abrir a lista de atualização para um aplicativo específico, No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos** → <nome do aplicativo> → **Atualizações disponíveis**.

   Aparece uma lista das atualizações disponíveis.

2. Marque as caixas de seleção ao lado das atualizações que deseja baixar.

3. Clique no botão **Instalar as atualizações**.

   Para instalar algumas atualizações de software, você deve aceitar o Contrato de Licença do Usuário Final (EULA). Se você recusar o EULA, a atualização do software não é instalada.

4. Selecione uma das seguintes opções:

   - **Nova tarefa**

     O Assistente para novas tarefa inicia. Se você tiver a licença do Gerenciamento de patches e vulnerabilidades, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será pré-selecionada. Se você não tiver a licença, a tarefa *Instalar as atualizações do Windows Update* será pré-selecionada. Seguem abaixo as etapas do assistente para concluir a criação da tarefa.

   - **Instalar a atualização (adicionar a regra à tarefa especificada)**

     Selecione uma tarefa à qual deseja adicionar as atualizações selecionadas. Se você tiver a licença de Gerenciamento de patches e vulnerabilidades, selecione a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Uma nova regra para instalar as atualizações selecionadas será adicionada automaticamente à tarefa escolhida. Se você não tiver a licença, selecione a tarefa *Instalar as atualizações do Windows Update*. As atualizações selecionadas serão adicionadas às propriedades da tarefa.

     A janela de propriedades da tarefa é aberta. Clique no botão **Salvar** para salvar as alterações.

   Se você escolheu criar uma nova tarefa, a tarefa será criada e exibida na lista de tarefas em **Dispositivos → Tarefas**. Se você optou por adicionar as atualizações a uma tarefa existente, as atualizações serão salvas nas propriedades da tarefa.

Para instalar atualizações de software de terceiros, inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. É possível iniciar qualquer uma dessas tarefas manualmente ou especificar configurações de agendamento nas propriedades da tarefa iniciada. Ao especificar o agendamento de tarefas, certifique-se de que a tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

Instalar atualizações de softwares de terceiros usando o assistente de Instalação de atualizações

O Assistente de instalação das Atualizações só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

Para criar uma tarefa para instalar atualizações de softwares de terceiros usando o assistente de Instalação de atualizações:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.

2. Marque a caixa de seleção ao lado da atualização que deseja instalar.

3. Clique no botão **Executar o assistente de instalação de atualização**.

   O Assistente de instalação de atualizações inicia. A página **Selecionar tarefa de instalação da atualização** exibe a lista de todas as tarefas existentes dos seguintes tipos:

   - *Instalar as atualizações necessárias e corrigir vulnerabilidades*
   - *Instalar as atualizações do Windows Update*
   - *Corrigir vulnerabilidades*

   Você não pode modificar as tarefas dos dois últimos tipos para instalar novas atualizações. Para instalar novas atualizações, você só pode usar as tarefas do tipo *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

4. Caso deseje que o assistente exiba apenas as tarefas que instalam a atualização selecionada, ative a opção **Exibir apenas tarefas que instalam esta atualização**.

5. Selecione o que deseja fazer:

   - Para iniciar uma tarefa, marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Iniciar**.
   - Para adicionar uma nova regra a uma tarefa existente:

     a. Marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Adicionar regra**.

     b. Na página aberta, configure a nova regra:

     - **Regra de instalação de atualizações deste nível de importância**

       Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

       Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

       Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

       Por padrão, esta opção está desativada.

     - **Regra de instalação de atualizações deste nível de importância de acordo com o MSRC**

       Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

       Se esta opção estiver ativada (disponível apenas para atualizações do Windows Update), as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

       Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

       Por padrão, esta opção está desativada.

     - **Regra de instalação para atualizações deste fornecedor**

       Esta opção está disponível apenas para atualizações de aplicativos de terceiros. O Kaspersky Security Center instala apenas as atualizações relacionadas aos aplicativos feitos pelo mesmo fornecedor que a atualização selecionada. As atualizações recusadas e as atualizações dos aplicativos feitos por outros fornecedores não são instaladas.

       Por padrão, esta opção está desativada.

     - **Regra de instalação para atualizações do tipo**
     - **Regra de instalação para a atualização selecionada**

- Aprovar atualizações selecionadas

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

- Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas

  Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

  Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

  Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

  Por padrão, esta opção está ativada.

c. Clique no botão **Adicionar**.

- Para criar uma tarefa:

  a. Clique no botão **Nova tarefa**.

  b. Na página aberta, configure a nova regra:

  - Regra de instalação de atualizações deste nível de importância

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

    Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

    Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

    Por padrão, esta opção está desativada.

  - Regra de instalação de atualizações deste nível de importância de acordo com o MSRC

Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

Se esta opção estiver ativada (disponível apenas para atualizações do Windows Update), as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

Por padrão, esta opção está desativada.

- Regra de instalação para atualizações deste fornecedor

  Esta opção está disponível apenas para atualizações de aplicativos de terceiros. O Kaspersky Security Center instala apenas as atualizações relacionadas aos aplicativos feitos pelo mesmo fornecedor que a atualização selecionada. As atualizações recusadas e as atualizações dos aplicativos feitos por outros fornecedores não são instaladas.

  Por padrão, esta opção está desativada.

- **Regra de instalação para atualizações do tipo**

- **Regra de instalação para a atualização selecionada**

- Aprovar atualizações selecionadas

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

- Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas

  Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

  Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

  Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

  Por padrão, esta opção está ativada.

c. Clique no botão **Adicionar**.

Se você optou por iniciar uma tarefa, poderá fechar o assistente. A tarefa será concluída no modo de segundo plano. Nenhuma outra ação será necessária.

Se você escolheu adicionar uma regra a uma tarefa existente, a janela de propriedades da tarefa é aberta. A nova regra já foi adicionada às propriedades da tarefa. Você pode visualizar ou modificar a regra ou outras configurações de tarefa. Clique no botão **Salvar** para salvar as alterações.

Caso tenha optado por criar uma tarefa, continue a criar a tarefa no assistente para Novas tarefas. A nova regra adicionada no assistente de Instalação de atualizações é exibida no Assistente para Novas Tarefas. Ao concluir o assistente, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será adicionada na lista de tarefas.

Criar a tarefa Encontrar vulnerabilidades e atualizações necessárias

Através da tarefa Encontrar as vulnerabilidades e as atualizações necessárias, o Kaspersky Security Center recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para o software de terceiro instalado nos dispositivos gerenciados.

A tarefa Encontrar as vulnerabilidades e as atualizações necessárias é criada automaticamente quando o Assistente de Início Rápido é executado. Caso não tenha executado o assistente, é possível criar a tarefa manualmente.

Para criar uma tarefa Encontrar as vulnerabilidades e as atualizações necessárias:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Encontrar as vulnerabilidades e as atualizações necessárias**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.
6. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.
7. Clique no botão **Criar**.

   A tarefa é criada e exibida na lista de tarefas.
8. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.
9. Na janela Propriedades da tarefa, especifique as configurações gerais da tarefa.

10. Na guia **Configurações do aplicativo**, especifique as seguintes configurações:

- **Buscar por vulnerabilidades e atualizações listadas pela Microsoft**

  Ao procurar por vulnerabilidades e atualizações, o Kaspersky Security Center usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft, que estão disponíveis no momento.

  Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

  As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

- **Conectar com o servidor de atualizações para atualizar dados**

O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

- Servidor de Administração do Kaspersky Security Center Cloud Console (consulte as Configurações da política do Agente de Rede)
- Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
- Servidores de atualizações da Microsoft

Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

Caso esta opção esteja desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows recebidas da fonte de atualizações da Microsoft antes.

A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

Por padrão, esta opção está ativada.

A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

- O Windows Update Agent em um dispositivo gerenciado se conecta com o servidor de atualização para obter atualizações somente se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada nas propriedades da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* e a opção **Modo de pesquisa do Windows Update** estiver definida como **Ativo** nas configurações da política do Agente de Rede.
- Caso não precise do Agente de Rede para iniciar uma conexão com a fonte de atualização do Microsoft Windows e as atualizações sejam baixadas durante a execução da tarefa de *Verificação de vulnerabilidades*, será possível definir a opção **Modo de pesquisa do Windows Update** como **Passivo**, enquanto a opção **Conectar com o servidor de atualizações para atualizar dados** deve permanecer ativada. Isso permite economizar recursos e usar atualizações do Windows recebidas anteriormente para verificar vulnerabilidades. É possível usar o modo passivo se o recebimento de atualizações do Microsoft Windows for configurado de uma forma diferente. Caso o recebimento de atualizações do Microsoft Windows não seja configurado de outra forma, não defina a opção **Modo de pesquisa do Windows Update** como **Passivo**, pois, nesse caso, as informações sobre as atualizações nunca serão recebidas.
- Independentemente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativado ou desativado), caso a opção **Modo de pesquisa do Windows Update** esteja definida como **Desativado**, o Kaspersky Security Center não solicitará nenhuma informação sobre as atualizações.

- Buscar por vulnerabilidades e atualizações de terceiros, listadas pela Kaspersky

Se esta opção estiver ativada, o Kaspersky Security Center pesquisará vulnerabilidades e atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

Se esta opção estiver desativada, o Kaspersky Security Center não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

Por padrão, esta opção está ativada.

- **Especifique caminhos para a pesquisa avançada de aplicativos no sistema de arquivos**

  As pastas nas quais o Kaspersky Security Center pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

  Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista contém pastas do sistema nas quais a maioria dos aplicativos está instalada.

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento mesmo que a gravação de arquivos de rastreamento esteja desativada para o Agente de Rede no Utilitário de Diagnóstico Remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

11. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Se os resultados da tarefa contiverem um aviso do erro 0x80240033 "Erro de atualização do Windows Update Agent 80240033 ("Não foi possível baixar os termos da licença.")", você poderá resolver esse problema no Registro do Windows.

As configurações da tarefa Encontrar vulnerabilidade e atualizações necessárias

A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente quando o Assistente de Início Rápido é executado. Caso não tenha executado o assistente, é possível criar a tarefa manualmente.

Além das configurações gerais da tarefa, é possível especificar as seguintes configurações ao criar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou mais recentes, ao configurar as propriedades da tarefa criada:

- **Buscar por vulnerabilidades e atualizações listadas pela Microsoft**

  Ao procurar por vulnerabilidades e atualizações, o Kaspersky Security Center usa as informações sobre atualizações aplicáveis da Microsoft a partir da fonte de atualizações da Microsoft, que estão disponíveis no momento.

  Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

  As informações sobre as atualizações adequadas ao Microsoft Windows não estão sendo enviados ao Servidor de Administração.

- **Conectar com o servidor de atualizações para atualizar dados**

O Windows Update Agent em um dispositivo gerenciado se conecta à fonte das atualizações da Microsoft. Os seguintes servidores podem atuar como uma fonte de atualizações da Microsoft:

- Servidor de Administração do Kaspersky Security Center Cloud Console (consulte as Configurações da política do Agente de Rede)
- Windows Server com o WSUS (Microsoft Windows Server Update Services) implementado na rede da sua organização
- Servidores de atualizações da Microsoft

Se esta opção estiver ativada, o Windows Update Agent em um dispositivo gerenciado se conecta à fonte de atualizações da Microsoft para atualizar as informações sobre as atualizações do Microsoft Windows aplicáveis.

Caso esta opção esteja desativada, o Windows Update Agent em um dispositivo gerenciado usa as informações sobre as atualizações aplicáveis do Microsoft Windows recebidas da fonte de atualizações da Microsoft antes.

A conexão à fonte de atualizações da Microsoft pode consumir muitos recursos. Você pode desativar esta opção se definir a conexão regular com esta fonte de atualizações em outra tarefa ou nas propriedades da política do Agente de Rede, na seção **Atualizações e vulnerabilidades de software**. Se não deseja desativar essa opção, para reduzir a sobrecarga no servidor, você pode configurar o agendamento da tarefa para atrasar aleatoriamente o início da tarefa em 360 minutos.

Por padrão, esta opção está ativada.

A combinação das seguintes opções das configurações da política do Agente de Rede define o modo de obter atualizações:

- O Windows Update Agent em um dispositivo gerenciado se conecta com o servidor de atualização para obter atualizações somente se a opção **Conectar com o servidor de atualizações para atualizar dados** estiver ativada nas propriedades da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* e a opção **Modo de pesquisa do Windows Update** estiver definida como **Ativo** nas configurações da política do Agente de Rede.
- Caso não precise do Agente de Rede para iniciar uma conexão com a fonte de atualização do Microsoft Windows e as atualizações sejam baixadas durante a execução da tarefa de *Verificação de vulnerabilidades*, será possível definir a opção **Modo de pesquisa do Windows Update** como **Passivo**, enquanto a opção **Conectar com o servidor de atualizações para atualizar dados** deve permanecer ativada. Isso permite economizar recursos e usar atualizações do Windows recebidas anteriormente para verificar vulnerabilidades. É possível usar o modo passivo se o recebimento de atualizações do Microsoft Windows for configurado de uma forma diferente. Caso o recebimento de atualizações do Microsoft Windows não seja configurado de outra forma, não defina a opção **Modo de pesquisa do Windows Update** como **Passivo**, pois, nesse caso, as informações sobre as atualizações nunca serão recebidas.
- Independentemente do status da opção **Conectar com o servidor de atualizações para atualizar dados** (ativado ou desativado), caso a opção **Modo de pesquisa do Windows Update** esteja definida como **Desativado**, o Kaspersky Security Center não solicitará nenhuma informação sobre as atualizações.

- **Buscar por vulnerabilidades e atualizações de terceiros, listadas pela Kaspersky**

  Se esta opção estiver ativada, o Kaspersky Security Center pesquisará vulnerabilidades e atualizações necessárias em aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft) no Registro do Windows e nas pastas especificadas em **Especifique caminhos para pesquisa avançada de aplicativos no sistema de arquivos**. A lista completa de suporte a aplicativos de terceiros é gerenciada pela Kaspersky.

  Se esta opção estiver desativada, o Kaspersky Security Center não procurará vulnerabilidades e atualizações necessárias de aplicativos de terceiros. Por exemplo, convém desativar esta opção se você tiver tarefas diferentes com configurações diferentes para atualizações do Microsoft Windows e atualizações de aplicativos de terceiros.

  Por padrão, esta opção está ativada.

- **Especifique caminhos para a pesquisa avançada de aplicativos no sistema de arquivos**

  As pastas nas quais o Kaspersky Security Center pesquisa aplicativos de terceiros que necessitem de correção de vulnerabilidades e de instalação de atualizações. Você pode usar variáveis de sistema.

  Especifique as pastas nas quais os aplicativos são instalados. Por padrão, a lista contém pastas do sistema nas quais a maioria dos aplicativos está instalada.

- **Ativar diagnóstico avançado**

  Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento mesmo que a gravação de arquivos de rastreamento esteja desativada para o Agente de Rede no Utilitário de Diagnóstico Remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

  Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

  Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

  Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

Recomendações sobre o agendamento de tarefas

Ao agendar a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*, certifique-se de que as duas opções **Executar tarefas ignoradas** e **Usar retardo aleatório automaticamente para início da tarefa** estejam desativadas.

Por padrão, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é configurada para iniciar manualmente. Caso as regras do local de trabalho da organização oferecerem o desligamento de todos os dispositivos nessa hora, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* será executada após os dispositivos serem ligados novamente, ou seja, na manhã do dia seguinte. Tal atividade pode ser indesejável porque uma verificação de vulnerabilidades pode aumentar a carga de subsistemas de disco e da CPU. Você deve definir o agendamento mais conveniente para a tarefa com base nas regras do local de trabalho adotadas na organização.

Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa lhe permite instalar várias atualizações e corrigir várias vulnerabilidades de acordo com certas regras.

Para instalar atualizações ou corrigir vulnerabilidades usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, execute uma das seguintes ações:

- Execute o assistente de Instalação das atualizações ou o assistente para Correção de vulnerabilidades.
- Crie uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.
- Adicione uma regra para instalação da atualização a uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.

Para criar uma tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades**.

   Se a tarefa não for exibida, verifique se sua conta tem direitos para **Ler**, **Modificar** e **Executar** na área funcional **Administração de sistema**: **Gerenciamento de Patches e Vulnerabilidades**. Você não pode criar e configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* sem esses direitos de acesso.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.

6. Especifique as regras para instalação da atualização e, então, especifique as seguintes configurações:

- **Iniciar a instalação ao reiniciar ou fechar o dispositivo**

  Se esta opção estiver ativada, as atualizações serão instaladas quando o dispositivo for reiniciado ou desligado. Caso contrário, as atualizações são instaladas segundo o agendamento.

  Use esta opção caso a instalação das atualizações afete o desempenho do dispositivo.

  Por padrão, esta opção está desativada.

- **Instalar os componentes gerais do sistema necessários**

  Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional.

  Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

  Por padrão, esta opção está desativada.

- **Permitir a instalação de novas versões dos aplicativos durante atualizações**

  Se esta opção estiver ativada, as atualizações serão permitidas quando resultarem na instalação de uma nova versão de um aplicativo de software.

  Se esta opção estiver desativada, o software não será atualizado. Você poderá então instalar novas versões do software manualmente ou através de outra tarefa. Por exemplo, você pode usar esta opção se a infraestrutura da sua empresa não tiver como base uma nova versão do software ou se você quiser verificar uma atualização usando uma infraestrutura de teste.

  Por padrão, esta opção está ativada.

  A atualização de um aplicativo pode causar o funcionamento incorreto de aplicativos dependentes instalados em dispositivos cliente.

- **Baixar atualizações para o dispositivo sem instalá-las**

  Se esta opção estiver ativada, o aplicativo baixa as atualizações em um dispositivo cliente, mas não as instala automaticamente. Você então poderá instalar manualmente as atualizações baixadas.

  As atualizações da Microsoft são baixadas no armazenamento de sistema do Windows. Atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky e à Microsoft) são baixados na pasta especificada no campo **Pasta para download de atualizações**.

  Se esta opção estiver desativada, as atualizações serão instaladas no dispositivo automaticamente.

  Por padrão, esta opção está desativada.

- **Pasta para download de atualizações**

  Esta pasta é usada para baixar atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft).

- **Ativar diagnóstico avançado**

Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento mesmo que a gravação de arquivos de rastreamento esteja desativada para o Agente de Rede no Utilitário de Diagnóstico Remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

7. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Tempo de espera antes do fechamento forçado de aplicativos nas sessões bloqueadas (min)**

Os aplicativos são fechados no modo forçado quando o dispositivo for bloqueado (automaticamente, após um intervalo especificado de inatividade ou manualmente).

Se esta opção estiver ativada, os aplicativos serão forçados a fechar no dispositivo bloqueado após a expiração do intervalo de tempo especificado no campo de entrada.

Se essa opção estiver ativada, os aplicativos não serão fechados no dispositivo bloqueado.

Por padrão, esta opção está desativada.

8. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.

10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

11. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

12. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

Se os resultados da tarefa contiverem um aviso do erro 0x80240033 "Erro de atualização do Windows Update Agent 80240033 ("Não foi possível baixar os termos da licença.")", você poderá resolver esse problema no Registro do Windows.

Adicionar regras para instalação da atualização

Esse recurso está disponível apenas sob a licença do Gerenciamento de patches e vulnerabilidades.

Ao instalar atualizações de software ou corrigir vulnerabilidades de software usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é necessário especificar regras para a instalação da atualização. Essas regras determinam as atualizações a serem instaladas e as vulnerabilidades a serem corrigidas.

As configurações exatas dependem de você ter adicionado uma regra para todas as atualizações, para atualizações do Windows Update ou para atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software que não sejam a Kaspersky ou a Microsoft). Ao adicionar uma regra para atualizações do Windows Update ou atualizações de aplicativos de terceiros, é possível selecionar aplicativos e versões de aplicativo específicos para os quais deseja instalar atualizações. Ao adicionar uma regra para todas as atualizações, é possível selecionar atualizações específicas que deseja instalar e vulnerabilidades que deseja corrigir com a instalação das atualizações.

É possível adicionar uma regra para a instalação da atualização das seguintes maneiras:

- Adicionando uma regra ao criar uma nova tarefa do tipo Instalar as atualizações necessárias e corrigir vulnerabilidades.
- Adicionando uma regra na guia **Configurações do aplicativo** na janela de propriedades de uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.
- Por meio do assistente de Instalação das atualizações ou do assistente para Correção de vulnerabilidades.

Para adicionar uma nova regra para todas as atualizações:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para todas as atualizações**.

3. Na página **Critérios gerais**, use as listas suspensas para especificar as seguintes configurações:

   - **Conjunto de atualizações a instalar**

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - **Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que**

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Atualizações**, selecione as atualizações a serem instaladas:

- **Instalar todas as atualizações adequadas**

  Instale todas as atualizações de software que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Instalar apenas as atualizações da lista**

  Instale somente as atualizações de software que você seleciona manualmente da lista. Essa lista contém todas as atualizações de software disponíveis.

  Por exemplo, pode ser necessário selecionar atualizações específicas nos seguintes casos: para verificar a instalação em um ambiente de teste, para atualizar somente aplicativos críticos ou para atualizar somente aplicativos específicos.

  - **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

    Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

    Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

    Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

    Por padrão, esta opção está ativada.

5. Na página **Vulnerabilidades**, selecione as vulnerabilidades que serão corrigidas instalando as atualizações selecionadas:

- **Corrigir todas as vulnerabilidades que correspondem a outros critérios**

  Corrija todas as vulnerabilidades que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Corrigir somente vulnerabilidades da lista**

  Corrija somente as vulnerabilidades que você seleciona manualmente da lista. Essa lista contém todas as vulnerabilidades detectadas.

  Por exemplo, pode ser necessário selecionar vulnerabilidades específicas nos seguintes casos: para verificar a correção em um ambiente de teste, para corrigir vulnerabilidades somente em aplicativos críticos ou para corrigir vulnerabilidades somente em aplicativos específicos.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para atualizações do Windows Update:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para o Windows Update**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

   - Corrigir vulnerabilidades com um nível de gravidade do MSRC igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Categorias de atualizações**, selecione as categorias das atualizações a serem instaladas. Essas categorias são iguais às no Catálogo do Microsoft Update. Por padrão, todas as categorias estão selecionadas.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para as atualizações de aplicativos de terceiros:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para atualizações de terceiros**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção Configurações da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Criar a tarefa Instalar atualizações do Windows Update

A tarefa *Instalar as atualizações do Windows Update* permite instalar as atualizações de software fornecidas pelo serviço Windows Update em dispositivos gerenciados.

Se você não possui uma licença do Gerenciamento de patches e vulnerabilidades, não pode criar novas tarefas do tipo *Instalar as atualizações do Windows Update*. Para instalar novas atualizações, adicione-as a uma tarefa *Instalar as atualizações do Windows Update* existente. Recomendamos usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* em vez da tarefa *Instalar as atualizações do Windows Update*. A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* permite instalar várias atualizações e corrigir várias vulnerabilidades automaticamente, de acordo com as regras definidas por você. Além disso, essa tarefa permite instalar atualizações de fornecedores de software que não sejam a Microsoft.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Para criar a tarefa Instalar atualizações do Windows Update:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Instalar as atualizações do Windows Update**.
4. Especifique o nome da tarefa que está criando.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.
6. Clique no botão **Adicionar**.

   A lista de atualizações é aberta.
7. Selecione as atualizações do Windows Update que deseja instalar e, a seguir, clique em **OK**.

8. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

9. Especificar as configurações da conta:

- **Conta padrão**

  A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

  Por padrão, esta opção está selecionada.

- **Especificar conta**

  Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

- **Conta**

  Conta sob a qual a tarefa é executada.

- **Senha**

  Senha da conta sob a qual a tarefa será executada.

10. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    A tarefa é criada e exibida na lista de tarefas.

12. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

13. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

14. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Exibir informações sobre atualizações disponíveis para software de terceiros

Você pode visualizar a lista de atualizações disponíveis para software de terceiros, incluindo software da Microsoft, instalado em dispositivos cliente.

Para exibir uma lista de atualizações disponíveis para aplicativos de terceiros instalados em dispositivos cliente,

No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

Aparece uma lista das atualizações disponíveis.

Você pode especificar um filtro para visualizar a lista de atualizações de software. Clique no ícone **Filtro** () no canto superior direito da lista de atualizações de software para gerenciar o filtro. Você também pode selecionar um dos filtros predefinidos na lista suspensa **Filtros predefinidos** acima da lista de vulnerabilidades de software.

Para visualizar as propriedades de uma atualização:

1. Clique no nome da atualização de software necessária.
2. A janela de propriedades da atualização é aberta, exibindo informações agrupadas nas seguintes guias:

- **Geral**

  Esta guia exibe detalhes gerais da atualização selecionada:

  - Status de aprovação da atualização (pode ser alterado manualmente, selecionando um novo status na lista suspensa)
  - Categoria do Windows Server Update Services (WSUS) à qual a atualização pertence
  - Data e hora em que a atualização foi registrada
  - Data e hora em que a atualização foi criada
  - Nível de importância da atualização
  - Requisitos de instalação impostos pela atualização
  - Família de aplicativos à qual a atualização pertence
  - Aplicativo ao qual a atualização se aplica
  - Número da revisão de atualização

- **Atributos**

Esta guia exibe um conjunto de atributos que você pode usar para obter mais informações sobre a atualização selecionada. Este conjunto difere, dependendo se a atualização é publicada pela Microsoft ou por um fornecedor terceiro.

A guia exibe as seguintes informações para uma atualização da Microsoft:

- O nível de importância da atualização, conforme definido pelo Microsoft Security Response Center (MSRC)
- Link para o artigo na Base de Dados de Conhecimento Microsoft que descreve a atualização
- Link para o artigo no Boletim de Segurança da Microsoft que descreve a atualização
- Identificador da atualização (ID)

A guia exibe as seguintes informações para uma atualização de terceiros:

- Se a atualização é um patch ou um pacote de distribuição completo
- Idioma de localização da atualização
- Se a atualização é instalada automática ou manualmente
- Se a atualização foi revogada após ser aplicada
- Link para baixar a atualização

- **Dispositivos**

  Esta guia exibe uma lista de dispositivos nos quais a atualização selecionada foi instalada.

- **Vulnerabilidades corrigidas**

  Esta guia exibe uma lista de vulnerabilidades que a atualização selecionada pode corrigir.

- **Cruzamento de atualizações**

  Esta guia exibe possíveis redundâncias entre várias atualizações publicadas para o mesmo aplicativo, ou seja, se a atualização selecionada pode substituir outras atualizações ou, vice-versa (disponíveis apenas para atualizações Windows).

- **Tarefas para instalar esta atualização**

  Esta guia exibe uma lista de tarefas cujo escopo inclui a instalação da atualização selecionada. A guia também permite que você crie uma nova tarefa de instalação remota para a atualização.

Para exibir as estatísticas de uma instalação de atualização:

1. Selecione a caixa de seleção ao lado da atualização de software necessária.
2. Clique no botão **Estatísticas de status da instalação de atualizações**.

O diagrama dos status de instalação da atualização é exibido. Clicar em um status abre uma lista de dispositivos nos quais a atualização tem o status selecionado.

Você pode visualizar informações sobre atualizações de software disponíveis para software de terceiros, incluindo software da Microsoft, instalado no dispositivo gerenciado selecionado que executa o Windows.

Para visualizar uma lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo para o qual você deseja visualizar atualizações de software de terceiros.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Na janela de propriedades do dispositivo selecionado selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Atualizações disponíveis**. Caso deseje visualizar apenas as atualizações instaladas, ative a opção **Exibir atualizações instaladas**.

A lista de atualizações de software de terceiros disponíveis para o dispositivo selecionado é exibida.

Exportando a lista de vulnerabilidades de software para um arquivo

Você pode exportar a lista de atualizações para software de terceiros, incluindo o software Microsoft, exibido no momento para os arquivos CSV e TXT. Você pode usar esses arquivos, por exemplo, para enviá-los ao seu gerente de segurança de informações ou para armazená-los para fins de estatística.

Para exportar como arquivo de texto a lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Atualizações de software**.

   A página exibe uma lista de atualizações disponíveis para software de terceiros instalado em todos os dispositivos gerenciados.

2. Clique no botão **Exportar linhas para arquivo TXT** ou **Exportar linhas para arquivo CSV**, dependendo do formato de exportação preferido.

O arquivo contendo a lista de atualizações para software de terceiros, incluindo software da Microsoft, é baixado para o dispositivo usado no momento.

Para exportar como arquivo de texto uma lista de atualizações disponíveis para software de terceiros instalado no dispositivo gerenciado selecionado:

1. Abra a lista de atualizações de software de terceiros disponíveis no dispositivo gerenciado selecionado.
2. Selecione as atualizações de software que você deseja exportar.

   Ignore esta etapa se desejar exportar uma lista completa de atualizações de software.

   Se você deseja exportar a lista completa de atualizações de software, apenas as vulnerabilidades exibidas na página atual serão exportadas.

   Se deseja exportar apenas as atualizações instaladas, marque a caixa **Exibir atualizações instaladas**.
3. Clique no botão **Exportar linhas para arquivo TXT** ou **Exportar linhas para arquivo CSV**, dependendo do formato de exportação preferido.

O arquivo contendo a lista de atualizações para software de terceiros, incluindo software da Microsoft, instalados no dispositivo gerenciado é baixado para o dispositivo usado no momento.

Aprovando e recusando atualizações de software de terceiros

Ao configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é possível criar uma regra que exija um status específico das atualizações a serem instaladas. Por exemplo, uma regra de atualização pode permitir a instalação do seguinte:

- Somente atualizações aprovadas
- Somente atualizações aprovadas e indefinidas
- Todas as atualizações, independentemente dos status de atualização

Você pode aprovar atualizações que devem ser instaladas e recusar as atualizações que não devem ser instaladas.

O uso do status *Aprovado* para gerenciar a instalação da atualização é eficiente para uma pequena quantidade de atualizações. Para instalar várias atualizações, use as regras que você pode configurar na tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Recomendamos que você defina o status *Aprovado* apenas para as atualizações específicas que não atendem aos critérios especificados nas regras. Ao aprovar manualmente uma grande quantidade de atualizações, o desempenho do Servidor de Administração é reduzido, o que pode levar à sua sobrecarga.

Para aprovar ou recusar uma ou várias atualizações:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.
2. Selecione as atualizações que deseja aprovar ou recusar.
3. Clique em **Aprovar** para aprovar as atualizações selecionadas ou **Recusar** para recusar as atualizações selecionadas.

   O valor padrão é *Indefinido*.

As atualizações selecionadas têm os status que você definiu.

Como opção, você pode alterar o status de aprovação nas propriedades de uma atualização específica.

Para aprovar ou recusar uma atualização em suas propriedades:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Atualizações de software**.

   Aparece uma lista das atualizações disponíveis.

2. Clique no nome da atualização que deseja aprovar ou recusar.

   A janela Propriedades da atualização é aberta.

3. Na seção **Geral**, selecione um status para a atualização, alterando a opção **Status de aprovação da atualização**. Você pode selecionar o status *Aprovado*, *Negado*, ou *Indefinido*.

4. Clique no botão **Salvar** para salvar as alterações.

A atualização selecionada tem o status que você definiu.

Se você definir o status **Negado** para atualizações de software de terceiros, estas atualizações não serão instaladas em dispositivos para os quais elas foram planejadas, mas que ainda não foram instaladas. As atualizações permanecerão nos dispositivos nos quais elas já foram instaladas. Se você tiver de exclui-las, poderá exclui-las manualmente localmente.

Criação da tarefa Executar a sincronização com o Windows Update

A tarefa *Executar a sincronização com o Windows Update* só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

A tarefa *Executar a sincronização com o Windows Update* é necessária caso deseje usar o Servidor de Administração como um servidor WSUS. Nesse caso, o Servidor de Administração baixa as atualizações do Windows para o banco de dados e fornece as atualizações para o Windows Update em dispositivos clientes no modo centralizado por meio de Agentes de Rede. Se a rede não usar um servidor WSUS, cada dispositivo cliente baixa as atualizações da Microsoft de servidores externos independentemente.

A tarefa *Executar a sincronização com o Windows Update* somente baixa metadados de servidores da Microsoft. O Kaspersky Security Center baixa as atualizações quando você executa uma tarefa de instalação de atualização e somente as atualizações selecionadas para instalação.

Ao executar a tarefa **Executar a sincronização com o Windows Update**, o aplicativo recebe uma lista das atualizações atuais de um servidor de atualização da Microsoft. A seguir, o Kaspersky Security Center compila uma lista das atualizações que se tornaram desatualizadas. Na próxima inicialização da tarefa **Encontrar as vulnerabilidades e as atualizações necessárias**, o Kaspersky Security Center sinaliza todas as atualizações desatualizadas e define a hora de exclusão para as mesmas. Na próxima inicialização da tarefa **Executar a sincronização com o Windows Update**, todas as atualizações sinalizadas para exclusão 30 dias atrás serão excluídas. O Kaspersky Security Center também verifica quanto a atualizações desatualizadas foram sinalizadas para a exclusão há mais de 180 dias, e então exclui estas atualizações mais antigas.

Quando a tarefa **Executar a sincronização com o Windows Update** for concluída e as atualizações desatualizadas são excluídas, o banco de dados ainda pode ter os códigos hash que pertencem aos arquivos de atualizações excluídas, assim como os arquivos correspondentes nos arquivos %AllUsersProfile%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles (se eles foram baixados anteriormente). É possível executar a tarefa de **Manutenção do Servidor de Administração** para excluir esses registros desatualizados do banco de dados e dos arquivos correspondentes.

Para criar uma tarefa Executar a sincronização com o Windows Update:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Executar a sincronização com o Windows Update**.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Ative a opção **Baixar arquivos de instalação rápida** se desejar que os arquivos de atualização expressa sejam baixados ao executar a tarefa.

   Quando o Kaspersky Security Center sincroniza as atualizações com Microsoft Windows Update Servers, as informações sobre todos os arquivos são salvas no banco de dados do Servidor de Administração. Todos os arquivos necessários para uma atualização também são baixados para a unidade durante a interação com o Windows Update Agent. Em particular, o Kaspersky Security Center salva as informações sobre arquivos de atualização expressa no banco de dados e as baixa quando necessário. Baixar os arquivos de atualização expressa conduz a diminuição do espaço livre na unidade.

   Para evitar uma redução no volume de espaço em disco e reduzir o tráfego, desative a opção **Baixar arquivos de instalação rápida**.
6. Selecione os aplicativos para os quais deseja baixar atualizações.

   Se a caixa de seleção **Todos os aplicativos** estiver marcada, as atualizações serão baixadas para todos os aplicativos existentes, e para todos os aplicativos que possam ser lançados no futuro.
7. Selecione as categorias de atualizações que deseja baixar para o Servidor de Administração.

   Se a caixa de seleção **Todas as categorias** estiver marcada, as atualizações serão baixadas para todas as categorias existentes, e para todas as categorias que podem aparecer no futuro.
8. Selecione os idiomas de localização das atualizações que deseja baixar para o Servidor de Administração. Selecione uma das seguintes opções:

   - Baixar todos os idiomas, incluindo os novos

     Se esta opção estiver selecionada, todos os idiomas de localização disponíveis das atualizações serão baixados para o Servidor de Administração. Por padrão, esta opção está selecionada.

   - Baixar idiomas selecionados

     Se esta opção estiver selecionada, você pode selecionar na lista os idiomas de localização das atualizações que serão baixados para o Servidor de Administração.

9. Especifique qual conta usar ao executar a tarefa. Selecione uma das seguintes opções:

   - **Conta padrão**

     A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

     Por padrão, esta opção está selecionada.

   - **Especificar conta**

     Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

10. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    A tarefa é criada e exibida na lista de tarefas.

12. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

13. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

14. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Atualizar aplicativos de terceiros automaticamente

Alguns aplicativos de terceiros podem ser atualizados automaticamente. O fornecedor do aplicativo define se o aplicativo é compatível ou não com o recurso de atualização automática. Se um aplicativo de terceiros instalado em um dispositivo gerenciado for compatível com atualização automática, você poderá especificar a configuração de atualização automática nas propriedades do aplicativo. Depois de alterar a configuração de atualização automática, os Agentes de Rede aplicam a nova configuração a cada dispositivo gerenciado no qual o aplicativo está instalado.

A configuração de atualização automática é independente dos outros objetos e configurações do recurso Gerenciamento de patches e vulnerabilidades. Por exemplo, esta configuração não depende de um status de aprovação de atualização ou das tarefas de instalação da atualização, como *Instalar as atualizações necessárias e corrigir vulnerabilidades*, *Instalar as atualizações do Windows Update* e *Corrigir vulnerabilidades*.

Para definir a configuração de atualização automática para um aplicativo de terceiros:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos**.

2. Clique no nome do aplicativo para o qual deseja alterar a configuração de atualização automática.

   Para simplificar a pesquisa, você pode filtrar a lista pela coluna **Status das atualizações automáticas**.

   A janela Propriedades do aplicativo é aberta.

3. Na seção **Geral**, selecione um valor para a seguinte configuração:

   Status das atualizações automáticas

   Selecione uma das seguintes opções:

   - **Indefinido**

     O recurso de atualização automática será desativado. O Kaspersky Security Center instala atualizações de aplicativos de terceiros usando as tarefas: *Instalar as atualizações necessárias e corrigir vulnerabilidades*, *Instalar as atualizações do Windows Update*, e *Corrigir vulnerabilidades*.

   - **Permitido**

     Depois que o fornecedor lança uma atualização para o aplicativo, esta atualização é instalada nos dispositivos gerenciados automaticamente. Nenhuma outra ação é necessária.

   - **Bloqueado**

     As atualizações do aplicativo não são instaladas automaticamente. O Kaspersky Security Center instala atualizações de aplicativos de terceiros usando as tarefas: *Instalar as atualizações necessárias e corrigir vulnerabilidades*, *Instalar as atualizações do Windows Update*, e *Corrigir vulnerabilidades*.

4. Clique no botão **Salvar** para salvar as alterações.

A configuração de atualização automática é aplicada ao aplicativo selecionado.

Cenário: Atualizando software de terceiros

Esta seção fornece um cenário para a atualização software de terceiros instalados nos dispositivos cliente. Software de terceiros incluem aplicativos da Microsoft e de outros fornecedores de software. As atualizações para aplicativos Microsoft são fornecidas pelo serviço Windows Update.

Pré-requisitos

O Servidor de Administração deve ter uma conexão com a Internet para instalar atualizações de software de terceiros que não sejam software Microsoft.

Por padrão, a conexão com a Internet não é necessária para que o Servidor de Administração instale atualizações de software da Microsoft nos dispositivos gerenciados. Por exemplo, os dispositivos gerenciados podem baixar as atualizações de software da Microsoft diretamente dos servidores de Atualizações da Microsoft ou do Windows Server com o Microsoft Windows Server Update Services (WSUS) implementado na rede da sua organização. O Servidor de Administração deve estar conectado à Internet quando você usa o Servidor de Administração como servidor WSUS.

Fases

A atualização de software de terceiros prossegue em fases:

1. **Procurar atualizações necessárias**

Para encontrar as atualizações de softwares de terceiros necessárias para os dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Kaspersky Security Center recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo Assistente de Início Rápido do Servidor de Administração. Caso não tenha executado o assistente, crie a tarefa ou execute o Assistente de Início Rápido rápido agora.

Instruções de como proceder:

- Console de administração: Verificando aplicativos em busca de vulnerabilidades, Agendando a tarefa Encontrar as vulnerabilidades e as atualizações necessárias
- Kaspersky Security Center Web Console: Criar a tarefa Encontrar as vulnerabilidades e as atualizações necessárias, Configurações da tarefa Encontrar as vulnerabilidades e as atualizações necessárias

2. **Analisar a lista de atualizações encontradas**

Exiba a lista **Atualizações de software** e decida quais atualizações devem ser instaladas. Para visualizar informações detalhadas sobre cada atualização, clique no nome da atualização na lista. Para cada atualização na lista, você também pode visualizar as estatísticas sobre a instalação da atualização nos dispositivos cliente.

Instruções de como proceder:

- Console de administração: Visualizando informações sobre atualizações disponíveis
- Kaspersky Security Center Web Console: Visualizando informações sobre atualizações de software de terceiros disponíveis

3. **Configurar instalação de atualizações**

Quando o Kaspersky Security Center receber a lista de atualizações de software de terceiros, será possível instalá-las em dispositivos clientes usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. Crie uma dessas tarefas. Você pode criar essas tarefas na guia **Tarefas** ou usando a lista **Atualizações de software**.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para instalar atualizações para aplicativos da Microsoft, incluindo as atualizações fornecidas pelo serviço Windows Update e atualizações de software de outros fornecedores. Observe que esta tarefa pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades.

A tarefa *Instalar as atualizações do Windows Update* não requer uma licença, mas pode ser usada para instalar apenas atualizações do Windows Update.

Para instalar algumas atualizações de software, você deve aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software. Se você recusar o EULA, a atualização do software não será instalada.

Você pode iniciar uma tarefa de instalação de atualizações. Ao especificar o agendamento de tarefas, certifique-se de que a tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

Instruções de como proceder:

- Console de administração: Corrigindo vulnerabilidades em aplicativos, exibindo informações sobre atualizações disponíveis
- Kaspersky Security Center Web Console: Criando a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades, Criando a tarefa Instalar as atualizações do Windows Update, Visualizando informações sobre atualizações de software de terceiros disponíveis

4. **Agendar as tarefas**

Para garantir que a lista de atualizações esteja sempre atualizada, agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para executá-la automaticamente de tempos em tempos. Por padrão, a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é configurada para iniciar manualmente.

Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência. Ao agendar a tarefa *Instalar as atualizações do Windows Update*, observe que, para essa tarefa, é necessário definir a lista de atualizações todas as vezes antes de iniciá-la.

Ao agendar as tarefas, certifique-se de que uma tarefa de instalação de atualização seja iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

5. **Aprovar e recusar atualizações de software (opcional)**

Se você tiver criado a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades, poderá especificar regras para instalação da atualização nas propriedades da tarefa. Se você criou a tarefa Instalar as atualizações do Windows Update, pule esta etapa.

Para cada regra, você pode definir as atualizações a serem instaladas, dependendo do status da atualização: *Indefinido*, *Aprovado* ou *Recusado*. Por exemplo, convém criar uma tarefa específica para servidores e definir uma regra para essa tarefa para permitir a instalação apenas de atualizações do Windows Update e somente aquelas com status *Aprovado*. Depois disso, você define manualmente o status *Aprovado* para as atualizações que deseja instalar. Nesse caso, as atualizações do Windows Update com status *Indefinido* ou *Recusado* não serão instaladas nos servidores especificados para a tarefa.

O uso do status *Aprovado* para gerenciar a instalação da atualização é eficiente para uma pequena quantidade de atualizações. Para instalar várias atualizações, use as regras que você pode configurar na tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades*. Recomendamos que você defina o status *Aprovado* apenas para as atualizações específicas que não atendem aos critérios especificados nas regras. Ao aprovar manualmente uma grande quantidade de atualizações, o desempenho do Servidor de Administração é reduzido, o que pode levar à sua sobrecarga.

Por padrão, as atualizações de software baixadas têm o status *Indefinido*. Você pode alterar o status para *Aprovado* ou *Recusado* na lista **Atualizações de software** (**Operações → Gerenciamento de patches → Atualizações de software**).

Instruções de como proceder:

- Console de Administração: Aprovação e recusa de atualizações de software
- Kaspersky Security Center Web Console: Aprovando e recusando atualizações de software de terceiros

6. **Configurando o Servidor de Administração para funcionar como servidor WSUS (Serviços de atualização do Windows Server) (opcional)**

Por padrão, as atualizações do Windows Update são baixadas para os dispositivos gerenciados diretamente dos servidores da Microsoft. Você pode alterar essa configuração para usar o Servidor de Administração como servidor WSUS. Nesse caso, o Servidor de Administração sincroniza os dados da atualização com o Windows Update na frequência especificada e fornece atualizações no modo centralizado para o Windows Update nos dispositivos em rede.

Para usar o Servidor de Administração como servidor WSUS, crie a tarefa Executar a sincronização com o Windows Update e marque a caixa de seleção **Usar Servidor de Administração como servidor WSUS** na política do Agente de Rede.

Instruções de como proceder:

- Console de Administração: Sincronizando atualizações do Windows Update com o Servidor de Administração, Configurando atualizações do Windows em uma política de Agente de Rede
- Kaspersky Security Center Web Console: Criação da tarefa Executar a sincronização com o Windows Update

7. **Execução de uma tarefa de instalação de atualização**

Inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações do Windows Update*. Quando você inicia essas tarefas, as atualizações são baixadas e instaladas nos dispositivos gerenciados. Após a conclusão da tarefa, verifique se ela possui o status *Concluída com êxito* na lista de tarefas.

8. **Criar o relatório sobre os resultados da instalação da atualização de software de terceiros (opcional)**

   Para ver estatísticas detalhadas sobre a instalação de atualização, gere um **Relatório de resultados da instalação de atualizações de software de terceiros**.

   Instruções de como proceder:

   - Console de Administração: Criando e visualizando um relatório
   - Kaspersky Security Center Web Console: Gerando e visualizando atualizações de software

Resultados

Se você tiver criado e configurado a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, as atualizações serão instaladas nos dispositivos gerenciados automaticamente. Quando novas atualizações são baixadas no repositório do Servidor de Administração, o Kaspersky Security Center verifica se elas atendem aos critérios especificados nas regras de atualização. Todas as novas atualizações que atendem aos critérios serão instaladas automaticamente na próxima tarefa executada.

Se você tiver criado a tarefa *Instalar atualizações do Windows Update*, apenas as atualizações especificadas nas propriedades da tarefa *Instalar atualizações do Windows Update* serão instaladas. No futuro, caso deseje instalar novas atualizações baixadas no repositório do Servidor de Administração, será preciso adicionar as atualizações necessárias à lista de atualizações da tarefa existente ou criar uma nova tarefa *Instalar atualizações do Windows Update*.

Corrigindo vulnerabilidades de software de terceiros

Esta seção descreve os recursos do Kaspersky Security Center relacionados à correção de vulnerabilidades no software instalado nos dispositivos gerenciados.

Cenário: Encontrar e corrigir vulnerabilidades de software de terceiros

Esta seção fornece um cenário para localizar e corrigir vulnerabilidades nos dispositivos gerenciados que executam o Windows. Você pode encontrar e corrigir vulnerabilidades de software no sistema operacional e em software de terceiros, incluindo software da Microsoft.

Pré-requisitos

- O Kaspersky Security Center está implementado em sua organização.
- Há dispositivos gerenciados executando o Windows na sua organização.
- A conexão com a Internet é necessária para que o Servidor de Administração execute as seguintes tarefas:
  - Para fazer uma lista de correções recomendadas para vulnerabilidades em softwares da Microsoft. A lista é criada e atualizada regularmente por especialistas da Kaspersky.
  - Para corrigir vulnerabilidades em software de terceiros que não sejam software da Microsoft.

Fases

A localização e a correção de vulnerabilidades de software ocorre em fases:

1. **Verificar vulnerabilidades no software instalado nos dispositivos gerenciados**

   Para encontrar vulnerabilidades no software instalado nos dispositivos gerenciados, execute a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*. Quando essa tarefa for concluída, o Kaspersky Security Center recebe as listas de vulnerabilidades detectadas e as atualizações necessárias para software de terceiros instalados nos dispositivos que você especificou nas propriedades da tarefa.

   A tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Caso não tenha executado o assistente, inicie-o agora ou crie a tarefa manualmente.

   Instruções de como proceder:

   - Console de administração: Verificando aplicativos em busca de vulnerabilidades, Agendando a tarefa Encontrar as vulnerabilidades e as atualizações necessárias
   - Kaspersky Security Center Web Console: Criar a tarefa Encontrar as vulnerabilidades e as atualizações necessárias, Configurações da tarefa Encontrar as vulnerabilidades e as atualizações necessárias

2. **Analisar a lista de vulnerabilidades de software detectadas**

   Visualize a lista **Vulnerabilidades de software** e decida quais vulnerabilidades devem ser corrigidas. Para visualizar informações detalhadas sobre cada vulnerabilidade, clique no nome da vulnerabilidade na lista. Para cada vulnerabilidade na lista, você também pode visualizar as estatísticas sobre a vulnerabilidade nos dispositivos gerenciados.

   Instruções de como proceder:

   - Console de Administração: Visualizar informações sobre vulnerabilidades do software, Visualizar estatísticas das vulnerabilidades em dispositivos gerenciados
   - Kaspersky Security Center Web Console: Visualização das informações sobre as vulnerabilidades de software, Visualização das estatísticas de vulnerabilidades em dispositivos gerenciados

3. **Configurar a correção de vulnerabilidades**

   Quando as vulnerabilidades de software são detectadas, é possível corrigi-las nos dispositivos gerenciados usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa lhe permite instalar várias atualizações e corrigir várias vulnerabilidades de acordo com certas regras. Observe que esta tarefa pode ser criada apenas se você tiver a licença para o recurso Gerenciamento de patches e vulnerabilidades. Para corrigir vulnerabilidades de software, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* usa as atualizações de software recomendadas.

A tarefa *Corrigir vulnerabilidades* não requer a opção de licença para o recurso Gerenciamento de patches e vulnerabilidades. Para usar esta tarefa, você deve especificar manualmente as correções para vulnerabilidades em softwares de terceiros definidas pelo usuário, listadas nas configurações da tarefa. A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para softwares de terceiros.

É possível iniciar o Assistente para Correção de Vulnerabilidades, que cria uma dessas tarefas automaticamente, ou criá-las manualmente.

Instruções de como proceder:

- Console de administração: Selecionar as correções de usuário para as vulnerabilidades de software de terceiros, Corrigir as vulnerabilidades em aplicativos
- Kaspersky Security Center Web Console: Selecionar as correções do usuário para vulnerabilidades em software de terceiros, Corrigir as vulnerabilidades de software de terceiros, Criar a tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades

4 Agendar as tarefas

Para garantir que a lista de vulnerabilidades esteja sempre atualizada, agende a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para executá-la automaticamente de tempo em tempo. A frequência média recomendada é de uma vez por semana.

Se você criou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, pode agendá-la para ser executada com a mesma frequência que a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* ou com menor frequência. Ao agendar a tarefa *Corrigir vulnerabilidades*, é necessário selecionar correções para o software da Microsoft ou especificar correções de usuário para o software de terceiros sempre que iniciar a tarefa.

Ao agendar as tarefas, certifique-se que uma tarefa para corrigir vulnerabilidades é iniciada após a conclusão da tarefa *Encontrar as vulnerabilidades e as atualizações necessárias*.

5 Ignorar vulnerabilidades de software (opcional)

Se você desejar, poderá ignorar as vulnerabilidades de software a ser corrigidas em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

Instruções de como proceder:

- Console de administração: Ignorar as vulnerabilidades do software
- Kaspersky Security Center Web Console: Ignorando vulnerabilidades de software

6 Executando uma tarefa de correção de vulnerabilidades

Inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*. Quando a tarefa estiver concluída, certifique-se que possui o status *Concluído com êxito* na lista de tarefas.

7 Criar o relatório sobre os resultados da correção de vulnerabilidades de software (opcional)

Para visualizar estatísticas detalhadas sobre a correção de vulnerabilidades, gere o Relatório de vulnerabilidades. O relatório exibe informações sobre vulnerabilidades de software que não são corrigidas. Assim, é possível ter uma ideia sobre como encontrar e corrigir vulnerabilidades em softwares de terceiros, incluindo softwares da Microsoft, em sua organização.

Instruções de como proceder:

- Console de Administração: Criando e visualizando um relatório
- Kaspersky Security Center Web Console: Gerando e visualizando atualizações de software

8. **Verificar a configuração para encontrar e corrigir vulnerabilidades em software de terceiros**

   Certifique-se de ter feito o seguinte:

   - Obtenção e revisão da lista de vulnerabilidades de software detectadas nos dispositivos gerenciados
   - Vulnerabilidades de software ignoradas, se desejado
   - A tarefa para corrigir vulnerabilidades está configurada
   - As tarefas para localizar e corrigir vulnerabilidades de software estão agendadas para que sejam iniciadas sequencialmente
   - Verificar se a tarefa para corrigir vulnerabilidades de software foi executada

Resultados

Se você criou e configurou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, as vulnerabilidades são corrigidas nos dispositivos gerenciados automaticamente. Quando a tarefa é executada, ela correlaciona a lista de atualizações de software disponíveis às regras especificadas nas configurações da tarefa. Todas as atualizações de software que atendem aos critérios das regras serão baixadas no repositório do Servidor de Administração e instaladas para corrigir as vulnerabilidades de software.

Se você criou a tarefa *Corrigir vulnerabilidades*, apenas as vulnerabilidades de software no software da Microsoft são corrigidas.

Sobre como encontrar e corrigir vulnerabilidades de software

O Kaspersky Security Center detecta e corrige vulnerabilidades de software em dispositivos gerenciados que executam os sistemas operacionais das famílias Microsoft Windows. As vulnerabilidades são detectadas no sistema operacional e no software de terceiros, incluindo o software da Microsoft.

> A funcionalidade de atualizações (incluindo o fornecimento de atualizações de assinatura de antivírus e atualizações da base de código), bem como a funcionalidade da KSN, podem não estar disponíveis no software nos EUA.

Localizar vulnerabilidades de software

Para encontrar vulnerabilidades de software, o Kaspersky Security Center usa características do banco de dados de vulnerabilidades conhecidas. Este banco de dados é criado por especialistas da Kaspersky. Ele contém informações sobre vulnerabilidades, como descrição da vulnerabilidade, data de detecção da vulnerabilidade, nível de gravidade da vulnerabilidade. Você pode encontrar os detalhes das vulnerabilidades de software no site da Kaspersky.

O Kaspersky Security Center usa a tarefa *Encontrar as vulnerabilidades e as atualizações necessárias* para encontrar vulnerabilidades de software.

Em certos casos, as vulnerabilidades detectadas em um sistema operacional Microsoft Windows podem ser corrigidas usando um dos seguintes métodos:

- Instalação de uma atualização para o SO.
- Atualização do SO para uma versão mais recente (por exemplo, do Windows 10 para o Windows 11).

Neste cenário, o Kaspersky Security Center exibe duas entradas para a mesma vulnerabilidade.

Corrigir vulnerabilidades de software

Para corrigir vulnerabilidades de software, o Kaspersky Security Center usa atualizações de software emitidas pelos fornecedores do software. Os metadados das atualizações de software são baixados no repositório do Servidor de Administração como um resultado da execução da tarefa a seguir:

- *Baixar atualizações no repositório do Servidor de Administração*. Esta tarefa tem como objetivo fazer o download de metadados de atualizações para o Kaspersky e software de terceiros. Essa tarefa é criada automaticamente pelo Assistente de início rápido do Kaspersky Security Center. Você pode criar a tarefa Baixar atualizações no repositório do Servidor de Administração manualmente.
- *Executar a sincronização com o Windows Update*. Esta tarefa tem como objetivo baixar metadados de atualizações para o software Microsoft.

As atualizações de software para corrigir vulnerabilidades podem ser representadas como pacotes ou patches de distribuição completos. As atualizações de software que corrigem vulnerabilidades de software são denominadas *correções*. As *correções recomendadas* são aquelas recomendadas para instalação pelos especialistas da Kaspersky. *Correções do usuário* são aquelas especificadas manualmente para instalação pelos usuários. Para instalar uma correção do usuário, você deve criar um pacote de instalação contendo essa correção.

Se você possui a licença do Kaspersky Security Center com o recurso Gerenciamento de patches e vulnerabilidades, para corrigir as vulnerabilidades de software, você pode usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Esta tarefa corrige automaticamente várias vulnerabilidades instalando as correções recomendadas. Para esta tarefa, você pode configurar manualmente certas regras para corrigir várias vulnerabilidades.

Se você não possui a licença do Kaspersky Security Center com o recurso Gerenciamento de patches e vulnerabilidades, para corrigir as vulnerabilidades de software, você pode usar a tarefa *Corrigir vulnerabilidades*. Por meio desta tarefa, você pode corrigir vulnerabilidades instalando as correções recomendadas para o software da Microsoft e as correções do usuário para outros softwares de terceiros.

Por motivos de segurança, todas as atualizações de softwares de terceiros instaladas usando o recurso Gerenciamento de patches e vulnerabilidades são verificadas automaticamente pelas tecnologias da Kaspersky em busca de malwares. Essas tecnologias são usadas para verificação automática de arquivos e incluem verificação de vírus, análise estática, análise dinâmica, análise de comportamento no ambiente sandbox e aprendizado de máquina.

Os especialistas da Kaspersky não realizam análises manuais de atualizações de softwares de terceiros que podem ser instaladas usando o recurso Gerenciamento de patches e vulnerabilidades. Além disso, os especialistas da Kaspersky não pesquisam vulnerabilidades (conhecidas ou desconhecidas) ou recursos não documentados nessas atualizações, nem realizam outros tipos de análise das atualizações além dos especificados no parágrafo acima.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Para corrigir algumas vulnerabilidades de software, é necessário aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software, se o aceite do EULA for solicitado. Se você recusar o EULA, a vulnerabilidade do software não será corrigida.

Corrigindo vulnerabilidades de software de terceiros

Depois de obter a lista de vulnerabilidades de software, você pode corrigir as vulnerabilidades de software nos dispositivos gerenciados que executam o Windows. É possível corrigir vulnerabilidades de software no sistema operacional e em softwares de terceiros, incluindo softwares da Microsoft, criando e executando a tarefa *Corrigir vulnerabilidades* ou a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Como opção, é possível criar uma tarefa para corrigir vulnerabilidades de software das seguintes maneiras:

- Abrindo a lista de vulnerabilidades e especificando quais vulnerabilidades corrigir.

  Como resultado, é criada uma nova tarefa para corrigir vulnerabilidades de software. Como opção, você pode adicionar as vulnerabilidades selecionadas a uma tarefa existente.

- Executando o assistente para Correção de vulnerabilidades.

  O Assistente para correção de vulnerabilidades só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

  O assistente simplifica a criação e a configuração de uma tarefa de correção de vulnerabilidades e permite eliminar a criação de tarefas redundantes que contenham as mesmas atualizações para instalação.

Corrigindo vulnerabilidades de software usando a lista de vulnerabilidades

Para corrigir vulnerabilidades de software:

1. Abra uma das listas de vulnerabilidades:

   - Para abrir a lista geral de vulnerabilidades, No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Vulnerabilidades de software**.
   - Para abrir a lista de vulnerabilidades de um dispositivo gerenciado, No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados** → <nome do dispositivo> → **Avançado** → **Vulnerabilidades de software**.
   - Para abrir a lista de vulnerabilidades de um aplicativo específico, No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos** → <nome do aplicativo> → **Vulnerabilidades**.

   Uma página com uma lista de vulnerabilidades em softwares de terceiros é exibida.

2. Selecione uma ou mais vulnerabilidades na lista e clique no botão **Corrigir vulnerabilidade**.

   Se a atualização de software recomendada para corrigir uma das vulnerabilidades selecionadas estiver ausente, uma mensagem informativa será exibida.

   Para corrigir algumas vulnerabilidades de software, é necessário aceitar o Contrato de Licença do Usuário Final (EULA) para a instalação do software, se o aceite do EULA for solicitado. Se você recusar o EULA, a vulnerabilidade do software não será corrigida.

3. Selecione uma das seguintes opções:

   - **Nova tarefa**

     O Assistente para novas tarefa inicia. Se você tiver a licença do Gerenciamento de patches e vulnerabilidades, a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* será pré-selecionada. Se você não tiver a licença, a tarefa *Corrigir vulnerabilidades* será pré-selecionada. Seguem abaixo as etapas do assistente para concluir a criação da tarefa.

   - **Corrigir vulnerabilidade (adicionar a regra à tarefa especificada)**

     Selecione uma tarefa à qual deseja adicionar as vulnerabilidades selecionadas. Se você tiver a licença de Gerenciamento de patches e vulnerabilidades, selecione a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*. Uma nova regra para corrigir as vulnerabilidades selecionadas será adicionada automaticamente à tarefa escolhida. Se você não tiver a licença, selecione a tarefa *Corrigir vulnerabilidades*. As vulnerabilidades selecionadas serão adicionadas às propriedades da tarefa.

     A janela de propriedades da tarefa é aberta. Clique no botão **Salvar** para salvar as alterações.

   Se você escolheu criar uma nova tarefa, a tarefa será criada e exibida na lista de tarefas em **Dispositivos** → **Tarefas**. Se você optou por adicionar as vulnerabilidades a uma tarefa existente, as vulnerabilidades serão salvas nas propriedades da tarefa.

Para corrigir as vulnerabilidades de software de terceiros, inicie a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* ou a tarefa *Corrigir vulnerabilidades*. Se você criou a tarefa *Corrigir vulnerabilidades*, deve especificar manualmente as atualizações de software para corrigir as vulnerabilidades de software listadas nas configurações da tarefa.

Corrigir vulnerabilidades de software usando o assistente para Correção de vulnerabilidades

O Assistente para correção de vulnerabilidades só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

Para corrigir vulnerabilidades de software usando o assistente para Correção de vulnerabilidades:

1. No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Vulnerabilidades de software**.

   Uma página com uma lista de vulnerabilidades em softwares de terceiros instalados em dispositivos gerenciados é exibida.

2. Marque a caixa de seleção ao lado da vulnerabilidade que deseja corrigir.

3. Clique no botão **Executar o assistente para correção de vulnerabilidades**.

   O assistente para Correção de vulnerabilidades é iniciado. A página **Selecionar tarefa de correção de vulnerabilidades** exibe a lista de todas as tarefas existentes dos seguintes tipos:

   - *Instalar as atualizações necessárias e corrigir vulnerabilidades*
   - *Instalar as atualizações do Windows Update*
   - *Corrigir vulnerabilidades*

   Você não pode modificar os dois últimos tipos de tarefas para instalar novas atualizações. Para instalar novas atualizações, você só pode usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.

4. Se desejar que o assistente exiba apenas as tarefas que corrigem a vulnerabilidade selecionada, ative a opção **Exibir apenas tarefas que corrigem esta vulnerabilidade**.

5. Selecione o que deseja fazer:

- Para iniciar uma tarefa, marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Iniciar**.
- Para adicionar uma nova regra a uma tarefa existente:

  a. Marque a caixa de seleção ao lado do nome da tarefa e clique no botão **Adicionar regra**.

  b. Na página aberta, configure a nova regra:

  - Regra para corrigir vulnerabilidades deste nível de gravidade

    Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

    Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

    Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

    Por padrão, esta opção está desativada.

  - **Regra para corrigir vulnerabilidades por meio de atualizações do mesmo tipo que a atualização definida como recomendada para a vulnerabilidade selecionada** (disponível apenas para vulnerabilidades de software da Microsoft)
  - **Regra para corrigir vulnerabilidades em aplicativos por fornecedor selecionado** (disponível apenas para vulnerabilidades de software de terceiros)
  - **Regra para corrigir uma vulnerabilidade em todas as versões do aplicativo selecionado** (disponível apenas para vulnerabilidades de software de terceiros)
  - **Regra para corrigir a vulnerabilidade selecionada**
  - Aprovar as atualizações que corrigem esta vulnerabilidade

    A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

    Por padrão, esta opção está desativada.

  c. Clique no botão **Adicionar**.

- Para criar uma tarefa:

  a. Clique no botão **Nova tarefa**.

  b. Na página aberta, configure a nova regra:

- Regra para corrigir vulnerabilidades deste nível de gravidade

  Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

  Se essa opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior à gravidade da atualização selecionada (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

  Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

  Por padrão, esta opção está desativada.

- **Regra para corrigir vulnerabilidades por meio de atualizações do mesmo tipo que a atualização definida como recomendada para a vulnerabilidade selecionada** (disponível apenas para vulnerabilidades de software da Microsoft)

- **Regra para corrigir vulnerabilidades em aplicativos por fornecedor selecionado** (disponível apenas para vulnerabilidades de software de terceiros)

- **Regra para corrigir uma vulnerabilidade em todas as versões do aplicativo selecionado** (disponível apenas para vulnerabilidades de software de terceiros)

- **Regra para corrigir a vulnerabilidade selecionada**

- Aprovar as atualizações que corrigem esta vulnerabilidade

  A atualização selecionada será aprovada para instalação. Ative esta opção se algumas regras de instalação da atualização aplicadas somente permitirem a instalação de atualizações aprovadas.

  Por padrão, esta opção está desativada.

c. Clique no botão **Adicionar**.

Se você optou por iniciar uma tarefa, poderá fechar o assistente. A tarefa será concluída no modo de segundo plano. Nenhuma outra ação será necessária.

Se você escolheu adicionar uma regra a uma tarefa existente, a janela de propriedades da tarefa é aberta. A nova regra já foi adicionada às propriedades da tarefa. Você pode visualizar ou modificar a regra ou outras configurações de tarefa. Clique no botão **Salvar** para salvar as alterações.

Caso tenha optado por criar uma tarefa, continue a criar a tarefa no assistente para Novas tarefas. A nova regra adicionada no assistente para Correção de vulnerabilidades é exibida no assistente para Novas tarefas. Ao concluir o assistente, a tarefa *Instalar atualizações necessárias e corrigir vulnerabilidades* é adicionada na lista de tarefas.

Criar a tarefa Corrigir vulnerabilidades

A tarefa *Corrigir vulnerabilidades* permite corrigir vulnerabilidades de software em dispositivos gerenciados executando Windows. É possível corrigir vulnerabilidades de software em softwares de terceiros, incluindo softwares da Microsoft.

Se você não possui uma licença do Gerenciamento de Patches e Vulnerabilidades, não pode criar novas tarefas do tipo *Corrigir vulnerabilidades*. Para corrigir novas vulnerabilidades, adicione-as a uma tarefa *Corrigir vulnerabilidades* existente. Recomendamos usar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* em vez da tarefa *Corrigir vulnerabilidades*. A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* permite instalar várias atualizações e corrigir várias vulnerabilidades automaticamente, de acordo com as regras definidas por você.

Uma interação do usuário pode ser necessária caso você atualize ou corrija uma vulnerabilidade em um aplicativo de terceiros instalado em um dispositivo gerenciado. Por exemplo, pode ser solicitado ao usuário fechar o aplicativo de terceiros, caso esteja aberto no momento.

Para criar uma tarefa Corrigir vulnerabilidades:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Corrigir vulnerabilidades**.
4. Especifique o nome da tarefa que está criando.

   O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (* <>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.
6. Clique no botão **Adicionar**.

   A lista de vulnerabilidades é aberta.
7. Selecione as vulnerabilidades que deseja corrigir e, a seguir, clique em **OK**.

   As vulnerabilidades de software da Microsoft geralmente têm correções recomendadas. Nenhuma ação adicional é necessária para elas. Para vulnerabilidades em softwares de outros fornecedores, primeiro é necessário especificar uma correção do usuário para cada vulnerabilidade que deseja corrigir. Depois disso, será possível adicionar essas vulnerabilidades à tarefa *Corrigir vulnerabilidades*.

8. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Forçar fechamento de aplicativos em sessões bloqueadas**

A execução de aplicativos pode impedir a reinicialização do dispositivo cliente. Por exemplo, se um documento estiver sendo editado em um aplicativo de processamento de texto e não for salvo, o aplicativo não permitirá que o dispositivo seja reiniciado.

Se essa opção estiver ativada, os aplicativos no dispositivo bloqueado serão forçados a fechar antes de o dispositivo ser reiniciado. Como resultado, os usuários podem perder as alterações não salvas.

Se esta opção estiver desativada, o dispositivo bloqueado não será reiniciado. O status da tarefa no dispositivo diz que é necessário reiniciar o dispositivo. Os usuários têm de fechar manualmente todos os aplicativos em execução nos dispositivos bloqueados e reiniciar esses dispositivos.

Por padrão, esta opção está desativada.

9. Especificar as configurações da conta:

- **Conta padrão**

  A tarefa será executada sob a mesma conta que o aplicativo que executa esta tarefa.

  Por padrão, esta opção está selecionada.

- **Especificar conta**

  Preencha os campos **Conta** e **Senha** para especificar os detalhes de uma conta na qual a tarefa é executada. A conta deve ter direitos suficientes para esta tarefa.

- **Conta**

  Conta sob a qual a tarefa é executada.

- **Senha**

  Senha da conta sob a qual a tarefa será executada.

10. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

11. Clique no botão **Concluir**.

    A tarefa é criada e exibida na lista de tarefas.

12. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

13. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

14. Clique no botão **Salvar**.

A tarefa é criada e configurada.

Criar a tarefa Instalar atualizações necessárias e corrigir vulnerabilidades

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* só está disponível sob a licença do Gerenciamento de patches e vulnerabilidades.

A tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* é usada para atualizar e corrigir vulnerabilidades em software de terceiros, incluindo software da Microsoft, instalado nos dispositivos gerenciados. Esta tarefa lhe permite instalar várias atualizações e corrigir várias vulnerabilidades de acordo com certas regras.

Para instalar atualizações ou corrigir vulnerabilidades usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, execute uma das seguintes ações:

- Execute o assistente de Instalação das atualizações ou o assistente para Correção de vulnerabilidades.
- Crie uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*.
- Adicione uma regra para instalação da atualização a uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.

Para criar uma tarefa Instalar as atualizações necessárias e corrigir vulnerabilidades:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.
3. Para o aplicativo Kaspersky Security Center, selecione o tipo de tarefa **Instalar as atualizações necessárias e corrigir vulnerabilidades**.

   Se a tarefa não for exibida, verifique se sua conta tem direitos para **Ler**, **Modificar** e **Executar** na área funcional **Administração de sistema**: **Gerenciamento de Patches e Vulnerabilidades**. Você não pode criar e configurar a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* sem esses direitos de acesso.
4. Especifique o nome da tarefa que está criando. O nome da tarefa não pode conter mais de 100 caracteres e não pode incluir nenhum caractere especial (*<>?:\"|).
5. Dispositivos aos quais a tarefa será atribuída.

6. Especifique as regras para instalação da atualização e, então, especifique as seguintes configurações:

- **Iniciar a instalação ao reiniciar ou fechar o dispositivo**

  Se esta opção estiver ativada, as atualizações serão instaladas quando o dispositivo for reiniciado ou desligado. Caso contrário, as atualizações são instaladas segundo o agendamento.

  Use esta opção caso a instalação das atualizações afete o desempenho do dispositivo.

  Por padrão, esta opção está desativada.

- **Instalar os componentes gerais do sistema necessários**

  Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional.

  Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

  Por padrão, esta opção está desativada.

- **Permitir a instalação de novas versões dos aplicativos durante atualizações**

  Se esta opção estiver ativada, as atualizações serão permitidas quando resultarem na instalação de uma nova versão de um aplicativo de software.

  Se esta opção estiver desativada, o software não será atualizado. Você poderá então instalar novas versões do software manualmente ou através de outra tarefa. Por exemplo, você pode usar esta opção se a infraestrutura da sua empresa não tiver como base uma nova versão do software ou se você quiser verificar uma atualização usando uma infraestrutura de teste.

  Por padrão, esta opção está ativada.

  A atualização de um aplicativo pode causar o funcionamento incorreto de aplicativos dependentes instalados em dispositivos cliente.

- **Baixar atualizações para o dispositivo sem instalá-las**

  Se esta opção estiver ativada, o aplicativo baixa as atualizações em um dispositivo cliente, mas não as instala automaticamente. Você então poderá instalar manualmente as atualizações baixadas.

  As atualizações da Microsoft são baixadas no armazenamento de sistema do Windows. Atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencentes à Kaspersky e à Microsoft) são baixados na pasta especificada no campo **Pasta para download de atualizações**.

  Se esta opção estiver desativada, as atualizações serão instaladas no dispositivo automaticamente.

  Por padrão, esta opção está desativada.

- **Pasta para download de atualizações**

  Esta pasta é usada para baixar atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software não pertencente à Kaspersky e à Microsoft).

- **Ativar diagnóstico avançado**

Se este recurso estiver ativado, o Agente de Rede gravará arquivos de rastreamento mesmo que a gravação de arquivos de rastreamento esteja desativada para o Agente de Rede no Utilitário de Diagnóstico Remoto do Kaspersky Security Center. Os rastreamentos são gravados em dois arquivos por vez; o tamanho total de ambos os arquivos é determinado pelo valor **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**. Quando ambos os arquivos estiverem cheios, o Agente de Rede começará a Gravação neles novamente. Os arquivos com rastreamentos são armazenados na pasta %WINDIR%\Temp. Estes arquivos ficam acessíveis no utilitário de diagnóstico remoto, você pode baixar ou excluí-los nesse local.

Se esse recurso estiver desativado, o Agente de Rede gravará rastreamentos de acordo com as configurações no Utilitário de diagnóstico remoto do Kaspersky Security Center. Nenhum rastreamento adicional é gravado.

Ao criar uma tarefa, você não precisa ativar o diagnóstico avançado. Você poderá querer usar esse recurso mais tarde se, por exemplo, uma execução de tarefa falhar em alguns dos dispositivos e você quiser obter informações adicionais durante outra execução de tarefa.

Por padrão, esta opção está desativada.

- **Tamanho máximo, em MB, de arquivos de diagnóstico avançado**

  O valor padrão é 100 MB e os valores disponíveis estão entre 1 MB e 2048 MB. Os especialistas de Suporte Técnico da Kaspersky podem solicitar que você altere o valor padrão se as informações nos arquivos de diagnóstico avançado que você enviou não forem suficientes para solucionar o problema.

7. Especifique as configurações para reiniciar o sistema operacional:

- **Não reiniciar o dispositivo**

  Os dispositivos clientes não são reiniciados automaticamente após a operação. Para concluir a operação, você deve reiniciar um dispositivo (por exemplo, manualmente ou por meio de uma tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário são salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**

  Os dispositivos clientes sempre serão reiniciados automaticamente se um reinício for necessário para a conclusão da operação. Esta opção é útil para tarefas em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**

  O lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). Esta opção é a mais conveniente para estações de trabalho onde os usuários devem ser capazes de selecionar o momento mais adequado para uma reinicialização.

  Por padrão, esta opção está selecionada.

- **Repetir aviso a cada (min.)**

  Se esta opção estiver ativada, o aplicativo envia uma solicitação para o usuário reiniciar o sistema operacional com a frequência especificada.

  Por padrão, esta opção está ativada. O intervalo predefinido é de 5 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

  Se esta opção estiver desativada, a solicitação será exibida somente uma vez.

- **Reiniciar após (min.)**

  Depois de enviar a solicitação ao usuário, o aplicativo força o reinício do sistema operacional após o término do intervalo de tempo especificado.

  Por padrão, esta opção está ativada. O atraso predefinido é de 30 minutos. Os valores disponíveis estão entre 1 e 1.440 minutos.

- **Tempo de espera antes do fechamento forçado de aplicativos nas sessões bloqueadas (min)**

Os aplicativos são fechados no modo forçado quando o dispositivo for bloqueado (automaticamente, após um intervalo especificado de inatividade ou manualmente).

Se esta opção estiver ativada, os aplicativos serão forçados a fechar no dispositivo bloqueado após a expiração do intervalo de tempo especificado no campo de entrada.

Se essa opção estiver ativada, os aplicativos não serão fechados no dispositivo bloqueado.

Por padrão, esta opção está desativada.

8. Se deseja modificar as configurações padrão da tarefa, ative a opção **Abrir detalhes da tarefa quando a criação for concluída** na página **Concluir a criação da tarefa**. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

9. Clique no botão **Concluir**.

   A tarefa é criada e exibida na lista de tarefas.

10. Clique no nome da tarefa criada para abrir a janela de propriedades da tarefa.

11. Na janela de propriedades da tarefa, especifique as configurações gerais da tarefa de acordo com as suas necessidades.

12. Clique no botão **Salvar**.

    A tarefa é criada e configurada.

Se os resultados da tarefa contiverem um aviso do erro 0x80240033 "Erro de atualização do Windows Update Agent 80240033 ("Não foi possível baixar os termos da licença.")", você poderá resolver esse problema no Registro do Windows.

Adicionar regras para instalação da atualização

Esse recurso está disponível apenas sob a licença do Gerenciamento de patches e vulnerabilidades.

Ao instalar atualizações de software ou corrigir vulnerabilidades de software usando a tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades*, é necessário especificar regras para a instalação da atualização. Essas regras determinam as atualizações a serem instaladas e as vulnerabilidades a serem corrigidas.

As configurações exatas dependem de você ter adicionado uma regra para todas as atualizações, para atualizações do Windows Update ou para atualizações de aplicativos de terceiros (aplicativos criados por fornecedores de software que não sejam a Kaspersky ou a Microsoft). Ao adicionar uma regra para atualizações do Windows Update ou atualizações de aplicativos de terceiros, é possível selecionar aplicativos e versões de aplicativo específicos para os quais deseja instalar atualizações. Ao adicionar uma regra para todas as atualizações, é possível selecionar atualizações específicas que deseja instalar e vulnerabilidades que deseja corrigir com a instalação das atualizações.

É possível adicionar uma regra para a instalação da atualização das seguintes maneiras:

- Adicionando uma regra ao criar uma nova tarefa do tipo Instalar as atualizações necessárias e corrigir vulnerabilidades.
- Adicionando uma regra na guia **Configurações do aplicativo** na janela de propriedades de uma tarefa *Instalar as atualizações necessárias e corrigir vulnerabilidades* existente.
- Por meio do assistente de Instalação das atualizações ou do assistente para Correção de vulnerabilidades.

Para adicionar uma nova regra para todas as atualizações:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para todas as atualizações**.

3. Na página **Critérios gerais**, use as listas suspensas para especificar as seguintes configurações:

   - **Conjunto de atualizações a instalar**

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - **Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que**

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Atualizações**, selecione as atualizações a serem instaladas:

- **Instalar todas as atualizações adequadas**

  Instale todas as atualizações de software que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Instalar apenas as atualizações da lista**

  Instale somente as atualizações de software que você seleciona manualmente da lista. Essa lista contém todas as atualizações de software disponíveis.

  Por exemplo, pode ser necessário selecionar atualizações específicas nos seguintes casos: para verificar a instalação em um ambiente de teste, para atualizar somente aplicativos críticos ou para atualizar somente aplicativos específicos.

  - **Instalar automaticamente todas as atualizações de aplicativos anteriores necessárias para instalar as atualizações selecionadas**

    Mantenha essa opção ativada se você concorda com a instalação de versões provisórias do aplicativo quando forem necessárias para instalar as atualizações selecionadas.

    Se essa opção for desativada, somente as versões selecionadas dos aplicativos são instaladas. Desative esta opção se você quiser atualizar aplicativos de uma forma direta, sem tentar instalar versões sucessivas gradativamente. Se não for possível instalar as atualizações selecionadas sem instalar as versões anteriores dos aplicativos, ocorrerá falha na atualização do aplicativo.

    Por exemplo, você tem a versão 3 de um aplicativo instalado em um dispositivo e quer atualizá-la para a versão 5, mas a versão 5 do aplicativo só pode ser instalada sobre a versão 4. Se essa opção estiver ativada, primeiro o software instalará a versão 4 e, em seguida, a versão 5. Se esta opção estiver desativada, o software não conseguirá atualizar o aplicativo.

    Por padrão, esta opção está ativada.

5. Na página **Vulnerabilidades**, selecione as vulnerabilidades que serão corrigidas instalando as atualizações selecionadas:

- **Corrigir todas as vulnerabilidades que correspondem a outros critérios**

  Corrija todas as vulnerabilidades que atendem aos critérios especificados na página **Critérios gerais** do assistente. Selecionado por padrão.

- **Corrigir somente vulnerabilidades da lista**

  Corrija somente as vulnerabilidades que você seleciona manualmente da lista. Essa lista contém todas as vulnerabilidades detectadas.

  Por exemplo, pode ser necessário selecionar vulnerabilidades específicas nos seguintes casos: para verificar a correção em um ambiente de teste, para corrigir vulnerabilidades somente em aplicativos críticos ou para corrigir vulnerabilidades somente em aplicativos específicos.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para atualizações do Windows Update:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para o Windows Update**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

   - Corrigir vulnerabilidades com um nível de gravidade do MSRC igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pelo Microsoft Security Response Center (MSRC) for igual ou superior ao valor selecionado na lista (**Baixo**, **Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Categorias de atualizações**, selecione as categorias das atualizações a serem instaladas. Essas categorias são iguais às no Catálogo do Microsoft Update. Por padrão, todas as categorias estão selecionadas.

6. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção **Configurações** da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Para adicionar uma nova regra para as atualizações de aplicativos de terceiros:

1. Clique no botão **Adicionar**.

   O assistente de Criação de regras é iniciado. Prossiga pelo assistente usando o botão **Avançar**.

2. Na página **Tipo de regra**, selecione **Regra para atualizações de terceiros**.

3. Na página **Critérios gerais**, especifique as seguintes configurações:

   - Conjunto de atualizações a instalar

     Selecione as atualizações que devem ser instaladas nos dispositivos clientes:

     - **Instale apenas atualizações aprovadas**. Isso instala apenas as atualizações aprovadas.
     - **Instalar todas as atualizações (exceto as recusadas)**. Isso instala as atualizações com o status de aprovação *Aprovado* ou *Indefinido*.
     - **Instalar todas as atualizações (incluindo as recusadas)**. Isso instala todas as atualizações, independentemente dos status de aprovação. Selecione essa esta opção com cuidado. Por exemplo, use esta opção se você quiser verificar a instalação de algumas atualizações recusadas em uma infraestrutura de teste.

   - Corrigir vulnerabilidades com um nível de gravidade igual ou maior do que

     Às vezes as atualizações de software podem prejudicar a experiência do usuário com o software. Nesses casos, você pode decidir instalar somente as atualizações que são críticas para a operação do software e ignorar outras atualizações.

     Se esta opção estiver ativada, as atualizações corrigirão somente as vulnerabilidades cujo nível de gravidade definido pela Kaspersky for igual ou superior ao valor selecionado na lista (**Médio**, **Alto** ou **Crítico**). As vulnerabilidades com um nível de gravidade inferior ao do valor selecionado não são corrigidas.

     Se essa opção estiver desativada, as atualizações corrigirão todas as vulnerabilidades, independentemente do nível de gravidade.

     Por padrão, esta opção está desativada.

4. Na página **Aplicativos**, selecione os aplicativos e versões de aplicativo para os quais você deseja instalar atualizações. Por padrão, todas os aplicativos estão selecionados.

5. Na página **Nome**, especifique o nome para a regra que você está adicionando. É possível mudar esse nome mais tarde na seção Configurações da janela de propriedades da tarefa criada.

Depois que o assistente de Criação de regras concluir a operação, a nova regra será adicionada e exibida na lista de regras no assistente para Novas tarefas ou nas propriedades da tarefa.

Selecionar as correções do usuário para vulnerabilidades em software de terceiros

Para usar a tarefa *Corrigir vulnerabilidades*, você deve especificar manualmente as atualizações de software para corrigir as vulnerabilidades em softwares de terceiros listadas nas configurações da tarefa. A tarefa *Corrigir vulnerabilidades* usa as correções recomendadas para o software da Microsoft e as correções do usuário para outros softwares de terceiros. *Correções do usuário* são atualizações de software para corrigir as vulnerabilidade que o administrador especifica manualmente para instalação.

Para selecionar correções do usuário para vulnerabilidades em software de terceiros:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   A página exibe a lista de vulnerabilidades de software detectadas nos dispositivos cliente.

2. Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade de software para o qual você deseja especificar uma correção do usuário.

   A janela Propriedades da vulnerabilidade é aberta.

3. No painel esquerdo, selecione a seção **Correções do usuário e outras correções**.

   A lista de correções do usuário para a vulnerabilidade de software selecionada é exibida.

4. Clique em **Adicionar**.

   A lista de pacotes de instalação disponíveis é exibida. A lista de pacotes de instalação exibidos corresponde à lista **Operações → Repositórios → Pacotes de instalação**. Se você não criou um pacote de instalação contendo a correção do usuário para a vulnerabilidade selecionada, poderá criar o pacote agora iniciando o Assistente de novo pacote.

5. Selecione um pacote de instalação (ou pacotes) que contenha uma correção (ou correções) do usuário para a vulnerabilidade no software de terceiros.

6. Clique em **Salvar**.

Os pacotes de instalação que contenham correções do usuário para a vulnerabilidade de software são especificados. Quando a tarefa *Corrigir vulnerabilidades* for iniciada, o pacote de instalação será instalado e a vulnerabilidade de software será corrigida.

Visualizar informações sobre vulnerabilidades de software detectadas em todos os dispositivos gerenciados

Depois de verificar o software em dispositivos gerenciados quanto a vulnerabilidades, você pode visualizar a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados. Se você executar a tarefa para a hierarquia de Servidores de Administração, poderá visualizar a lista de dispositivos gerenciados com vulnerabilidades detectadas somente para o Servidor de Administração selecionado.

Para exibir a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados,

No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

A página exibe a lista de vulnerabilidades de software detectadas nos dispositivos cliente.

Você também pode gerar e visualizar um Relatório de vulnerabilidades.

Você pode especificar um filtro para visualizar a lista de vulnerabilidades de software. Clique no ícone **Filtro** () no canto superior direito da lista de vulnerabilidades de software para gerenciar o filtro. Você também pode selecionar um dos filtros predefinidos na lista suspensa **Filtros predefinidos** acima da lista de vulnerabilidades de software.

Você pode obter informações detalhadas sobre qualquer vulnerabilidade na lista.

Para obter informações sobre uma vulnerabilidade de software:

Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade.

A janela de propriedades da vulnerabilidade de software é aberta.

Visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado

Você pode visualizar informações sobre vulnerabilidades de software detectadas no dispositivo gerenciado selecionado que executa o Windows.

Para visualizar a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo para o qual você deseja visualizar as vulnerabilidades de software detectadas.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Na janela de propriedades do dispositivo selecionado selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Vulnerabilidades de software**.

A lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado é exibida.

Para visualizar as propriedades da vulnerabilidade de software selecionada,

Clique no link com o nome da vulnerabilidade de software na lista de vulnerabilidades de software.

A janela de propriedades de vulnerabilidade de software selecionada é exibida.

Visualizar as estatísticas de vulnerabilidades em dispositivos gerenciados

Você pode visualizar estatísticas para cada vulnerabilidade de software em dispositivos gerenciados. As estatísticas são representadas como um diagrama. O diagrama exibe o número de dispositivos com os seguintes status:

- *Ignorado em: <número de dispositivos>*. O status será atribuído se, nas propriedades da vulnerabilidade, o usuário tiver definido manualmente a opção para ignorá-la.
- *Corrigido em: <número de dispositivos>*. O status será atribuído se a tarefa para correção de vulnerabilidade for concluída com êxito.
- *Correção agendada em: <número de dispositivos>*. O status será atribuído se o usuário tiver criado a tarefa para correção de vulnerabilidades, mas a tarefa ainda não tiver sido executada.
- *Correção aplicada em: <número de dispositivos>*. O status será atribuído se o usuário tiver selecionado manualmente uma atualização de software para correção de vulnerabilidades, mas essa atualização de software não tiver corrigido a vulnerabilidade.
- *Correção necessária em: <número de dispositivos>*. Esse status é atribuído se a vulnerabilidade tiver sido corrigida somente em alguns dispositivos gerenciados e precisar ser corrigida em mais dispositivos gerenciados.

Para exibir as estatísticas de uma vulnerabilidade nos dispositivos gerenciados:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   A página exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos gerenciados.

2. Selecione a caixa de seleção ao lado da vulnerabilidade necessária.

3. Clique no botão **Estatísticas de vulnerabilidades em dispositivos**.

O diagrama dos status de vulnerabilidade é exibido. Clicar em um status abre uma lista de dispositivos nos quais a vulnerabilidade tem o status selecionado.

Exportar a lista de vulnerabilidades de software para um arquivo

Você pode exportar a lista de vulnerabilidades exibidas para os arquivos CSV ou TXT. Você pode usar esses arquivos, por exemplo, para enviá-los ao seu gerente de segurança de informações ou para armazená-los para fins de estatística.

Para exportar a lista de vulnerabilidades de software detectadas em todos os dispositivos gerenciados para um arquivo de texto:

1. No menu principal, vá para **Operações → Gerenciamento de patches → Vulnerabilidades de software**.

   A página exibe uma lista de vulnerabilidades nos aplicativos detectados nos dispositivos gerenciados.

2. Clique no botão **Exportar linhas para arquivo TXT** ou **Exportar linhas para arquivo CSV**, dependendo do formato de exportação preferido.

O arquivo que contém a lista de vulnerabilidades de software é baixado no dispositivo que você está usando no momento.

Para exportar a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado para um arquivo de texto:

1. Abra a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado.
2. Selecione as vulnerabilidades de software que você deseja exportar.

   Pule esta etapa se desejar exportar uma lista completa de vulnerabilidades de software detectadas no dispositivo gerenciado.

   Se você deseja exportar a lista completa de vulnerabilidades de software detectadas no dispositivo gerenciado, apenas as vulnerabilidades exibidas na página atual serão exportadas.
3. Clique no botão **Exportar linhas para arquivo TXT** ou **Exportar linhas para arquivo CSV**, dependendo do formato de exportação preferido.

O arquivo que contém a lista de vulnerabilidades de software detectadas no dispositivo gerenciado selecionado é baixado no dispositivo que você está usando no momento.

Ignorar as vulnerabilidades de software

Você pode ignorar as vulnerabilidades do software a ser corrigidas. Os motivos para ignorar vulnerabilidades de software, por exemplo, os seguintes:

- A vulnerabilidade de software não é considerada crítica para sua organização.
- Você entende que a correção de vulnerabilidade do software pode danificar os dados relacionados ao software que exigia a correção da vulnerabilidade.
- Você tem certeza de que a vulnerabilidade do software não é perigosa para a rede da sua organização porque usa outras medidas para proteger seus dispositivos gerenciados.

Você pode ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados ou apenas nos dispositivos gerenciados selecionados.

Para ignorar uma vulnerabilidade de software em todos os dispositivos gerenciados:

1. No menu principal, vá para **Operações** → **Gerenciamento de patches** → **Vulnerabilidades de software**.

   A página exibe a lista de vulnerabilidades de software detectadas nos dispositivos gerenciados.
2. Na lista de vulnerabilidades de software, clique no link com o nome da vulnerabilidade de software que você deseja ignorar.

   A janela Propriedades de vulnerabilidade do software é aberta.
3. Na guia **Geral**, ative a opção **Ignorar vulnerabilidade**.
4. Clique no botão **Salvar**.

   A janela de propriedades de vulnerabilidade do software é fechada.

A vulnerabilidade de software é ignorada em todos os dispositivos gerenciados.

Para ignorar uma vulnerabilidade de software no dispositivo gerenciado selecionado:

1. No menu principal, vá para **Dispositivos → Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Na lista de dispositivos gerenciados, clique no link com o nome do dispositivo no qual você deseja ignorar uma vulnerabilidade de software.

   A janela Propriedades do dispositivo é aberta.

3. Na janela Propriedades do dispositivo, selecione a guia **Avançado**.

4. No painel esquerdo, selecione a seção **Vulnerabilidades de software**.

   A lista de vulnerabilidades de software detectadas no dispositivo é exibida.

5. Na lista de vulnerabilidades de software, selecione a vulnerabilidade que você deseja ignorar no dispositivo selecionado.

   A janela Propriedades de vulnerabilidade do software é aberta.

6. Na janela de propriedades da vulnerabilidade de software, na guia **Geral**, ative a opção **Ignorar vulnerabilidade**.

7. Clique no botão **Salvar**.

   A janela de propriedades de vulnerabilidade do software é fechada.

8. Feche a janela Propriedades do dispositivo.

A vulnerabilidade de software é ignorada no dispositivo selecionado.

A vulnerabilidade de software ignorada não será corrigida após a conclusão das tarefas *Corrigir vulnerabilidades* ou *Instalar as atualizações necessárias e corrigir vulnerabilidades*. É possível excluir as vulnerabilidades de software ignoradas na lista de vulnerabilidades por meio do filtro.

Gerenciando a execução de aplicativos em dispositivos cliente

Esta seção descreve os recursos do Kaspersky Security Center relacionados ao gerenciamento de aplicativos executados nos dispositivos cliente.

Usar o Controle de Aplicativos para gerenciar arquivos executáveis

Você pode usar o componente Controle de Aplicativos para permitir ou bloquear a inicialização de arquivos executáveis nos dispositivos de usuário. O componente Controle de Aplicativos é compatível com sistemas operacionais baseados em Windows e Linux.

Para sistemas operacionais baseados em Linux, o componente Controle de Aplicativos está disponível no Kaspersky Endpoint Security 11.2 para Linux. O componente também está disponível para o Kaspersky Embedded Systems Security para Windows 3.0 ou posterior.

Pré-requisitos

- O Kaspersky Security Center está implementado em sua organização.
- A política do Kaspersky Endpoint Security for Windows ou do Kaspersky Endpoint Security for Linux está criada e ativa.

Fases

O cenário de uso do Controle de Aplicativos prossegue em fases:

1. **Formar e visualizar a lista de arquivos executáveis em dispositivos clientes**

   Esta etapa ajuda a descobrir quais arquivos executáveis são encontrados nos dispositivos gerenciados. Exiba a lista de arquivos executáveis e compare-a com a lista de arquivos executáveis permitidos e proibidos. As restrições sobre a utilização de arquivos executáveis podem estar relacionadas às políticas de segurança da informação em sua organização.

   Instruções de como proceder:

   - Console de administração: Inventário de arquivos executáveis
   - Kaspersky Security Center Web Console: Obtendo e visualizando uma lista de arquivos executáveis armazenados nos dispositivos cliente

2. **Criar categorias para arquivos executáveis usados em sua organização**

   Analise a lista de arquivos executáveis armazenados nos dispositivos gerenciados. Com base na análise, crie categorias para arquivos executáveis. É recomendável criar uma categoria "Aplicativos de trabalho" que cubra o conjunto padrão de arquivos executáveis usados na sua organização. Se diferentes grupos de segurança usarem seus próprios conjuntos de arquivos executáveis em seu trabalho, uma categoria poderá ser criada para cada grupo de segurança.

   Instruções de como proceder:

   - Console de Administração: Criação de uma categoria de aplicativo com conteúdo adicionado manualmente, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir de dispositivos selecionados, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir da pasta selecionada.
   - Kaspersky Security Center Web Console: Criação de uma categoria de aplicativo com conteúdo adicionado manualmente, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir de dispositivos selecionados, Criação de uma categoria de aplicativo que inclui arquivos executáveis a partir da pasta específica.

3. **Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security**

   Configure o componente Controle de Aplicativos na política do Kaspersky Endpoint Security usando as categorias criadas no estágio anterior.

   Instruções de como proceder:

   - Console de Administração: Configurar o gerenciamento da inicialização do aplicativo em dispositivos cliente
   - Kaspersky Security Center Web Console: Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows

4. **Ativar o componente Controle de Aplicativos no modo de teste**

Para garantir que as regras do Controle de Aplicativos não bloqueiem os arquivos executáveis necessários para o trabalho do usuário, é recomendável ativar o teste das regras do Controle de Aplicativos e analisar a sua operação após a criação de novas regras. Quando o teste está ativado, o Kaspersky Endpoint Security for Windows não bloqueia os arquivos executáveis cuja inicialização é proibida pelas regras do Controle de Aplicativos, mas envia notificações sobre a inicialização ao Servidor de Administração.

Ao testar as regras do Controle de Aplicativos, é recomendável realizar as seguintes ações:

- Determine o período de teste. O período de teste pode variar de vários dias a dois meses.
- Examine os eventos resultantes do teste da operação do Controle de Aplicativos.

Instruções para o Kaspersky Security Center Web Console: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e ative a opção **Modo de teste** no processo de configuração.

5. **Alteração das configurações de categorias do componente Controle de Aplicativos**

   Se necessário, faça alterações nas configurações do Controle de Aplicativos. Com base nos resultados do teste, você pode adicionar arquivos executáveis relativos a eventos do componente Controle de Aplicativos a uma categoria com conteúdo adicionado manualmente.

   Instruções de como proceder:

   - Console de Administração: Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos
   - Kaspersky Security Center Web Console: Adicionar arquivos executáveis relacionados a eventos à categoria de aplicativo

6. **Aplicar as regras do Controle de Aplicativos no modo de operação**

   Após as regras de Controle de Aplicativos terem sido testadas e a configuração das categorias estar concluída, você pode aplicar as regras do Controle de Aplicativos no modo de operação.

   Instruções para o Kaspersky Security Center Web Console: Configurar o componente Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows. Siga estas instruções e desative a opção **Modo de teste** no processo de configuração.

7. **Verificar a configuração do Controle de Aplicativos**

   Certifique-se de ter feito o seguinte:

   - Categorias criadas para arquivos executáveis.
   - Configurado o Controle de Aplicativos usando as categorias.
   - Aplicado as regras do Controle de Aplicativos no modo de operação.

Resultados

Quando o cenário estiver concluído, a inicialização dos arquivos executáveis nos dispositivos gerenciados será controlada. Os usuários podem executar apenas aqueles arquivos executáveis permitidos na sua organização e não podem executar arquivos executáveis proibidos na sua organização.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux

- Kaspersky Security for Virtualization Light Agent
- Ajuda do Kaspersky Embedded Systems Security for Windows
- Ajuda do Kaspersky Embedded Systems Security for Linux

Modos e categorias do Controle de Aplicativos

O componente Controle de Aplicativos monitora as tentativas dos usuários de iniciar arquivos executáveis. Você pode usar as regras de Controle de Aplicativos para controlar a inicialização de arquivos executáveis.

> O componente Controle de Aplicativos está disponível para Kaspersky Endpoint Security for Windows, Kaspersky Endpoint Security 11.2 for Linux e versões posteriores, e para o Kaspersky Security for Virtualization Light Agent. Todas as instruções nesta seção descrevem a configuração do Controle de Aplicativos para o Kaspersky Endpoint Security for Windows.

A inicialização de arquivos executáveis cujas configurações não correspondem a nenhuma das regras do Controle de Aplicativos é regulada pelo modo de operação selecionado do componente:

- *Lista de bloqueio*. O modo é usado se você deseja permitir a inicialização de todos os arquivos executáveis, exceto aqueles especificados nas regras de bloqueio. Este modo é selecionado por padrão.
- *Lista de permissão*. O modo é usado se você deseja bloquear a inicialização de todos os arquivos executáveis, exceto aqueles especificados nas regras de permissão.

As regras de Controle de Aplicativos são implementadas por meio de categorias para arquivos executáveis. No Kaspersky Security Center, há três tipos de categorias:

- Categoria com conteúdo adicionado manualmente. Você define condições, por exemplo, metadados do arquivo, código de hash do arquivo, certificado do arquivo, categoria KL, caminho do arquivo, para incluir arquivos executáveis na categoria.
- Categoria que inclui os arquivos executáveis dos dispositivos selecionados. Você especifica um dispositivo cujos arquivos executáveis são incluídos automaticamente na categoria.
- Categoria que inclui os arquivos executáveis da pasta selecionada. Você especifica uma pasta da qual os arquivos executáveis são incluídos automaticamente na categoria.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ajuda do Kaspersky Embedded Systems Security for Windows
- Ajuda do Kaspersky Embedded Systems Security for Linux

Obter e visualizar uma lista de aplicativos instalados nos dispositivos clientes

O Kaspersky Security Center executa um inventário de todos os softwares instalados nos dispositivos cliente gerenciados que executam o Linux e Windows.

O Agente de Rede compila uma lista de aplicativos instalados em um dispositivo cliente e, a seguir, transmite esta lista para o Servidor de Administração. São necessários cerca de 10 a 15 minutos para o Agente de Rede atualizar a lista de aplicativos.

Para dispositivos clientes baseados no Windows, o Agente de Rede recebe a maioria das informações sobre os aplicativos instalados do registro do Windows. Para dispositivos clientes baseados em Linux, os gerenciadores de pacotes fornecem ao Agente de Rede informações sobre os aplicativos instalados.

Caso um aplicativo da seção de **Registro de aplicativos** tenha sido detectado em um dispositivo Linux, as propriedades do aplicativo não conterão as informações sobre os arquivos executáveis relacionados.

Para exibir a lista de aplicativos instalados nos dispositivos gerenciados:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Registro de aplicativos**.

   A página exibe uma tabela com os aplicativos instalados nos dispositivos gerenciados. Selecione o aplicativo para visualizar suas propriedades, por exemplo, nome do fornecedor, número da versão, lista de arquivos executáveis, lista de dispositivos nos quais o aplicativo está instalado, lista de atualizações de software disponíveis e lista de vulnerabilidades de software detectadas.

2. É possível agrupar e filtrar os dados da tabela com os aplicativos instalados da seguinte forma:

   - Clique no ícone de configurações ( ) no canto superior direito da tabela.

     No menu **Configurações de colunas** resultante, selecione as colunas a serem exibidas na tabela. Para visualizar o tipo de sistema operacional dos dispositivos clientes nos quais o aplicativo está instalado, selecione a coluna **Tipo de sistema operacional**.

   - Clique no ícone de filtro ( ) no canto superior direito da tabela e depois, especifique e aplique o critério de filtro no menu resultante.

     A tabela filtrada de aplicativos instalados é exibida.

Para visualizar a lista de aplicativos instalados em um dispositivo gerenciado específico,

No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados** → **<nome do dispositivo>** → **Avançado** → **Registro de aplicativos**. Neste menu, é possível exportar a lista de aplicativos para um arquivo CSV ou TXT.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

- Ajuda do Kaspersky Embedded Systems Security for Windows
- Ajuda do Kaspersky Embedded Systems Security for Linux

Obter e visualizar uma lista de arquivos executáveis instalados em dispositivos clientes

É possível obter a lista de arquivos executáveis armazenados em dispositivos clientes de uma das seguintes maneiras:

- Habilitar notificações sobre inicialização de aplicativos na política do Kaspersky Endpoint Security.
- Criar uma tarefa de inventário.

Ativar notificações sobre inicialização de aplicativos na política do Kaspersky Endpoint Security

Para habilitar notificações sobre a inicialização de aplicativos:

1. Abra as configurações da política do Kaspersky Endpoint Security e vá para **Configurações gerais → Relatórios e armazenamento**.
2. No grupo de configurações **Transferência de dados para o Servidor de Administração**, marque a caixa de seleção **Sobre aplicativos iniciados** e salve as alterações.

Quando um usuário tenta iniciar arquivos executáveis, informações sobre esses arquivos são adicionadas à lista de arquivos executáveis em um dispositivo cliente. O Kaspersky Endpoint Security envia essas informações ao Agente de Rede e, em seguida, o Agente de Rede as envia ao Servidor de Administração.

Criar uma tarefa de inventário

O recurso de inventário de arquivos executáveis está disponível para os seguintes aplicativos:

- Kaspersky Endpoint Security for Windows
- Kaspersky Endpoint Security for Linux versão 11.2 e posterior
- Kaspersky Security for Virtualization 4.0 Light Agent e versões posteriores

É possível reduzir a carga no banco de dados enquanto as informações sobre os aplicativos instalados são obtidas. Para economizar espaço em um banco de dados, execute uma tarefa de inventário em dispositivos de referência nos quais um conjunto padrão de software está instalado. O número desejável de dispositivos é entre 1 e 3.

Não recomendamos executar a tarefa de inventário ao usar os seguintes bancos de dados: MySQL, PostgreSQL, SQL Server Express Edition, MariaDB (todas as edições).

Para criar uma tarefa de inventário para arquivos executáveis em dispositivos cliente:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.

   A lista de tarefas é exibida.

2. Clique no botão **Adicionar**.

   O Assistente para novas tarefas inicia. Siga as etapas do Assistente.

3. Na página **Nova tarefa**, na lista suspensa **Aplicativo**, selecione Kaspersky Endpoint Security for Windows ou Kaspersky Endpoint Security for Linux, dependendo do tipo de sistema operacional dos dispositivos clientes.

4. Na lista suspensa **Tipo de tarefa**, selecione **Inventário**.

5. Na página **Concluir a criação da tarefa**, clique no botão **Concluir**.

   Após a conclusão do Assistente para novas tarefas, a tarefa **Inventário** será criada e configurada. Se desejar, você pode alterar as configurações da tarefa criada. A tarefa recém-criada é exibida na lista de tarefas.

Para uma descrição detalhada da tarefa de inventário, consulte as seguintes ajudas:

- Ajuda do Kaspersky Endpoint Security for Windows
- Ajuda do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent

Após a tarefa **Inventário** ser executada, a lista de arquivos executáveis armazenados nos dispositivos gerenciados é formada e você pode visualizá-la.

Durante o inventário, arquivos executáveis nos seguintes formatos podem ser detectados (dependendo da opção selecionada nas propriedades da tarefa de inventário): MZ, COM, PE, NE, SYS, CMD, BAT, PS1, JS, VBS, REG, MSI, CPL, DLL, JAR e HTML.

Visualizar a lista de arquivos executáveis armazenados nos dispositivos gerenciados

Para exibir a lista dos arquivos executáveis armazenados nos dispositivos clientes:

No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Arquivos executáveis**.

A página exibe a lista de arquivos executáveis armazenados nos dispositivos clientes.

Se necessário, é possível enviar o arquivo executável do dispositivo gerenciado para o dispositivo em que o Kaspersky Security Center Web Console está aberto.

Para enviar um arquivo executável:

1. No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Arquivos executáveis**.

2. Clique no link do arquivo executável que deseja enviar.

3. Na janela que é aberta, vá para a seção **Dispositivos** e marque a caixa de seleção do dispositivo gerenciado do qual você deseja enviar o arquivo executável.

   Antes de enviar o arquivo executável, certifique-se de que o dispositivo gerenciado tenha uma conexão direta com o Servidor de Administração marcando a caixa de seleção **Não desconectar do Servidor de Administração**.

4. Clique no botão **Enviar**.

   O arquivo executável selecionado é baixado para envio posterior ao dispositivo onde o Kaspersky Security Center Web Console está aberto.

Criar uma categoria de aplicativos com conteúdo adicionado manualmente

Você pode especificar um conjunto de critérios como um modelo de arquivos executáveis cuja inicialização deseja permitir ou bloquear na sua organização. Com base nos arquivos executáveis correspondentes aos critérios, você poderá criar uma categoria de aplicativos e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria de aplicativos com conteúdo adicionado manualmente:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Categorias de aplicativos**.

   A página com uma lista de categorias de aplicativos é exibida.

2. Clique no botão **Adicionar**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na etapa **Selecionar método de criação de categoria**, selecione a opção **Categoria com conteúdo adicionado manualmente. Os dados dos arquivos executáveis são adicionados manualmente à categoria**.

4. Na etapa **Condições**, clique no botão **Adicionar** para adicionar um critério de condição para incluir arquivos na criação da categoria.

5. Na etapa **Critérios da condição**, selecione um tipo de regra para a criação de categoria na lista:

- **Da categoria KL**

  Se esta opção estiver selecionada, você poderá especificar uma categoria de aplicativos da Kaspersky como a condição para adicionar aplicativos da categoria do usuário. Os aplicativos da categoria da Kaspersky especificada serão adicionados à categoria de aplicativos do usuário.

- **Selecionar certificado do repositório**

  Se esta opção estiver selecionada, você pode especificar certificados do armazenamento. A condição de categoria só se relaciona com os arquivos executáveis assinados pelo certificado definido.

- **Especificar caminho para o aplicativo (máscaras aceitas)**

  Se esta opção estiver selecionada, você pode especificar o caminho para a pasta no dispositivo cliente contendo os arquivos executáveis a serem adicionados à categoria de aplicativos do usuário. Você pode usar expressões regulares como *C:\path_to_exe*.*, por exemplo: *C:\Program Files\Internet Explorer*.*

- **Unidade removível**

  Se esta opção estiver selecionada, você pode especificar o tipo de mídia (qualquer unidade ou unidade removível) no qual o aplicativo será executado. Os aplicativos que foram executados no tipo de unidade selecionado são adicionados à categoria de aplicativo do usuário.

- **Hash, metadados ou certificado**:

  - **Selecionar na lista de arquivos executáveis**

    Se esta opção estiver selecionada, você poderá utilizar a lista de arquivos executáveis no dispositivo cliente para selecionar e adicionar aplicativos deles à categoria.

  - **Selecionar do registro de aplicativos**

Se esta opção for selecionada, o registro dos aplicativos será exibido. Após selecionar um aplicativo no registro, uma janela se abrirá com os parâmetros já preenchidos com metadados do aplicativo selecionado:

- Nome do arquivo.
- Versão do arquivo. Você pode especificar um valor preciso da versão ou descrever uma condição, por exemplo "posterior a 5.0".
- Nome do aplicativo.
- Versão do aplicativo. Você pode especificar um valor preciso da versão ou descrever uma condição, por exemplo "posterior a 5.0".
- Fornecedor.

Observe que só será bloqueada a inicialização de arquivos executáveis que atendam aos parâmetros especificados, mas não a inicialização de aplicativos que você selecionou. Você poderá prosseguir para a próxima etapa se os metadados do aplicativo selecionado corresponderem ao do arquivo executável que é iniciado quando você inicia o aplicativo. Caso contrário, altere manualmente os valores para que correspondam aos metadados do arquivo executável.

- **Especificar manualmente**

Se esta opção estiver selecionada, você deve especificar hash do arquivo, metadados ou certificado como a condição para adicionar aplicativos à categoria do usuário.

Hash do arquivo

Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é necessário selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center de arquivos nessa categoria. As informações de valores de hash calculados por funções de hash são armazenadas no banco de dados do Servidor de Administração.

SHA256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center de arquivos na categoria:

- Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.

- Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA256 hash criptográfica para arquivos da categoria.

- Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

Metadados

Se esta opção for selecionada, você poderá especificar os metadados do arquivo como nome, versão e fornecedor. A condição de categoria só se relaciona aos arquivos executáveis com os mesmos metadados.

Certificado

Se esta opção estiver selecionada, você pode especificar certificados do armazenamento. A condição de categoria só se relaciona com os arquivos executáveis assinados pelo certificado definido.

- Do arquivo ou do pacote MSI/pasta arquivada

Se esta opção estiver selecionada, você poderá especificar um arquivo de instalador MSI como a condição para adicionar aplicativos à categoria de usuário. Os metadados do instalador do aplicativo serão enviados ao Servidor de Administração. Os aplicativos para os quais o instalador de metadados for o mesmo para o instalador MSI especificado, são adicionados à categoria de aplicativos do usuário.

O critério selecionado é adicionado à lista de condições.

Você pode adicionar quantos critérios para a categoria de aplicativo de criação forem necessários.

6. Na etapa **Exclusões**, clique no botão **Adicionar** para adicionar um critério de condição exclusivo para excluir arquivos da categoria que está sendo criada.

7. Na etapa **Critérios da condição**, selecione um tipo de regra na lista tal como você selecionou um tipo de regra para a criação da categoria.

Quando o assistente for concluído, uma categoria de aplicativos será criada. Ela é exibida na lista de categorias de aplicativos. Você pode usar a categoria de aplicativos criada ao configurar o Controle de Aplicativos.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ajuda do Kaspersky Embedded Systems Security for Windows
- Ajuda do Kaspersky Embedded Systems Security for Linux

Criar uma categoria de aplicativo que inclua arquivos executáveis dos dispositivos selecionados

Você pode usar arquivos executáveis de dispositivos selecionados como um modelo de arquivos executáveis que deseja permitir ou bloquear. Com base nos arquivos executáveis dos dispositivos selecionados, é possível criar uma categoria e usá-la na configuração do componente Controle de Aplicativos.

Para recuperar a lista de arquivos executáveis de dispositivos:

1. Certifique-se de que a política do Kaspersky Endpoint Security for Windows ou do Kaspersky Endpoint Security for Linux foi criada e está ativa. Ative o componente Controle de Aplicativos na política.

2. Obtenha uma lista de arquivos executáveis armazenados nos dispositivos cliente.

Para criar uma categoria que inclua arquivos executáveis de dispositivos selecionados:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Categorias de aplicativos**.

   A página com uma lista de categorias é exibida.

2. Clique no botão **Adicionar**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na etapa **Selecionar método de criação de categoria**, especifique o nome da categoria e selecione a opção **Categoria que inclui arquivos executáveis dos dispositivos selecionados. Esses arquivos executáveis são processados automaticamente e suas métricas são adicionadas à categoria**.

4. Clique em **Adicionar**.

5. Na janela exibida, selecione um dispositivo ou dispositivos cujos arquivos executáveis serão usados para criar a categoria.

6. Especificar as seguintes configurações:

- Algoritmo de cálculo do valor hash

  Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é necessário selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center de arquivos nessa categoria. As informações de valores de hash calculados por funções de hash são armazenadas no banco de dados do Servidor de Administração.

  SHA256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

  Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center de arquivos na categoria:

  - Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.

  - Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA256 hash criptográfica para arquivos da categoria.

  Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

  A caixa de seleção **Calcular SHA256 para arquivos nesta categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e quaisquer versões posteriores)** está marcada por padrão.

  A caixa de seleção **Calcular o MD5 para os arquivos nesta categoria (suportado pelas versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** é selecionado por padrão.

- Sincronizar dados com o repositório do Servidor de Administração

  Selecione esta opção se você desejar que o Servidor de Administração verifique periodicamente as alterações na pasta (ou pastas) especificada.

  Por padrão, esta opção está desativada.

  Se você ativar esta opção, especifique o período (em horas) para verificar as alterações nas pastas especificadas. Por padrão, o intervalo de verificação é de 24 horas.

- Tipo de arquivo

Nesta seção, você pode especificar o tipo de arquivo usado para criar a categoria de aplicativo.

Todos os arquivos. Todos os arquivos são levados em consideração durante a criação da categoria. Por padrão, esta opção está selecionada.

Somente arquivos fora das categorias de aplicativos. Somente arquivos fora das categorias de aplicativos são levados em consideração durante a criação da categoria.

- **Pastas**

  Nesta seção, você pode especificar quais pastas dos dispositivos selecionados contendo arquivos usados para criar a categoria de aplicativos.

  Todas as pastas. Todas as pastas são levadas em consideração para a categoria de criação. Por padrão, esta opção está selecionada.

  Pasta especificada. Somente a pasta especificada é levada em consideração para a categoria de criação. Se você selecionar esta opção, deverá especificar o caminho para a pasta.

Quando o assistente for concluído, a categoria de arquivos executáveis será criada. Ela é exibida na lista de categorias. Você pode usar a categoria criada ao configurar o Controle de Aplicativos.

Criar uma categoria de aplicativo que inclua arquivos executáveis da pasta selecionada

Você pode usar arquivos executáveis da pasta selecionada como um padrão de arquivos executáveis que deseja permitir ou bloquear. Com base nos arquivos executáveis da pasta selecionada, você poderá criar uma categoria de aplicativos e usá-la na configuração do componente Controle de Aplicativos.

Para criar uma categoria que inclui arquivos executáveis da pasta selecionada:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Categorias de aplicativos**.

   A página com uma lista de categorias é exibida.

2. Clique no botão **Adicionar**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

3. Na etapa **Selecionar método de criação de categoria**, especifique o nome da categoria e selecione a opção **Categoria que inclui arquivos executáveis de uma pasta específica. Os arquivos executáveis de aplicativos copiados para a pasta especificada são processados automaticamente e suas métricas são adicionadas à categoria**.

4. Especifique a pasta cujos arquivos executáveis serão usados para criar a categoria.

5. Defina as seguintes configurações:

- **Incluir bibliotecas de link dinâmico (DLL) nessa categoria**

  A categoria de aplicativo inclui bibliotecas de link dinâmico (arquivos no formato de DLL), e o componente Controle de Aplicativos registra as ações de tais bibliotecas que ocorrem no sistema. A inclusão de arquivos DLL na categoria pode abaixar o desempenho do Kaspersky Security Center.

  Por padrão, esta caixa de seleção está desmarcada.

- **Incluir dados de script nesta categoria**

  A categoria do aplicativo inclui dados sobre scripts, e os scripts não são bloqueados pelo Proteção Contra Ameaças da Web. Incluir os dados de script na categoria pode diminuir o desempenho do Kaspersky Security Center.

  Por padrão, esta caixa de seleção está desmarcada.

- **Algoritmo de cálculo de valor hash**: **Calcular o SHA-256 para arquivos nessa categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores)/Calcular o MD5 para os arquivos nesta categoria (compatível com versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)**

Dependendo da versão do aplicativo de segurança instalada em dispositivos na sua rede, é necessário selecionar um algoritmo para o cálculo do valor hash pelo Kaspersky Security Center de arquivos nessa categoria. As informações de valores de hash calculados por funções de hash são armazenadas no banco de dados do Servidor de Administração.

SHA256 é uma função hash criptográfica: nenhuma vulnerabilidade foi encontrada nesse algoritmo, portanto ela é considerada a função criptográfica mais confiável na atualidade. O Kaspersky Endpoint Security 10 Service Pack 2 for Windows e versões posteriores suportam o cálculo SHA256. O cálculo da função MD5 hash é suportado por todas as versões anteriores do Kaspersky Endpoint Security 10 Service Pack 2 for Windows.

Selecione qualquer das opções de cálculo do valor hash pelo Kaspersky Security Center de arquivos na categoria:

- Se todas as instâncias dos aplicativos de segurança instalados em sua rede forem versões do Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou posteriores, selecione a caixa de seleção **SHA-256**. Não recomendamos que você adicione nenhuma categoria criada de acordo com o critério do hash SHA256 de um arquivo executável para versões anteriores à versão do Kaspersky Endpoint Security 10 Service Pack 2 for Windows. Isto pode resultar em falhas na operação do aplicativo de segurança. Neste caso, você pode usar a função MD5 hash criptográfica para arquivos da categoria.

- Se alguma versão anterior ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows estiver instalada na sua rede, selecione **Hash MD5**. Você não pode adicionar uma categoria que foi criada com base no critério do checksum MD5 de um arquivo executável para o Kaspersky Endpoint Security 10 Service Pack 2 for Windows ou versões posteriores. Neste caso, você pode usar a função SHA256 hash criptográfica para arquivos da categoria.

Se diferentes dispositivos usam versões anteriores e posteriores do Kaspersky Endpoint Security 10, selecione as caixas de seleção **SHA-256** e **Hash MD5**.

A caixa de seleção **Calcular SHA256 para arquivos nesta categoria (compatível com o Kaspersky Endpoint Security 10 Service Pack 2 for Windows e quaisquer versões posteriores)** está marcada por padrão.

A caixa de seleção **Calcular o MD5 para os arquivos nesta categoria (suportado pelas versões anteriores ao Kaspersky Endpoint Security 10 Service Pack 2 for Windows)** é selecionado por padrão.

- **Forçar verificação da pasta para procurar alterações**

Se esta opção estiver ativada, o aplicativo verifica regularmente a pasta de inclusão de conteúdo à categoria, buscando por alterações. Você pode especificar a frequência de verificações (em horas) no campo de entrada próximo da caixa de seleção. Por padrão, o tempo de intervalo entre verificações forçadas é de 24 horas.

Se esta opção estiver ativada, o aplicativo não força nenhuma verificação da pasta. O Servidor tenta acessar arquivos se eles tiverem sido modificados, adicionados ou excluídos.

Por padrão, esta opção está desativada.

Quando o assistente for concluído, a categoria de arquivos executáveis será criada. Ela é exibida na lista de categorias. Você pode usar a categoria na configuração do Controle de Aplicativos.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux

- Kaspersky Security for Virtualization Light Agent
- Ajuda do Kaspersky Embedded Systems Security for Windows
- Ajuda do Kaspersky Embedded Systems Security for Linux

Visualizando a lista de categorias de aplicativo

Você pode visualizar a lista de categorias de arquivos executáveis configuradas, bem como as configurações de cada uma delas.

Para visualizar a lista de categorias de aplicativos,

No menu principal, vá para **Operações** → **Aplicativos de terceiros** → **Categorias de aplicativos**.

A página com uma lista de categorias é exibida.

Para visualizar propriedades de uma categoria de aplicativos,

Clique no nome da categoria.

A janela de propriedades da categoria é exibida. As propriedades estão agrupadas em várias guias.

Configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows

Após você criar as categorias do Controle de Aplicativos, poderá usá-las para configurar o Controle de Aplicativos nas políticas do Kaspersky Endpoint Security for Windows.

Para configurar o Controle de Aplicativos na Política do Kaspersky Endpoint Security for Windows:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
   Uma página com uma lista de políticas é exibida.
2. Clique na Política do **Kaspersky Endpoint Security for Windows**.
   A janela Propriedades da política será aberta.
3. Acesse **Configurações do aplicativo** → **Controles de Segurança** → **Controle de Aplicativos**.
   A janela **Controle de Aplicativos** com as configurações de Controle de Aplicativos é exibida.
4. A opção **Controle de Aplicativos** está ativada por padrão. Certifique-se de que o botão de alternância **Controle de Aplicativos DESABILITADO** esteja na posição desabilitada.

5. No configurações de bloqueio **Configurações de Controle de Aplicativos**, ative o modo de operação para aplicar as Regras de Controle de Aplicativos e permita que o Kaspersky Endpoint Security for Windows bloqueie a inicialização de aplicativos.

   Se você quiser testar as Regras de Controle de Aplicativos, na seção **Configurações de Controle de Aplicativos**, ative o modo de teste. No modo de teste, o Kaspersky Endpoint Security for Windows não bloqueia a inicialização de aplicativos, mas registra no relatório informações sobre as regras acionadas. Clique no link **Ver relatório** para visualizar esta informação.

6. Ative a opção **Controlar carregamento dos módulos DLL** caso desejar que o Kaspersky Endpoint Security for Windows monitore o carregamento dos módulos DLL quando os aplicativos forem iniciados pelos usuários.

   As informações sobre o módulo e o aplicativo que carregou o módulo serão salvas em um relatório.

   O Kaspersky Endpoint Security for Windows monitora apenas os módulos DLL e drivers carregados após a opção **Controlar carregamento dos módulos DLL** tiver sido selecionada. Reinicie o dispositivo após selecionar a opção **Controlar carregamento dos módulos DLL** se quiser que o Kaspersky Endpoint Security for Windows monitore todos os módulos DLL e drivers, incluindo aqueles carregados antes do Kaspersky Endpoint Security for Windows ter sido iniciado.

7. (Opcional) No bloco **Modelos de mensagem**, altere o modelo da mensagem exibida quando um aplicativo é impedido de iniciar e o modelo da mensagem de e-mail enviada para você.

8. Nas configurações de bloqueio **Modo de Controle de Aplicativos**, selecione o modo **Lista de bloqueio** ou **Lista de permissão**.

   Por padrão, o modo **Lista de bloqueio** é selecionado.

9. Clique no link **Configurações das listas de regras**.

   A janela **Listas de bloqueio e permissão** é aberta para permitir a adição de uma categoria de aplicativo. Por padrão, a guia **Lista de bloqueio** é selecionada se o modo **Lista de bloqueio** estiver selecionado ou a guia **Lista de aprovação** é selecionada se o modo **Lista de aprovação** estiver selecionado.

10. Na janela **Listas de bloqueio e de aprovação**, clique no botão **Adicionar**.

    A janela **Regra de Controle de Aplicativos** abre.

11. Clique no link **Escolha uma categoria**.

    A janela **Categoria de Aplicativo** é aberta.

12. Adicione a categoria de aplicativo (ou categorias) que você criou anteriormente.

    Você pode editar as configurações de uma categoria criada clicando no botão **Editar**.

    Você pode criar uma nova categoria clicando no botão **Adicionar**.

    Você pode excluir uma categoria da lista clicando no botão **Excluir**.

13. Após lista de categorias de aplicativos estiver completa, clique no botão **OK**.

    A janela **Categoria de Aplicativos** é fechada.

14. Na janela Regra de **Controle de Aplicativos**, na seção **Pessoas e seus direitos**, crie uma lista de usuários e grupos de usuários para aplicar a regra de Controle de Aplicativos.

15. Clique no botão **OK** para salvar as configurações e fechar a janela **Regra de Controle de Aplicativos**.

16. Clique no botão **OK** para salvar as configurações e fechar a janela **Listas de bloqueio e de aprovação**.

17. Clique no botão **OK** para salvar as configurações e fechar a janela **Controle de Aplicativos**.

18. Feche a janela com as configurações da política do Kaspersky Endpoint Security for Windows.

O Controle de Aplicativos está configurado. Após a política ter sido propagada para os dispositivos cliente, a inicialização dos arquivos executáveis é gerenciada.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ajuda do Kaspersky Embedded Systems Security for Windows
- Ajuda do Kaspersky Embedded Systems Security for Linux

Adicionar arquivos executáveis relativos ao evento na categoria de aplicativos

Após configurar o Controle de Aplicativos nas políticas do Kaspersky Endpoint Security for Windows, os seguintes eventos serão exibidos na lista de eventos:

- **Inicialização do aplicativo proibida** (evento *Crítico*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para aplicar regras.
- **Proibida a inicialização do aplicativo em modo de teste** (evento *Informativo*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para testar regras.
- **Mensagem ao administrador sobre a proibição de inicialização do aplicativo** (evento de *Advertência*). Este evento será exibido se você tiver configurado o Controle de Aplicativos para aplicar regras e um usuário tiver solicitado acesso ao aplicativo bloqueado para inicialização.

É recomendável criar seleções de eventos para visualizar eventos relacionados à operação do Controle de Aplicativos.

Você pode adicionar arquivos executáveis relacionados aos eventos do Controle de Aplicativos à uma categoria de aplicativos existente ou a uma nova categoria de aplicativos. Você pode adicionar arquivos executáveis apenas à categoria de aplicativos com conteúdo adicionado manualmente.

Para adicionar arquivos executáveis relativos aos eventos de Controle de Aplicativos para uma categoria de aplicativos:

1. No menu principal, acesse **Monitoramento e relatórios → Seleções de eventos**.

   A lista de seleção de eventos é exibida.

2. Selecione a seleção de eventos para visualizar os eventos relacionados ao Controle de Aplicativos e iniciar essa seleção de eventos.

   Se você não criou uma seleção de eventos relacionada ao Controle de Aplicativos, poderá selecionar e iniciar uma seleção predefinida, por exemplo, **Eventos recentes**.

   A lista de eventos é exibida.

3. Selecione os eventos cujos arquivos executáveis associados você deseja adicionar à categoria de aplicativos e clique no botão **Atribuir à categoria**.

   O Assistente para Novas Categorias inicia. Prossiga pelo assistente usando o botão **Avançar**.

4. Na página do assistente, especifique as configurações relevantes:

- Na seção **Ação em arquivo executável relacionado ao evento**, selecione uma das seguintes opções:
  - Adicionar a uma nova categoria de aplicativos

    Selecione esta opção se desejar criar uma nova categoria de aplicativo com base nos arquivos executáveis relacionados ao evento.

    Por padrão, esta opção está selecionada.

    Se você selecionou esta opção, especifique um novo nome de categoria.

  - Adicionar a uma categoria de aplicativos existente

    Selecione esta opção se você quiser adicionar arquivos executáveis relativos ao evento a uma categoria de aplicativo existente.

    Por padrão, esta opção não está selecionada.

    Se você selecionou essa opção, selecione a categoria de aplicativo com conteúdo adicionado manualmente ao qual você deseja adicionar arquivos executáveis.

- Na seção **Tipo de regra**, selecione uma das seguintes opções:
  - **Regras para adicionar às inclusões**
  - **Regras para adicionar às exclusões**
- Na seção **Parâmetro usado como condição**, selecione uma das seguintes opções:
  - Detalhes do certificado (ou hashes SHA-256 para arquivos sem certificado)

    Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

    Cada arquivo tem a sua própria função SHA256 hash única. Quando você seleciona uma função SHA256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

    Selecione esta opção se você quiser adicionar às regras de categoria os detalhes do certificado de um arquivo executável (ou a função SHA256 hash de arquivos sem um certificado).

    Por padrão, esta opção está selecionada.

  - Detalhes do certificado (arquivos sem um certificado serão ignorados)

Os arquivos podem ser assinados com um certificado. Múltiplos arquivos podem ser assinados com o mesmo certificado. Por exemplo, as versões diferentes do mesmo aplicativo podem ser assinadas com o mesmo certificado, ou diversos aplicativos diferentes do mesmo fornecedor podem ser assinados com o mesmo certificado. Quando você seleciona um certificado, diversas versões de um aplicativo ou diversos aplicativos do mesmo fornecedor podem terminar na categoria.

Selecione esta opção se você quiser adicionar os detalhes do certificado de um arquivo executável às regras de categoria. Se o arquivo executável não tiver um certificado, este arquivo será ignorado. Nenhuma informação sobre este arquivo será adicionada à categoria.

- **Somente SHA-256 (arquivos sem hash serão ignorados)**

  Cada arquivo tem a sua própria função SHA256 hash única. Quando você seleciona uma função SHA256 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

  Selecione esta opção se você quiser adicionar somente os detalhes da função SHA256 hash do arquivo executável.

- **Somente MD5 (modo descontinuado, somente para a versão Kaspersky Endpoint Security 10 Service Pack 1)**

  Cada arquivo tem a sua própria função MD5 hash única. Quando você seleciona uma função MD5 hash, somente um arquivo correspondente, por exemplo, versão do aplicativo definida, termina na categoria.

  Selecione esta opção se você quiser adicionar somente os detalhes da função MD5 hash do arquivo executável. O cálculo função MD5 hash é suportado por versões do Service Pack 1 do Kaspersky Endpoint Security 10 for Windows e posteriores.

5. Clique em **OK**.

Quando o assistente for concluído, os arquivos executáveis relacionados aos eventos do Controle de Aplicativos serão adicionados à categoria de aplicativos existente ou a uma nova categoria de aplicativos. Você pode visualizar as configurações da categoria de aplicativos que modificou ou criou.

Para obter informações detalhadas sobre o Controle de Aplicativos, consulte os seguintes tópicos da Ajuda:

- Ajuda on-line Kaspersky Endpoint Security for Windows
- Ajuda on-line do Kaspersky Endpoint Security for Linux
- Kaspersky Security for Virtualization Light Agent
- Ajuda do Kaspersky Embedded Systems Security for Windows
- Ajuda do Kaspersky Embedded Systems Security for Linux

Criação de um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky

O Kaspersky Security Center Web Console permite executar a instalação remota de aplicativos de terceiros usando pacotes de instalação. Esses aplicativos de terceiros são incluídos em um banco de dados dedicado da Kaspersky. O banco de dados da Kaspersky é criado automaticamente quando a tarefa *Baixar as atualizações no repositório do Servidor de Administração* for executada pela primeira vez.

Para criar um pacote de instalação de um aplicativo de terceiros a partir do banco de dados da Kaspersky:

1. No menu principal, vá para **Descoberta e implementação** → **Implementação e atribuição** → **Pacotes de instalação**.
2. Clique no botão **Adicionar**.
3. Na página do Assistente de novo pacote aberta, selecione a opção **Selecione um aplicativo no banco de dados da Kaspersky para criar um pacote de instalação** e clique em **Avançar**.
4. Na lista de aplicativos aberta, selecione o aplicativo relevante e clique em **Avançar**.
5. Selecione o idioma de localização relevante na lista suspensa e clique em **Avançar**.

   Esta etapa só será exibida se o aplicativo oferecer várias opções de idioma.

6. Se for solicitado que você aceite um Contrato de Licença para a instalação, na página **Contrato de Licença de Usuário Final** que é aberta, clique no link para ler o Contrato de Licença no site do fornecedor e selecione a caixa de seleção **Confirmo que li, entendi e aceito totalmente os termos e condições deste Contrato de Licença de Usuário Final**.
7. Na página **Nome do novo pacote de instalação** aberta, no campo **Nome do pacote**, digite o nome do pacote de instalação e clique em **Avançar**.

Aguarde até que o pacote de instalação recém-criado seja carregado no Servidor de Administração. Quando o Assistente de novo pacote exibir a mensagem de que o processo de criação do pacote foi realizado com êxito, clique em **Concluir**.

O pacote de instalação recém-criado aparece na lista de pacotes de instalação. Você pode selecionar esse pacote ao criar ou reconfigurar a tarefa *Instalar aplicativo remotamente*.

Ver e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky

Se você já criou algum pacote de instalação de aplicativos de terceiros listados no banco de dados da Kaspersky, poderá visualizar e modificar as configurações desse pacote posteriormente.

A modificação das configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky está disponível apenas para a licença de Gerenciamento de patches e vulnerabilidades.

Para visualizar e modificar as configurações de um pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky:

1. No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Pacotes de instalação**.
2. Na lista de pacotes de instalação aberta, clique no nome do pacote relevante.
3. Na página de propriedades aberta, modifique as configurações, conforme necessário.
4. Clique no botão **Salvar**.

As configurações que você modificou são salvas.

Configurações do pacote de instalação de um aplicativo de terceiros do banco de dados da Kaspersky

As configurações do pacote de instalação de um aplicativo de terceiros são agrupadas nas seguintes guias:

Apenas uma parte das configurações listadas abaixo são exibidas por padrão, então você pode adicionar as colunas correspondentes clicando no botão **Filtro** e selecionando nomes de colunas relevantes da lista.

- Guia **Geral**:
  - Campo de entrada que contém o nome do pacote de instalação que pode ser editado manualmente
  - Aplicativo

    O nome do aplicativo de terceiros para o qual o pacote de instalação foi criado.
  - Versão

    O número da versão do aplicativo de terceiros para o qual o pacote de instalação foi criado.
  - Tamanho

    O tamanho do pacote de instalação de terceiros (em kilobytes).
  - Criação

    A data e hora em que o pacote de instalação de terceiros foi criado.
  - Caminho

    O caminho para a pasta de rede em que o pacote de instalação de terceiros está localizado.
- Guia **Procedimento de instalação**:
  - Instalar os componentes gerais do sistema necessários

    Caso a opção esteja ativada, antes de instalar uma atualização, o aplicativo instala automaticamente todos os componentes gerais do sistema (pré-requisitos) necessários para instalar a atualização. Por exemplo, estes pré-requisitos podem ser atualizações do sistema operacional.

    Se esta opção estiver desativada, talvez você precise instalar os pré-requisitos manualmente.

    Por padrão, esta opção está desativada.
  - Tabela que exibe as propriedades de atualização e contendo as seguintes colunas:
    - Nome

      O nome da atualização.
    - Descrição

      A descrição da atualização.

- **Origem**

  A fonte da atualização, isto é, se foi lançada pela Microsoft ou por outro desenvolvedor terceiro.

- **Tipo**

  O tipo da atualização, ou seja, se é destinada a um driver ou aplicativo.

- **Categoria**

  A categoria WSUS (Windows Server Update Services) exibida para atualizações da Microsoft (atualizações críticas, atualizações de definições, drivers, pacotes de recursos, atualizações de segurança, service packs, ferramentas, pacotes cumulativos de atualizações, atualizações ou upgrades).

- **Nível de importância de acordo com o MSRC**

  O nível de importância da atualização definido pelo Microsoft Security Response Center (MSRC).

- **Nível de importância**

  O nível de importância da atualização definido pela Kaspersky.

- **Nível de importância do patch (para patches destinados aos aplicativos Kaspersky)**

  O nível de importância do patch caso se destine a um aplicativo Kaspersky.

- **Artigo**

  O identificador (ID) do artigo na Base de Conhecimento que descreve a atualização.

- **Boletim**

  O ID do boletim de segurança que descreve a atualização.

- **Não atribuído para a instalação (nova versão)**

  Exibe se a atualização tem o status Não atribuída para instalação.

- **A ser instalado**

  Exibe se a atualização tem o status A ser instalada.

- **Instalando**

  Exibe se a atualização tem o status Instalando.

- **Instalado**

Exibe se a atualização tem o status Instalada.

- **Falhou**

  Exibe se a atualização tem o status Falha.

- **A reinicialização é necessária**

  Exibe se a atualização tem o status Reinicialização necessária.

- **Registrado**

  Exibe a data e a hora em que a atualização foi registrada.

- **Instalado no modo interativo**

  Exibe se a atualização requer interação com o usuário durante a instalação.

- **Revogado**

  Exibe a data e a hora em que a atualização foi revogada.

- **Status de aprovação da atualização**

  Exibe se a atualização está aprovada para instalação.

- **Revisão**

  Exibe o número da revisão atual da atualização.

- **ID de atualização**

  Exibe o ID da atualização.

- **Versão do aplicativo**

  Exibe o número da versão para a qual o aplicativo deve ser atualizado.

- **Substituído**

  Exibe outras atualizações que podem substituir a atualização.

- **Substituição**

  Exibe outras atualizações que podem ser substituídas pela atualização.

- **Você deve aceitar os termos do Contrato de Licença**

Exibe se a atualização requer aceitação dos termos de um Contrato de Licença do Usuário Final (EULA).

- **URL de descrição**

  Exibe o nome do fornecedor da atualização.

- **Família do aplicativo**

  Exibe o nome da família de aplicativos à qual a atualização pertence.

- **Aplicativo**

  Exibe o nome do aplicativo ao qual a atualização pertence.

- **Idioma da localização**

  Exibe o idioma da localização da atualização.

- **Não atribuído para a instalação (nova versão)**

  Exibe se a atualização tem o status Não atribuída para instalação (nova versão).

- **Requer a instalação de pré-requisitos**

  Exibe se a atualização tem o status de instalação Requer pré-requisitos.

- **Modo de download**

  Exibe o modo de download da atualização.

- **É um patch**

  Exibe se a atualização é um patch.

- **Não instalado**

  Exibe se a atualização tem o status Não instalada.

- Guia **Configurações** que exibe as configurações do pacote de instalação, com seus nomes, descrições e valores usados como parâmetros de linha de comando durante a instalação. Se o pacote não fornecer estas configurações, a mensagem correspondente será exibida. Você pode modificar os valores destas configurações.

- Guia **Histórico de revisões** que exibe as revisões do pacote de instalação e contém as seguintes colunas:

  - **Revisão** - O número da revisão dos pacotes de instalação.

  - **Hora** - Data e hora em que as configurações do pacote de instalação foram modificadas.

  - **Usuário** - Nome do usuário que modificou as configurações do pacote de instalação.

  - **Ação** - Ação executada no pacote de instalação dentro da revisão.

  - **Descrição** - Descrição da revisão relacionada à alteração feita nas configurações do pacote de instalação.

    Por padrão, a descrição da revisão fica em branco. Para adicionar uma descrição a uma revisão, selecione a revisão relevante e clique no botão **Editar descrição**. Na janela aberta, insira algum texto para a descrição da revisão.

Tags de aplicativo

O Kaspersky Security Center permite marcar os aplicativos pelo registro de aplicativos. Uma tag é o rótulo de um aplicativo que pode ser usada para agrupar ou encontrar dispositivos. Uma tag destinada a aplicativos pode servir como uma condição em seleções de dispositivos.

Por exemplo, você pode criar a tag `[Browsers]` e atribuí-la a todos os navegadores, como Microsoft Internet Explorer, Google Chrome, Mozilla Firefox etc.

Criando uma tag de aplicativo

Para criar um tag de aplicativo:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Tags de aplicativos**.

2. Clique em **Adicionar**.

   Uma nova janela de tag é exibida.

3. Insira o nome da tag.

4. Clique em **OK** para salvar as alterações.

A nova tag aparece na lista de tags de aplicativos.

Renomeando uma tag de aplicativo

Para renomear um identificador de aplicativos:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Tags de aplicativos**.
2. Marque a caixa de seleção ao lado do identificador que deseja renomear e clique em **Editar**.

   A janela de propriedades do identificador é exibida.
3. Altere o nome do identificador.
4. Clique em **OK** para salvar as alterações.

A tag atualizado aparece na lista de tags de aplicativos.

Atribuindo uma tag de aplicativos

Para atribuir uma ou várias tags a um aplicativo:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Registro de aplicativos**.
2. Clique no nome do aplicativo ao qual deseja atribuir tags.
3. Selecione a guia **Tags**.

   A guia exibe todos as tags de aplicativos existentes no Servidor de Administração. Para tags atribuídas ao aplicativo selecionado, a caixa de seleção na coluna **Tag atribuída** é selecionada.
4. Para as tags que deseja atribuir, marque as caixas de seleção na coluna **Tag atribuída**.
5. Clique em **Salvar** para salvar as alterações.

As tags são atribuídas ao aplicativo.

Removendo tags atribuídas de um aplicativo

Para remover uma ou várias tags de um aplicativo:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Registro de aplicativos**.
2. Clique no nome do aplicativo do qual deseja remover tags.
3. Selecione a guia **Tags**.

   A guia exibe todos as tags de aplicativos existentes no Servidor de Administração. Para tags atribuídas ao aplicativo selecionado, a caixa de seleção na coluna **Tag atribuída** é selecionada.

4. Para tags que deseja remover, desmarque as caixas de seleção na coluna **Tag atribuída**.

5. Clique em **Salvar** para salvar as alterações.

As tags são removidas do dispositivo.

As tags de aplicativos removidas não são excluídas. Se quiser, você pode excluí-los manualmente.

Excluir uma tag de aplicativos

Para excluir um identificador de aplicativos:

1. No menu principal, vá para **Operações → Aplicativos de terceiros → Tags de aplicativos**.

2. Na lista, selecione o identificador de aplicativos que deseja excluir.

3. Clique no botão **Excluir**.

4. Na janela que se abre, clique em **OK**.

O identificador de aplicativos é excluído. O identificador excluído é automaticamente removido de todos dos aplicativos aos quais foi atribuído.

Monitoramento e relatórios

Esta seção descreve os recursos de monitoramento e emissão de relatórios no Kaspersky Security Center. Esses recursos fornecem a você uma visão geral da infraestrutura, dos status de proteção e das estatísticas.

Após a implementação do Kaspersky Security Center ou durante a operação, você pode configurar os recursos de monitoramento e emissão de relatórios de forma a melhor atender às suas necessidades.

Cenário: Monitoramento e relatórios

Esta seção fornece um cenário para a configuração do recurso de monitoramento e de relatórios no Kaspersky Security Center.

Pré-requisitos

Após ter implementado o Kaspersky Security Center na rede de uma organização, você poderá iniciar o seu monitoramento e gerar relatórios sobre o seu funcionamento.

O monitoramento e relatórios em na rede de uma organização prossegue em estágios:

1. **Configurar a alternância dos status do dispositivo**

Conheça as configurações para os status do dispositivo dependendo de condições específicas. Modificando essas configurações, você pode alterar o número de eventos com os níveis de importância *Crítico* ou *Advertência*. Ao configurar a alternância dos status do dispositivo, esteja seguro do seguinte:

- As novas configurações não entram em conflito com as políticas de segurança de informações da sua organização.
- Você pode reagir a eventos de segurança importantes na rede da sua organização de maneira oportuna.

2. **Configurar as notificações de eventos em dispositivos clientes**

   Instruções de como proceder:

   Configure a notificação (por e-mail, SMS ou executando um arquivo executável) de eventos em dispositivos cliente

3. **Alteração da resposta da sua rede de segurança para o evento de Surto de vírus**

   Você pode alterar os limites específicos nas propriedades do Servidor de Administração. Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.

4. **Execução das ações recomendadas para as notificações Crítico e Advertência**

   Instruções de como proceder:

   Execute as ações recomendadas para a rede da sua organização

5. **Análise do status de segurança da rede da sua organização**

   Instruções de como proceder:

   - Revise o widget Status da proteção
   - Gere e revise o Relatório do status da proteção
   - Gere e revise o Relatório de erros

6. **Localize dispositivos clientes que não estão protegidos**

   Instruções de como proceder:

   - Revise o widget Novos dispositivos
   - Gere e revise o Relatório de implementação de proteção

7. **Verificação da proteção de dispositivos clientes**

   Instruções de como proceder:

   - Gere e revise os relatórios das categorias Status da proteção e Estatísticas de ameaças
   - Inicie e analise a seleção de eventos de Crítico

8. **Avaliação e limitação da carga de eventos no banco de dados**

   As informações sobre eventos que ocorrem durante a operação de aplicativos gerenciados são transferidas a partir de um dispositivo cliente e registradas no banco de dados do Servidor de Administração. Para reduzir a carga do Servidor de Administração, avalie e limite o número máximo de eventos que podem ser armazenados no banco de dados.

   Instruções de como proceder:

- Cálculo do espaço do banco de dados
- Limitação do número máximo de eventos

9. **Análise de informações de licença**

   Instruções de como proceder:

   - Adicione o widget de Uso de chaves de licença ao painel e o analise
   - Gere e revise o Relatório de uso das chaves de licença

Resultados

Após a conclusão do cenário, você é informado sobre a proteção da rede da sua organização e, portanto, poderá planejar ações para proteção adicional.

Sobre os tipos do monitoramento e relatórios

As informações sobre eventos de segurança na rede de uma organização são armazenadas no banco de dados do Servidor de Administração. Com base nos eventos, o Kaspersky Security Center Web Console fornece os seguintes tipos de monitoramento e relatórios na rede da sua organização:

- Painel
- Relatórios
- Seleções de eventos
- Notificações

Painel

O painel permite monitorar tendências de segurança na rede da sua organização fornecendo uma exibição gráfica das informações.

Relatórios

O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las.

Seleções de eventos

As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. Esses conjuntos de eventos são agrupados de acordo com as seguintes categorias:

- Por nível de importância – **Eventos críticos**, **Falhas funcionais**, **Advertências** e **Eventos de informações**
- Por tempo – **Eventos recentes**

- Por tipo – **Pedidos de usuário** e **Eventos de auditoria**

Você pode criar e visualizar seleções de eventos definidas pelos usuários baseado nas configurações disponíveis para configuração na interface do Kaspersky Security Center Web Console.

Notificações

As Notificações alertam sobre os eventos e ajudam a agilizar as respostas a estes eventos executando ações recomendadas ou ações que você considera apropriadas.

Painel e widgets

Esta seção contém informações sobre o painel e os widgets que o painel fornece. A seção inclui instruções sobre como gerenciar e definir as configurações dos widgets.

Usar o painel

O painel permite monitorar tendências de segurança na rede da sua organização fornecendo uma exibição gráfica das informações.

O painel está disponível no Kaspersky Security Center Web Console, na seção **Monitoramento e relatórios**, clicando em **Painel**.

O painel fornece widgets que podem ser personalizados. Você pode selecionar um grande número de widgets diferentes, apresentadas como gráficos de pizza ou gráficos de rosca, tabelas, gráficos, gráficos de barras e listas. As informações exibidas nos widgets são atualizadas automaticamente em um intervalo de dois minutos. O intervalo entre atualizações varia para widgets diferentes. Você pode atualizar dados sobre um widget manualmente a qualquer momento por meio do menu de configurações.

Por padrão, os widgets contém informações sobre todos os eventos armazenados no banco de dados do Servidor de Administração.

O Kaspersky Security Center Web Console tem um conjunto padrão de widgets para as seguintes categorias:

- **Status da proteção**
- **Implementação**
- **Atualizando**
- **Estatísticas de ameaças**
- **Outro**

Alguns widgets têm informações de texto com links. Você pode exibir informações detalhadas clicando em um link.

Ao configurar o painel, você pode adicionar os widgets de que precisa, ocultar widgets de que não precisa, modificar o tamanho ou a aparência de widgets, mover widgets e modificar suas configurações.

Adição de widgets ao painel

Para adicionar widgets ao painel:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no botão **Adicionar ou restaurar widget da Web**.
3. Na lista de widgets disponíveis, selecione os widgets que deseja adicionar ao painel.

   Os widgets são agrupados por categoria. Para visualizar a lista de widgets incluídos em uma categoria, clique no ícone de insígnia (>) ao lado do nome da categoria.
4. Clique no botão **Adicionar**.

Os widgets selecionados são adicionados no final do painel.

Você pode editar agora a representação e os parâmetros dos widgets adicionados.

Ocultação de um widget do painel

Para ocultar um widget exibido do painel:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja ocultar.
3. Selecione **Ocultar widget da Web**.
4. Na janela **Advertência** que se abre, clique em **OK**.

O widget selecionado fica oculto. Depois, você pode adicionar esse widget ao painel novamente.

Movimentação de um widget no painel

Para mover um widget no painel:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja mover.
3. Selecione **Migrar**.
4. Clique no lugar para o qual deseja mover o widget. Você pode selecionar apenas outro widget.

Os lugares dos widgets selecionados são trocados.

Alteração do tamanho ou da aparência do widget

Para widgets que exibem um gráfico, você pode alterar sua representação: um gráfico de barras ou um gráfico de linhas. Para alguns widgets, você pode alterar seu tamanho: compacto, médio ou máximo.

Para alterar a representação do widget:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja editar.
3. Execute uma das seguintes ações:
   - Para exibir o widget como um gráfico de barras, selecione **Tipo de gráfico: barras**.
   - Para exibir o widget como um gráfico de linhas, selecione **Tipo de gráfico: linhas**.
   - Para alterar a área ocupada pelo widget, selecione um dos valores:
     - **Compacto**
     - **Compacto (somente barra)**
     - **Médio (gráfico de rosca)**
     - **Médio (gráfico de barras)**
     - **Máximo**

A representação do widget selecionado é alterada.

Alteração das configurações do widget

Para alterar as configurações de um widget:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja alterar.
3. Selecione **Mostrar configurações**.
4. Na janela de configurações de widget exibida, modifique as configurações de widget conforme necessário.
5. Clique em **Salvar** para salvar as alterações.

As configurações do widget selecionado são alteradas.

O conjunto de configurações depende do widget específico. Abaixo estão algumas configurações comuns:

- **Escopo do widget da Web** (o conjunto de objetos para os quais o widget exibe informações): por exemplo, um grupo de administração ou uma seleção de dispositivos.
- **Selecionar tarefa** (a tarefa para a qual o widget exibe informações).
- **Intervalo de tempo** (o intervalo de tempo durante o qual as informações são exibidas no widget): entre as duas datas especificadas; desde a data especificada até o dia atual; ou do dia atual menos o número especificado de dias até o dia atual.
- **Se especificados, definir como Crítico** e **Se especificados, definir como Advertência** (as regras que determinam a cor de um semáforo).

Depois de alterar as configurações do widget, você pode atualizar os dados manualmente.

Para atualizar dados e um widget:

1. No menu principal, vá para **Monitoramento e relatórios** → **Painel**.
2. Clique no ícone de configurações (⚙) ao lado do widget que deseja mover.
3. Selecione **Atualizar**.

Os dados no widget são atualizados.

Sobre o modo somente painel

É possível configurar o modo somente painel para funcionários que não gerenciam a rede, mas que desejam visualizar as estatísticas de proteção da rede no Kaspersky Security Center (por exemplo, um gerente superior). Quando um usuário tem esse modo ativado, apenas um painel com um conjunto predefinido de widgets é exibido para o usuário. Assim, ele pode monitorar as estatísticas especificadas nos widgets, por exemplo, o status de proteção de todos os dispositivos gerenciados, o número de ameaças detectadas recentemente ou a lista das ameaças mais frequentes na rede.

Quando um usuário trabalha no modo somente painel, as seguintes restrições são aplicadas:

- O menu principal não é exibido para o usuário, portanto, ele não pode alterar as configurações de proteção de rede.
- O usuário não pode realizar nenhuma ação com widgets, por exemplo, adicioná-los ou ocultá-los. Portanto, não é necessário colocar todos os widgets requeridos para o usuário no painel e configurá-los, por exemplo, para definir a regra de contagem de objetos ou especificar o intervalo de tempo.

Não é possível atribuir o modo somente painel a si mesmo. Caso queira trabalhar nesse modo, entre em contato com um administrador do sistema, o Provedor de Serviços Gerenciados (MSP) ou um usuário com o direito **Modificar ACLs de objetos** na área funcional **Recursos gerais: Permissões do usuário**.

Configurando o modo somente painel

Antes de iniciar a configuração do Modo somente painel, verifique se os seguintes pré-requisitos foram atendidos:

- O usuário tem o direito de **Modificar ACLs de objetos** na área funcional **Recursos gerais: permissões do usuário**. Caso não tenha esse direito, a guia para configurar o modo estará ausente.
- O usuário tem o direito de **Leitura** na área funcional **Recursos gerais: funcionalidade básica**.

Caso uma hierarquia de Servidores de Administração esteja organizada em sua rede, para configurar o modo somente Painel, acesse o servidor onde a conta de usuário está disponível na seção **Usuários e funções → Usuários**. Pode ser um servidor principal ou um servidor secundário físico. Não é possível ajustar o modo em um servidor virtual.

Para configurar o modo somente painel:

1. No menu principal, vá para **Usuários e funções → Usuários**.
2. Clique no nome da conta de usuário para a qual deseja ajustar o painel com widgets.
3. Na janela aberta de configurações do usuário, selecione a guia **Painel**.

   Na guia aberta, o mesmo painel é exibido para você e para o usuário.
4. Caso o **modo Exibir o console no modo somente painel** estiver habilitado, alterne o botão de alternância para desativá-la.

   Quando essa opção está habilitada, também não será possível alterar o painel. Depois de desativar a opção, será possível gerenciar widgets.
5. Configure a aparência do painel. O conjunto de widgets preparados na guia **Painel** está disponível para o usuário com a conta personalizável. Ele ou ela não pode alterar nenhuma configuração ou tamanho dos widgets, adicionar ou remover quaisquer widgets do painel. Portanto, ajuste-os para o usuário, para que ele possa visualizar as estatísticas de proteção da rede. Para isso, na guia **Painel** é possível executar as mesmas ações com widgets como na seção **Monitoramento e relatórios → Painel**:
   - Adicionar novos widgets ao painel.
   - Ocultar widgets que o usuário não precisa.
   - Mover widgets em uma ordem específica.
   - Alterar o tamanho ou a aparência de widgets.
   - Alterar as configurações do widget.
6. Alterne o botão de alternância para habilitar a opção **Exibir o console no modo somente painel**.

   Depois disso, apenas o painel ficará disponível para o usuário. Ele ou ela pode monitorar as estatísticas, mas não pode alterar as configurações de proteção de rede e a aparência do painel. Como o mesmo painel é exibido para você e para o usuário, você também não pode alterar o painel.

   Caso mantenha a opção desativada, o menu principal será exibido ao usuário, para que ele possa realizar várias ações no Kaspersky Security Center, inclusive alterar as configurações de segurança e os widgets.

7. Clique no botão **Salvar** quando terminar de configurar o modo somente painel. Somente depois disso o dashboard preparado será exibido ao usuário.

8. Caso o usuário queira visualizar as estatísticas de aplicativos Kaspersky compatíveis e precisar de direitos de acesso para isso, configure os direitos para o usuário. Depois disso, os dados dos aplicativos Kaspersky são exibidos para o usuário nos widgets desses aplicativos.

Agora, o usuário pode fazer login no Kaspersky Security Center com a conta personalizada e monitorar as estatísticas de proteção de rede no modo somente painel.

Relatórios

Esta seção descreve como usar relatórios, gerenciar modelos de relatórios personalizados, usar modelos de relatórios para gerar novos relatórios e criar tarefas de entrega de relatórios.

Usar os relatórios

O recurso Relatórios permite obter informações numéricas detalhadas sobre a segurança da rede da sua organização, salvar essas informações em um arquivo, enviá-las por e-mail e imprimi-las.

Os relatórios estão disponíveis no Kaspersky Security Center Web Console, na seção **Monitoramento e relatórios**, clicando em **Relatórios**.

Por padrão, os relatórios contém informações dos últimos 30 dias.

O Kaspersky Security Center tem um conjunto padrão de relatórios para as seguintes categorias:

- **Status da proteção**
- **Implementação**
- **Atualizando**
- **Estatísticas de ameaças**
- **Outro**

Você pode criar modelos de relatório personalizados, editar modelos de relatório e excluí-los.

Você pode criar relatórios que são baseados em modelos existentes, exportar relatórios para arquivos e criar tarefas para entrega de relatório.

Criação de um modelo de relatório

Para criar um modelo de relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. Clique em **Adicionar**.

   O assistente de novo modelo de relatório é iniciado. Prossiga pelo assistente usando o botão **Avançar**.
3. Insira o nome e selecione o tipo de relatório.
4. Na etapa **Escopo** do assistente, selecione o conjunto de dispositivos clientes (grupo de administração, seleção de dispositivos, dispositivos selecionados ou todos os dispositivos em rede) cujos dados serão exibidos em relatórios que são baseados nesse modelo de relatório.
5. Na etapa **Período do relatório** do assistente, especifique o período de relatório. Os valores disponíveis são:

   - Entre as duas datas especificadas
   - A partir da data especificada até à data de criação do relatório
   - Desde a data de criação do relatório menos o número especificado de dias, até a data de criação do relatório

   Essa página pode não aparecer para alguns relatórios.
6. Clique em **OK** para fechar o assistente.
7. Execute uma das seguintes ações:

   - Clique no botão **Salvar e executar** para salvar o novo modelo de relatório e executar um relatório baseado nele.

     O modelo de relatório é salvo. O relatório é gerado.
   - Clique no botão **Salvar** para salvar o novo modelo de relatório.

     O modelo de relatório é salvo.

Você pode usar o novo modelo para gerar e visualizar relatórios.

Visualização e edição das propriedades do modelo de relatório

Você pode visualizar e editar propriedades básicas de um modelo de relatório como, por exemplo, o nome do modelo de relatório ou os campos exibidos no relatório.

Para visualizar e editar propriedades de um modelo de relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. Marque a caixa de seleção ao lado do modelo de relatório cujas propriedades deseja visualizar e editar.

   Como uma alternativa, você pode primeiro gerar o relatório e depois clicar no botão **Editar**.

3. Clique no botão **Abrir propriedades do modelo de relatório**.

   A janela **Edição de relatório <Nome do relatório>** é exibida com a guia **Geral** selecionada.

4. Edite as propriedades do modelo de relatório:

- Guia **Geral**:
  - Nome do modelo de relatório
  - Número máximo de entradas a exibir

    Se esta opção estiver ativada, o número de entradas exibidas na tabela com dados de relatório detalhados não será maior que o valor especificado.

    As entradas de relatório são primeiro classificadas segundo as regras especificadas na seção **Campos → Campos de detalhes** das propriedades do modelo de relatório e, em seguida, apenas a primeira das entradas resultantes é mantida. O cabeçalho da tabela com dados de relatório detalhados mostra o número de entradas exibidas e o número total de entradas disponíveis que combinam com outras configurações do modelo de relatório.

    Se esta opção estiver desativada, a tabela com dados de relatório detalhados exibe todas as entradas disponíveis. Não recomendamos que você desative essa opção. Limitar o número de entradas de relatório exibidas reduz a carga do sistema de gerenciamento de banco de dados (DBMS) e reduz o tempo necessário para gerar e exportar o relatório. Alguns dos relatórios contêm entradas excessivas. Se este for o caso, você pode ter dificuldade para ler e analisar todas elas. Além disso, o seu dispositivo pode ficar sem memória ao gerar um relatório e, consequentemente, você não poderá exibir o relatório.

    Por padrão, esta opção está ativada. O valor predefinido é de 1.000.

  - **Grupo**

    Clique no botão **Configurações** para alterar o conjunto de dispositivos clientes para os quais o relatório é criado. Para alguns tipos dos relatórios, o botão pode estar indisponível. As configurações reais dependem das configurações especificadas durante a criação do modelo de relatório.

  - **Intervalo de tempo**

    Clique no botão **Configurações** para modificar o período de relatório. Para alguns tipos dos relatórios, o botão pode estar indisponível. Os valores disponíveis são:

    - Entre as duas datas especificadas
    - A partir da data especificada até à data de criação do relatório
    - Desde a data de criação do relatório menos o número especificado de dias, até a data de criação do relatório

  - Incluir dados dos Servidores de Administração secundários e virtuais

    Se esta opção estiver ativada, o relatório inclui as informações dos Servidores de Administração secundário e virtual subordinados ao Servidor de Administração para o qual o modelo de relatório é criado.

    Desative esta opção se você quiser visualizar dados somente do Servidor de Administração atual.

    Por padrão, esta opção está ativada.

  - Até o nível de aninhamento

O relatório inclui dados de servidores de administração secundários e virtuais localizados sob o Servidor de administração atual a um nível de agrupamento menor ou igual ao valor especificado.

O valor padrão é 1. Convém alterar esse valor caso necessite recuperar as informações dos Servidores de administração secundários localizados em níveis mais baixos na árvore.

- Intervalo de espera dos dados (min.)

  Antes de gerar o relatório, o Servidor de administração para o qual o modelo de relatório é criado aguarda pelos dados de Servidores de administração secundários durante o número de minutos especificado. Se nenhum dado for recebido de um Servidor de administração secundário ao fim desse período, o relatório é executado mesmo assim. Em vez de dados reais, o relatório exibe os dados retirados do cache (se a opção **Dados em cache dos Servidores de Administração secundários** estiver ativada) ou, caso contrário, **N/A** (não acessível).

  O valor predefinido é de 5 (minutos).

- Dados em cache dos Servidores de Administração secundários

  Os Servidores de Administração secundários regularmente transferem dados para o Servidor de Administração para o qual o modelo de relatório é criado. Nesse local, os dados transferidos são armazenados em cache.

  Se o Servidor de administração atual não puder receber dados de um Servidor de administração secundário enquanto o relatório estiver sendo gerado, o relatório exibirá dados retirados do cache. A data em que os dados foram transferidos para o cache também é exibida.

  Ativar essa opção permite a visualização das informações dos Servidores de administração secundários, mesmo se os dados atualizados não puderem ser recuperados. Entretanto, os dados exibidos podem ser obsoletos.

  Por padrão, esta opção está desativada.

- Frequência de atualização de cache (h)

  Os Servidores de administração secundários regularmente transferem dados para o Servidor de administração para o qual o modelo de relatório é criado. É possível especificar o período em horas. Se o valor for 0, os dados serão transferidos somente quando o relatório for gerado.

  O valor padrão é 0.

- Transferir informações detalhadas dos Servidores de Administração secundários

  No relatório gerado, a tabela contendo dados de relatório detalhados inclui dados dos Servidores de Administração secundários do Servidor de Administração para o qual o modelo de relatório é criado.

  Ativar esta opção reduz a velocidade de geração de relatórios e aumenta o tráfego entre Servidores de Administração. Entretanto, você pode visualizar todos os dados em um relatório.

  Em vez de ativar a opção, convém analisar dados de relatório detalhados para detectar um Servidor de administração secundário defeituoso e, em seguida, gerar o mesmo relatório apenas para o Servidor de administração defeituoso.

  Por padrão, esta opção está desativada.

- Guia **Campos**

Selecione os campos que serão exibidos no relatório e use os botões **Para cima** e **Para baixo** para alterar a ordem desses campos. Use o botão **Adicionar** ou **Editar** para especificar se as informações no relatório devem ser classificadas e filtradas segundo cada um dos campos.

Na seção **Filtros dos campos Detalhes**, você também pode clicar em **Converter filtros** para começar a usar o formato de filtragem estendido. Este formato permite combinar as condições de filtragem especificadas em vários campos, usando a operação lógica OR. Depois de clicar no botão, o painel **Converter filtros** abre à direita. Clique no botão **Converter filtros** para confirmar a conversão. Agora, você pode definir um filtro convertido com as condições da seção **Campos de detalhes**, que são aplicadas usando a operação lógica OR.

> A conversão de um relatório para o formato compatível com as condições de filtragem complexas tornará o relatório incompatível com as versões anteriores do Kaspersky Security Center (11 e anteriores). Além disso, o relatório convertido não conterá nenhum dado dos Servidores de Administração secundários executando tais versões incompatíveis.

5. Clique em **Salvar** para salvar as alterações.
6. Feche a janela **Editar relatório <Nome do relatório>**.

O modelo de relatório atualizado aparece na lista de modelos de relatório.

Exportar um relatório para um arquivo

Você pode exportar um relatório para um arquivo XML, HTML ou PDF.

Para exportar um relatório para um arquivo:

1. No menu principal, vá para **Monitoramento e relatórios → Relatórios**.
2. Marque a caixa de seleção ao lado do relatório que deseja exportar para um arquivo.
3. Clique no botão **Exportar relatório**.
4. Na janela exibida, altere o nome do arquivo de relatório no campo **Nome**. Por padrão, o nome do arquivo coincide com o nome do modelo de relatório selecionado.
5. Selecione o tipo de arquivo de relatório: XML, HTML ou PDF.
6. Clique no botão **Exportar relatório**.

   O relatório no formato selecionado será baixado para o seu dispositivo (para a pasta padrão do seu dispositivo), ou uma janela padrão **Salvar como** será exibida no navegador para permitir que você salve o arquivo onde quiser.

O relatório é salvo no arquivo.

Como gerar e visualizar um relatório

Para criar e visualizar um relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. Clique no nome do modelo de relatório que deseja usar para criar um relatório.

   Um relatório usando o modelo selecionado é gerado e exibido.

Os dados do relatório são exibidos de acordo com a localização definida para o Servidor de Administração.

O relatório exibe os seguintes dados:

- Na guia **Resumo**:
  - O nome e tipo de relatórios, uma breve descrição e o período de relatórios, assim como as informações sobre o grupo de dispositivos para os quais o relatório é gerado.
  - Gráfico que mostra os dados do relatório mais representativos.
  - Tabela consolidada com os indicadores do relatório calculados.
- Na guia **Detalhes**, uma tabela com dados detalhados do relatório é exibida.

Criação de uma tarefa de entrega de relatório

Você pode criar uma tarefa que entregará os relatórios selecionados.

Para criar uma tarefa de entrega de um relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.
2. [Opcional] Marque as caixas de seleção ao lado dos modelos de relatório para os quais deseja criar uma tarefa de entrega de relatório.
3. Clique no botão **Nova tarefa de entrega de relatórios**.
4. O Assistente para novas tarefas inicia. Prossiga pelo assistente usando o botão **Avançar**.
5. Na primeira página do assistente, digite o nome da tarefa. O nome padrão é **Entregar relatórios (<N>)**, em que <N> é o número de sequência da tarefa.

6. Na página de configurações da tarefa do assistente, especifique as seguintes configurações:

    a. Modelos de relatório a serem entregues pela tarefa. Caso os tenha selecionado na etapa 2, ignore esta etapa.

    b. O formato do relatório: HTML, XLS ou PDF.

    c. Se os relatórios precisarem ser enviados por e-mail, em conjunto com as configurações de notificação por e-mail.

    d. Se os relatórios precisarem ser salvos em uma pasta, se os relatórios anteriormente salvos nessa pasta precisarem ser sobrescrito e se uma conta específica precisar ser usada para acessar a pasta (para uma pasta compartilhada).

7. Se você deseja modificar outras configurações de tarefa após a criação da tarefa, na página **Concluir a criação da tarefa** do assistente, habilite a opção **Abrir detalhes da tarefa quando a criação for concluída**.

8. Clique no botão **Criar** para criar a tarefa e fechar o assistente.

    A tarefa de entrega de relatório é criada. Se você ativou a opção **Abrir detalhes da tarefa quando a criação for concluída**, a janela de configurações da tarefa é aberta.

Excluir os modelos de relatório

Para excluir um ou vários modelos de relatório:

1. No menu principal, vá para **Monitoramento e relatórios** → **Relatórios**.

2. Marque as caixas de seleção ao lado dos modelos de relatório que deseja excluir.

3. Clique no botão **Excluir**.

4. Na janela que se abre, clique em **OK** para confirmar a sua seleção.

Os modelos de relatório selecionados são excluídos. Se esses modelos de relatório tiverem sido incluídos nas tarefas de entrega de relatório, eles também serão removidos das tarefas.

Eventos e seleções de eventos

Esta seção fornece informações sobre eventos e seleções de eventos, sobre os tipos de eventos que ocorrem nos componentes do Kaspersky Security Center e sobre como gerenciar o bloqueio de eventos frequentes.

Sobre os eventos do Kaspersky Security Center

O Kaspersky Security Center lhe permite receber informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nestes dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração.

Tipos de eventos

No Kaspersky Security Center, há os seguintes tipos de eventos:

- Eventos gerais. Esses eventos ocorrem em todos os aplicativos Kaspersky gerenciados. Um exemplo de um evento geral é um Surto de vírus. Eventos gerais têm sintaxe e semântica estritamente definidas. Eventos gerais são usados, por exemplo, em relatórios e painéis.
- Eventos gerenciados específicos de aplicativos Kaspersky. Cada aplicativo Kaspersky gerenciado tem o seu próprio conjunto de eventos.

Fontes de eventos

Os eventos podem ser gerados pelos seguintes aplicativos:

- Componentes do Kaspersky Security Center:
  - Servidor de Administração
  - Agente de Rede
  - Servidor MDM do iOS
  - Servidor de dispositivos móveis Exchange
- Aplicativos gerenciados pela Kaspersky

  Para obter detalhes sobre os eventos gerados pelos aplicativos gerenciados pela Kaspersky, consulte a documentação do aplicativo correspondente.

É possível visualizar a lista completa dos eventos que podem ser gerados por um aplicativo na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar a lista de eventos nas propriedades do Servidor de Administração.

Nível de importância dos eventos

Cada evento tem o seu próprio nível de importância. Dependendo das condições da sua ocorrência, a um evento pode ser atribuídos diversos níveis de importância. Há quatro níveis de importância de eventos:

- Um *evento crítico* é um evento que indica a ocorrência de um problema crítico que pode levar à perda de dados, um funcionamento operacional ruim ou um erro crítico.
- Uma *falha funcional* é um evento que indica a ocorrência de um problema sério, erro ou funcionamento incorreto que ocorreu durante a operação do aplicativo ou ao executar um procedimento.
- Um *aviso* é um evento que não necessariamente é sério, mas no entanto indica um problema potencial no futuro. A maior parte de eventos são indicados como avisos se o aplicativo puder ser restaurado sem perda dos dados ou capacidades funcionais após a ocorrência de tais eventos.
- Um evento *de informação* é um evento que ocorre para fins de informar sobre conclusão bem sucedida de uma operação, funcionamento apropriado do aplicativo ou conclusão de um procedimento.

Cada evento tem um prazo de armazenamento definido, durante o qual você pode exibi-lo ou modificá-lo no Kaspersky Security Center. Alguns eventos não são salvos no banco de dados do Servidor de Administração por padrão porque o seu prazo de armazenamento definido é zero. Somente os eventos que serão armazenados no banco de dados do Servidor de Administração por ao menos um dia podem ser exportados aos sistemas externos.

Usar as seleções de eventos

As seleções de evento fornecem uma visualização na tela de conjuntos nomeados de eventos selecionados do banco de dados do Servidor de Administração. Esses conjuntos de eventos são agrupados de acordo com as seguintes categorias:

- Por nível de importância – **Eventos críticos**, **Falhas funcionais**, **Advertências** e **Eventos de informações**
- Por tempo – **Eventos recentes**
- Por tipo – **Pedidos de usuário** e **Eventos de auditoria**

Você pode criar e visualizar seleções de eventos definidas pelos usuários baseado nas configurações disponíveis para configuração na interface do Kaspersky Security Center Web Console.

As seleções de eventos estão disponíveis no Kaspersky Security Center Web Console, na seção **Monitoramento e relatórios**, clicando em **Seleções de eventos**.

Por padrão, as seleções de eventos incluem informações dos últimos sete dias.

O Kaspersky Security Center tem um conjunto padrão de seleções de eventos (predefinidas):

- Eventos com níveis de importância diferentes:
  - **Eventos críticos**
  - **Falhas funcionais**
  - **Advertências**
  - **Eventos informativos**
- **Solicitações de usuário** (eventos de aplicativos gerenciados)
- **Eventos recentes** (na semana passada)
- Eventos de auditoria.

Também é possível criar e configurar seleções adicionais definidas pelo usuário. Em seleções definidas pelos usuários, é possível filtrar eventos pelas propriedades dos dispositivos dos quais se originaram (nomes de dispositivos, conjuntos de IPs e grupos de administração), por tipos de evento e níveis de gravidade, por aplicativo e nome do componente e por intervalo de tempo. Também é possível incluir resultados da tarefa no escopo de pesquisa. Você também pode usar um campo de pesquisa simples em que uma palavra ou várias palavras podem ser digitadas. São exibidos todos os eventos que contêm alguma das palavras digitadas em qualquer lugar nos seus atributos (como nome do evento, descrição, nome do componente).

Para seleções predefinidas e definidas pelos usuários, você pode limitar o número de eventos exibidos ou o número de registros para pesquisar. Ambas as opções afetam o tempo necessário para o Kaspersky Security Center exibir os eventos. Quanto maior for o banco de dados, mais demorado será o processo.

Você pode fazer o seguinte:

- Editar propriedades das seleções de eventos
- Gerar seleções de eventos
- Visualizar detalhes das seleções de eventos
- Excluir seleções de eventos
- Excluir eventos do banco de dados do Servidor de Administração

Criar uma seleção de eventos

Para criar uma seleção de eventos:

1. No menu principal, vá para **Monitoramento e relatórios** → **Seleções de eventos**.
2. Clique em **Adicionar**.
3. Na janela **Nova seleção de eventos** que se abre, especifique as configurações da nova seleção de eventos. Faça isso em uma ou mais das seções na janela.
4. Clique em **Salvar** para salvar as alterações.

   A janela de confirmação é exibida.
5. Para visualizar o resultado da seleção de eventos, mantenha a caixa de seleção **Ir para o resultado da seleção** selecionada.
6. Clique em **Salvar** para confirmar a criação da seleção de eventos.

Se você tiver mantido a caixa de seleção **Ir para o resultado da seleção** selecionada, o resultado da seleção de eventos será exibido. Caso contrário, a nova seleção de eventos será exibida na lista de seleção de eventos.

Editar uma seleção de eventos

Para editar uma seleção de eventos:

1. No menu principal, acesse **Monitoramento e relatórios** → **Seleções de eventos**.
2. Marque a caixa de seleção ao lado da seleção de eventos que deseja editar.
3. Clique no botão **Propriedades**.

   Uma janela de configurações de seleção de eventos é aberta.

4. Edite as propriedades da seleção de eventos.

> Para seleções de eventos predefinidas, você pode editar somente as propriedades nas seguintes guias: **Geral** (exceto o nome de seleção), **Hora** e **Direitos de acesso**.

Para seleções definidas pelos usuários, você pode editar todas as propriedades.

5. Clique em **Salvar** para salvar as alterações.

A seleção de eventos editada é mostrada na lista.

Visualizando uma lista de uma seleção de eventos

Para visualizar a seleção de eventos:

1. No menu principal, acesse **Monitoramento e relatórios → Seleções de eventos**.
2. Marque a caixa de seleção ao lado da seleção de eventos que deseja iniciar.
3. Execute uma das seguintes ações:
   - Se você quiser configurar a classificação no resultado da seleção de eventos, faça o seguinte:
     a. Clique no botão **Reconfigurar classificação e iniciar**.
     b. Na janela exibida **Reconfigurar classificação para seleção de eventos**, especifique as configurações de classificação.
     c. Clique no nome da seleção.
   - Caso contrário, se você quiser visualizar a lista de eventos e como eles estão classificados no Servidor de Administração, clique no nome da seleção.

O resultado da seleção de eventos é exibido.

Excluir as seleções de eventos

> Você pode excluir apenas as seleções de eventos definidas pelo usuário. As seleções de eventos predefinidas não podem ser excluídas.

Para excluir uma ou várias seleções de eventos:

1. No menu principal, acesse **Monitoramento e relatórios → Seleções de eventos**.
2. Marque as caixas de seleção ao lado das seleções de eventos que deseja excluir.
3. Clique em **Excluir**.
4. Na janela que se abre, clique em **OK**.

A seleção de eventos é excluída.

Visualização dos detalhes de um evento

Para visualizar detalhes de um evento:

1. Nova seleção de eventos.
2. Clique na hora do evento necessário.
   A janela **Propriedades do evento** se abre.
3. Na janela exibida, você pode fazer o seguinte:
   - Visualizar as informações sobre o evento selecionado
   - Ir ao evento anterior e ao seguir no resultado da seleção de eventos
   - Ir ao dispositivo no qual o evento ocorreu
   - Ir ao grupo de administração que inclui o dispositivo no qual o evento ocorreu
   - Para um evento relacionado a uma tarefa, vá às propriedades da tarefa

Exportar eventos para um arquivo

O Kaspersky Security Center permite salvar eventos de uma seleção de eventos em um arquivo TXT.

Para exportar eventos para um arquivo:

1. Nova seleção de eventos.
2. Selecione a caixa de seleção junto ao evento necessário.
   Você também pode selecionar vários eventos ou toda a lista de eventos.
3. Clique no botão **Exportar para arquivo**.

O evento selecionado é exportado para um arquivo TXT.

Exportando eventos para os sistemas SIEM

Esta seção descreve como configurar a exportação de eventos para os sistemas SIEM.

Configuração da exportação de eventos para sistemas SIEM

O Kaspersky Security Center permite a configuração por um dos seguintes métodos: exportação para qualquer sistema SIEM que use o formato Syslog, exportação para sistemas QRadar, Splunk, ArcSight SIEM que usam formatos LEEF e CEF ou exportação de eventos para sistemas SIEM diretamente do banco de dados do Kaspersky Security Center. Ao concluir este cenário, o Servidor de Administração envia eventos ao sistema SIEM automaticamente.

Pré-requisitos

Antes de iniciar a exportação de configuração de eventos no Kaspersky Security Center:

- Saiba mais sobre os métodos de exportação de eventos.
- Certifique-se de que tem conhecimento dos os valores das configurações do sistema.

> Você pode executar as etapas deste cenário em qualquer ordem.

O processo de exportação de eventos para o sistema SIEM consiste nos seguintes passos:

- **Configurando o sistema SIEM para receber eventos do Kaspersky Security Center**

  Instruções: Configurando a exportação de eventos em um sistema SIEM

- **Selecionando os eventos que deseja exportar para o sistema SIEM:**

  Instruções de como proceder:

  - Console de Administração: Marcando eventos de um aplicativo Kaspersky para exportação em formato Syslog, Marcando eventos gerais para exportação em formato Syslog
  - Kaspersky Security Center Web Console: Marcando eventos de um aplicativo Kaspersky para exportação em formato Syslog, Marcando eventos gerais para exportação em formato Syslog

- **Configurando a exportação de eventos para o sistema SIEM usando um dos seguintes métodos:**

  - Usando TCP/IP, UDP ou TLS via protocolos TCP.

    Instruções de como proceder:

    - Console de Administração: configurando a exportação de eventos para sistemas SIEM
    - Kaspersky Security Center Web Console: configurando a exportação de eventos para sistemas SIEM

  - Usando a exportação de eventos diretamente do banco de dados do Kaspersky Security Center (um conjunto de visualizações públicas é fornecido no banco de dados do Kaspersky Security Center e é possível encontrar a descrição dessas visualizações públicas no documento klakdb.chm).

Resultados

Após configurar a exportação de eventos para o sistema SIEM, você pode ver os resultados de exportação se tiver selecionado eventos que deseja exportar.

Antes de iniciar

Ao configurar uma exportação automática de eventos no Kaspersky Security Center, você deve especificar algumas das configurações do sistema SIEM. Recomenda-se que você verifique estas configurações com antecedência para preparar-se para configurar o Kaspersky Security Center.

Para configurar com êxito o envio automático de eventos a um sistema SIEM, você deve conhecer as seguintes configurações:

- **Endereço do servidor do sistema SIEM**

  O endereço IP do servidor onde o sistema SIEM atualmente usado está instalado. Verifique este valor nas suas configurações de sistema SIEM.

- **Porta do servidor do sistema SIEM**

  O número da porta usada para estabelecer a conexão entre o Kaspersky Security Center e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center e nas configurações do receptor do seu sistema SIEM.

- **Protocolo**

  Protocolo usado para transferir mensagens do Kaspersky Security Center ao seu sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center e nas configurações do receptor do seu sistema SIEM.

Sobre a exportação de evento

Você pode usar a exportação de evento dentro de sistemas centralizados que tratam de questões de segurança em nível organizacional e técnico, que fornecem serviços de monitoramento da segurança e consolidam informações de diferentes soluções. Estes são sistemas SIEM, que fornecem a análise em tempo real de alertas de segurança e eventos gerados por hardware de rede e aplicativos ou Centros de Operação de Segurança (SOCs).

Estes sistemas recebem dados de muitas fontes, incluindo redes, segurança, servidores, bancos de dados e aplicativos. Os sistemas de SIEM também fornecem a funcionalidade para consolidar os dados monitorados para ajudá-lo a evitar faltar a eventos críticos. Além disso, os sistemas executam a análise automatizada de eventos correlacionados e alertas para notificar os administradores de problemas de segurança imediatos. Um alerta pode ser implementado através de um painel ou pode ser enviado por canais de terceiros, tal como por um e-mail.

O processo de exportar eventos do Kaspersky Security Center para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center) e um receptor do evento (sistema SIEM). Para exportar com sucesso eventos, é necessário configurar isso no seu sistema SIEM e no Kaspersky Security Center. Não importa que lado você configura primeiro. Você pode configurar a transmissão de eventos no Kaspersky Security Center e depois configurar o recebimento de eventos pelo sistema SIEM, ou vice-versa.

Métodos para enviar eventos do Kaspersky Security Center

Há três métodos para enviar eventos do Kaspersky Security Center aos sistemas externos:

- Enviando eventos sob o protocolo Syslog à qualquer sistema SIEM

  Usando o protocolo Syslog, você pode encaminhar qualquer evento que ocorre no Servidor de Administração do Kaspersky Security Center e em aplicativos Kaspersky que são instalados em dispositivos gerenciados. O protocolo Syslog é um protocolo de registro de mensagem padrão. É possível usá-lo para exportar os eventos para qualquer sistema SIEM.

  Para isso, é preciso marcar os eventos que deseja retransmitir ao sistema SIEM. É possível marcar os eventos no console de administração ou no Kaspersky Security Center Web Console. Apenas os eventos marcados serão retransmitidos para o sistema SIEM. Caso não tenha marcado nada, nenhum evento será retransmitido.

- Enviando eventos sobre os protocolos CEF e LEEF para os sistemas QRadar, Splunk e ArcSight

  Você pode usar os protocolos CEF e LEEF para exportar eventos gerais. Ao exportar eventos sobre os protocolos CEF e LEEF, você não tem a capacidade de selecionar eventos específicos para exportar. Em vez disso, todos os eventos gerais são exportados. Para converter eventos do Kaspersky Security Center em eventos no formato CEF e LEEF, você precisa usar o arquivo siem_conversion_rules.xml. Esse arquivo contém a lista de atributos de eventos do Kaspersky Security Center e atributos correspondentes de eventos nos formatos CEF e LEEF. Além disso, o arquivo siem_conversion_rules.xml contém as regras para gerar mensagens correspondentes aos eventos. Esse arquivo está incluído no kit de distribuição do Kaspersky Security Center.

  Diferentemente do protocolo Syslog, os protocolos CEF e LEEF não são universais. CEF e LEEF são destinados para os sistemas SIEM apropriados (QRadar, Splunk e ArcSight). Portanto, quando você escolhe exportar eventos através de um desses protocolos, você usa o analisador necessário no sistema SIEM.

- Diretamente do banco de dados do Kaspersky Security Center para qualquer sistema SIEM

  Este método de exportar eventos pode ser usado para receber eventos diretamente das vistas públicas do banco de dados por meio de consultas SQL. Os resultados de uma consulta são salvos em um arquivo XML que pode ser usado como dados de entrada para um sistema externo. Somente os eventos disponíveis nas vistas públicas podem ser exportados diretamente do banco de dados.

Recebimento de eventos pelo sistema SIEM

O sistema SIEM deve receber e corretamente analisar os eventos recebidos do Kaspersky Security Center. Para estes propósitos, você deve configurar apropriadamente o sistema SIEM. A configuração depende do sistema SIEM específico utilizado. No entanto, há um número de etapas gerais na configuração de todos os sistemas SIEM, tal como a configuração do receptor e do analisador.

Sobre a configuração de exportação de eventos em um sistema SIEM

O processo de exportar eventos do Kaspersky Security Center para sistemas SIEM externos envolve duas partes: um remetente de evento (Kaspersky Security Center) e um receptor do evento (sistema SIEM). Você deve configurar a exportação de eventos no seu sistema SIEM e no Kaspersky Security Center.

As configurações especificadas no sistema SIEM dependem de qual sistema que você estiver usando. Normalmente, para todos os sistemas SIEM você deve definir um receptor e, opcionalmente, um analisador de mensagem para analisar os eventos recebidos.

Configurar o receptor

Para poder receber eventos enviados pelo Kaspersky Security Center, configure o receptor no seu sistema SIEM. Em geral, as seguintes configurações devem ser especificadas no sistema SIEM:

- **Protocolo para exportar ou tipo de entrada**

  É o protocolo de transferência de mensagem, TCP/IP ou UDP. Este protocolo deve ser o mesmo protocolo que você especificou no Kaspersky Security Center.

- **Porta**

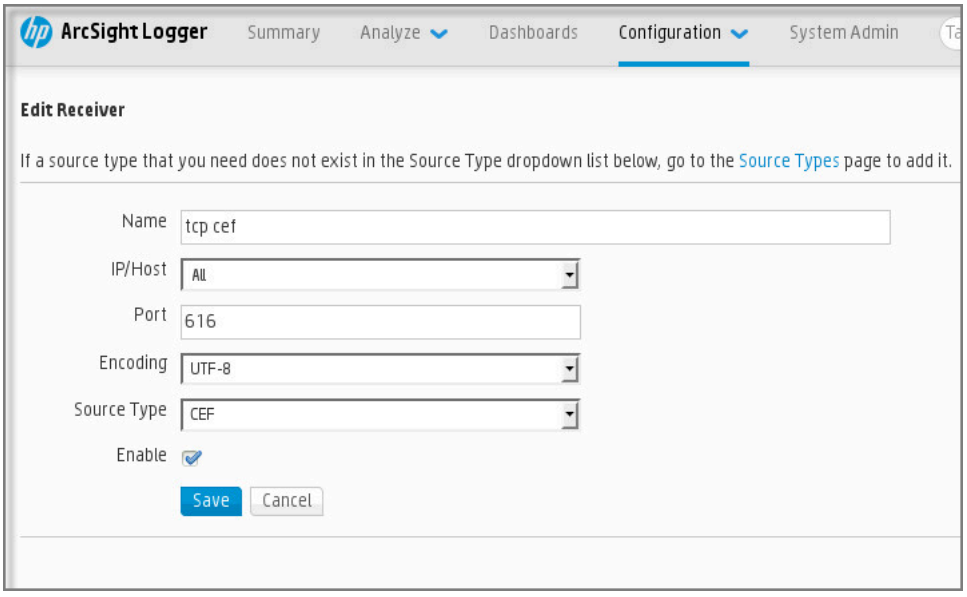
  Número da porta para conectar-se ao Kaspersky Security Center. Esta porta deve ser a mesma que a porta que você especificou no Kaspersky Security Center.

- **Protocolo de mensagem ou tipo de origem**

  O protocolo usado para exportar eventos ao sistema SIEM. Pode ser um dos protocolos padrão: Syslog, CEF ou LEEF. O sistema SIEM seleciona o analisador de mensagem de acordo com o protocolo que você especifica.

Dependendo do sistema SIEM usado, você pode ter que especificar algumas configurações adicionais de receptor.

A figura abaixo mostra tela de configuração de receptor no ArcSight.



Configuração do receptor no ArcSight

Analisador de mensagem

Os eventos exportados são passados aos sistemas SIEM como mensagens. Estas mensagens devem ser apropriadamente analisadas para que as informações nos eventos possam ser usadas pelo sistema SIEM. Os analisadores de mensagem são uma parte do sistema SIEM; eles são usados para dividir o conteúdo da mensagem em campos relevantes, como ID do evento, gravidade, descrição e parâmetros. Isto ativa o sistema SIEM para processar eventos recebidos do Kaspersky Security Center para que eles possam ser armazenados no banco de dados do sistema SIEM.

Marcando eventos para exportação para sistemas SIEM em formato Syslog

Após ativar a exportação automática de eventos, você deve selecionar quais eventos serão exportados ao sistema SIEM externo.

Você pode configurar a exportação de eventos em formato Syslog para um sistema externo com base em uma das seguintes condições:

- Marcando eventos gerais. Se você marcar eventos para exportar em uma política, nas configurações de um evento ou no Servidor de Administração, o sistema SIEM receberá os eventos marcados que ocorreram em todos os aplicativos gerenciados pela política específica. Se os eventos exportados foram selecionados na política, você não será capaz de redefini-los para um aplicativo individual gerenciado por esta política.

- Marcando eventos para um aplicativo individual. Se você marcar eventos para exportar para um aplicativo gerenciado instalado em um dispositivo gerenciado, o sistema SIEM somente receberá os eventos que ocorreram neste aplicativo.

Sobre a marcação de eventos para exportação para o sistema SIEM no formato Syslog

Após ativar a exportação automática de eventos, você deve selecionar quais eventos serão exportados ao sistema SIEM externo.

Você pode configurar a exportação de eventos em formato Syslog para um sistema externo com base em uma das seguintes condições:

- Marcando eventos gerais. Se você marcar eventos para exportar em uma política, nas configurações de um evento ou no Servidor de Administração, o sistema SIEM receberá os eventos marcados que ocorreram em todos os aplicativos gerenciados pela política específica. Se os eventos exportados foram selecionados na política, você não será capaz de redefini-los para um aplicativo individual gerenciado por esta política.

- Marcando eventos para um aplicativo individual. Se você marcar eventos para exportar para um aplicativo gerenciado instalado em um dispositivo gerenciado, o sistema SIEM somente receberá os eventos que ocorreram neste aplicativo.

Marcando eventos de um aplicativo da Kaspersky para exportação em formato Syslog

Se você desejar exportar eventos que ocorreram em um aplicativo gerenciado específico instalado nos dispositivos gerenciados, marque os eventos para exportação na política do aplicativo. Nesse caso, os eventos marcados são exportados de todos os dispositivos incluídos no escopo da política.

Para marcar eventos para exportação para um aplicativo gerenciado específico:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.

2. Clique na política do aplicativo para o qual você deseja marcar eventos.

   A janela Propriedades da política será aberta.

3. Siga para a seção **Configuração de eventos**.

4. Marque as caixas de seleção ao lado dos eventos que você deseja exportar para um sistema SIEM.

5. Clique no botão **Marcar exportação para o sistema SIEM usando o Syslog**.

   Também é possível marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, que é aberta ao clicar no link do evento.

6. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.

7. Clique no botão **Salvar**.

Os eventos marcados do aplicativo gerenciado estão prontos para serem exportados para um sistema SIEM.

É possível marcar quais eventos exportar para um sistema SIEM para um dispositivo gerenciado específico. Se os eventos exportados anteriormente foram marcados em uma política de aplicativo, não será possível redefinir os eventos marcados para um dispositivo gerenciado.

Para marcar eventos para exportação para um dispositivo gerenciado:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.

   A lista de dispositivos gerenciados é exibida.

2. Clique no link com o nome do dispositivo desejado na lista de dispositivos gerenciados.

   A janela Propriedades do dispositivo selecionado é exibida.

3. Siga para a seção **Aplicativos**.

4. Clique no link com o nome do aplicativo desejado na lista de aplicativos.

5. Siga para a seção **Configuração de eventos**.

6. Marque as caixas de seleção ao lado dos eventos que deseja exportar para um arquivo.

7. Clique no botão **Marcar exportação para o sistema SIEM usando o Syslog**.

   Além disso, você pode marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, aberta ao se clicar no link do evento.

8. O sinal de verificação (✓) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.

A partir de agora, o Servidor de Administração envia os eventos marcados para o sistema SIEM se a exportação para o sistema SIEM estiver configurada.

Marcando eventos gerais para exportação no formato Syslog

Você pode marcar eventos gerais que o Servidor de Administração exportará para os sistemas SIEM usando o formato Syslog.

Para configurar eventos gerais para um sistema SIEM:

1. Execute uma das seguintes ações:

   - No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   - No menu principal, vá para **Dispositivos** → **Políticas e perfis** e clique no link de uma política.

2. Na janela aberta, vá para **Configuração de eventos**.

3. Clique em **Marcar exportação para o sistema SIEM usando o Syslog**.

   Além disso, você pode marcar um evento para exportação para o sistema SIEM na seção **Registro de eventos**, aberta ao se clicar no link do evento.

4. O sinal de verificação ( ) aparece na coluna **Syslog** de um ou mais eventos marcados para exportação para o sistema SIEM.

A partir de agora, o Servidor de Administração envia os eventos marcados para o sistema SIEM se a exportação para o sistema SIEM estiver configurada.

Sobre a exportação de eventos usando formatos CEF e LEEF

Você pode usar os formatos CEF e LEEF para exportar eventos gerais, bem como eventos transferidos pelos aplicativos Kaspersky para o Servidor de Administração. O conjunto de eventos exportado é predefinido, e você não pode selecionar os eventos a ser exportados. Antes de enviar eventos para o sistema SIEM (QRadar, ArcSight ou Splunk), é necessário interpretar os eventos do Kaspersky Security Center para eventos no formato CEF e LEEF com o uso das regras especificadas no arquivo siem_conversion_rules.xml.

Selecione o formato de exportação com base no sistema SIEM usado. A tabela abaixo mostra os sistemas SIEM e os formatos de exportação correspondentes.

Formatos da exportação de eventos para um sistema SIEM

SIEM system	Formato de exportação
QRadar	LEEF
ArcSight	CEF
Splunk	CEF

- LEEF (Formato Estendido de Evento de Log) – Um formato de evento customizado para o IBM Security QRadar SIEM. O QRadar pode integrar, identificar e processar eventos LEEF. Os eventos de LEEF devem usar a codificação de caractere UTF-8. Você pode encontrar as informações detalhadas sobre o protocolo LEEF no IBM Knowledge Center.

- CEF (Formato de Evento Comum) – Um padrão de gerenciamento de registro aberto que aprimora a interoperabilidade da informação relativa a segurança de diferentes dispositivos de segurança e de rede e aplicativos. O CEF lhe permite usar um formato de registro de evento comum para que os dados possam ser facilmente integrados e agregados para a análise por um sistema de gerenciamento corporativo. Os eventos de CEF devem usar a codificação de caractere UTF-8.

A exportação automática significa que o Kaspersky Security Center envie eventos gerais ao sistema SIEM. A exportação automática de eventos inicia imediatamente após você a ativar. Esta seção explica detalhadamente como ativar a exportação automática de eventos.

Sobre a exportação de eventos usando o formato Syslog

Você pode usar o formato Syslog para exportar aos sistemas SIEM os eventos que ocorrem no Servidor de Administração e em outros aplicativos Kaspersky instalados em dispositivos gerenciados.

Syslog é um padrão para o protocolo de registro da mensagem. Isso permite a separação do software que gera mensagens, o sistema que as armazena e o software que os reporta e os analisa. Cada mensagem é legendada com um código de instalação, indicando o tipo de software que gera a mensagem e à mesma é atribuído um nível de gravidade.

O formato Syslog é definido por documentos de Solicitação de Comentários (RFC) publicados pela Internet Engineering Task Force (padrões da Internet). O padrão RFC 5424 é usado para exportar os eventos do Kaspersky Security Center aos sistemas externos.

No Kaspersky Security Center, você pode configurar a exportação dos eventos aos sistemas externos usando o formato Syslog.

O processo de exportação consistem em duas etapas:

1. Ativar a exportação automática do evento. Nesta etapa, o Kaspersky Security Center é configurado para que ele envie eventos ao sistema SIEM. O Kaspersky Security Center começa a enviar eventos imediatamente após você ativar a exportação automática.

2. Selecionar os eventos a ser exportados ao sistema externo. Nesta etapa, você seleciona qual evento exportar ao sistema SIEM.

Configurando o Kaspersky Security Center para exportação de eventos para o sistema SIEM

Este artigo descreve como configurar a exportação de eventos para sistemas SIEM.

Antes de enviar eventos para o sistema SIEM (QRadar, ArcSight ou Splunk), é necessário interpretar os eventos do Kaspersky Security Center para eventos no formato CEF e LEEF com o uso das regras especificadas no arquivo siem_conversion_rules.xml.

Para configurar a exportação para sistemas SIEM no Kaspersky Security Center Web Console:

1. No menu principal, vá para **Configurações do console** → **Integração**.

2. Na guia **Integração**, selecione a seção **SIEM**.

3. Clique no link **Configurações**.

   A seção **Exportar as configurações** é aberta.

4. Especifique as configurações na seção **Exportar as configurações**:

- **Endereço do servidor do sistema SIEM**

  O endereço IP do servidor onde o sistema SIEM atualmente usado está instalado. Verifique este valor nas suas configurações de sistema SIEM.

- **Porta do sistema SIEM**

  O número da porta usada para estabelecer a conexão entre o Kaspersky Security Center e o seu servidor do sistema SIEM. Você especifica este valor nas configurações do Kaspersky Security Center e nas configurações do receptor do seu sistema SIEM.

- **Protocolo**

Selecione o protocolo a ser usado para transferir mensagens para o sistema SIEM. É possível selecionar o TCP, UDP ou TLS sobre protocolo TCP.

Especifique as seguintes configurações de TLS se selecionar o protocolo TLS sobre TCP:

- **Autenticação do servidor**

  No campo **Autenticação do servidor**, você pode selecionar os valores de **Certificados confiáveis** ou de **Impressões digitais SHA**:

  - **Certificados confiáveis**. Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação (CA) confiável e carregá-lo para o Kaspersky Security Center. O Kaspersky Security Center verifica se a cadeia de certificado do servidor do sistema SIEM é assinada por uma CA confiável.

    Para adicionar um certificado confiável, clique no botão **Procurar arquivo de certificados CA** e, em seguida, carregue o certificado.

  - **Impressões digitais SHA**. Você pode especificar impressões digitais SHA1 da cadeia de certificados completa do sistema SIEM (incluindo o certificado raiz) no Kaspersky Security Center. Para adicionar uma impressão digital SHA1, insira-a no campo **Impressões digital** e, em seguida, clique no botão **Adicionar**.

  Ao usar a configuração **Adicionar autenticação do cliente**, você pode gerar um certificado para autenticar o Kaspersky Security Center. Assim, você usará um certificado autoassinado emitido pelo Kaspersky Security Center. Nesse caso, você pode usar um certificado confiável e uma impressão digital SHA para autenticar o servidor do sistema SIEM.

- **Adicionar nome do assunto/Nome alternativo do assunto**

  Nome do assunto é um nome de domínio para o qual o certificado foi recebido. O Kaspersky Security Center não pode se conectar ao servidor do sistema SIEM se o nome de domínio do servidor do sistema SIEM não corresponder ao nome da entidade do certificado do servidor do sistema SIEM. No entanto, o servidor do sistema SIEM pode alterar seu nome de domínio se o nome tiver sido alterado no certificado. Neste caso, você pode especificar nomes de assuntos no campo **Adicionar nome do assunto/Nome alternativo do assunto**. Se qualquer um dos nomes de assunto especificados corresponder ao nome do assunto do certificado do sistema SIEM, o Kaspersky Security Center valida o certificado do servidor do sistema SIEM.

- **Adicionar autenticação do cliente**

  Para autenticação de cliente, você pode inserir o seu certificado ou gerá-lo no Kaspersky Security Center.

  - **Inserir certificado**. Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer CA confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

    - **Certificado X.509 PEM**. Carregue um arquivo com um certificado no campo **Arquivo com certificado** e um arquivo com uma chave privada no campo **Arquivo com chave**. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Quando os dois arquivos forem carregados, especifique a senha para decodificar a chave privada no campo **Verificação de senha ou certificado**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

    - **Certificado X.509 PKCS12**. Carregue um único arquivo que contenha um certificado e sua chave privada no campo **Arquivo com certificado**. Quando o arquivo for carregado, especifique a senha para decodificar a chave privada no campo **Verificação de senha ou certificado**. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- **Gerar chave**. Você pode gerar um certificado autoassinado no Kaspersky Security Center. Como resultado, o Kaspersky Security Center armazena o certificado autoassinado gerado e você pode passar a parte pública do certificado ou a impressão digital SHA1 para o sistema SIEM.

- Formato de data

  Você pode selecionar os formatos de log do sistema, CEF ou LEEF, dependendo dos requisitos do sistema SIEM.

Se selecionar o formato Syslog, você deve especificar:

- Tamanho máximo da mensagem de eventos, em bytes

  Especifique o tamanho máximo (em bytes) de uma mensagem encaminhada ao sistema SIEM. Cada evento é encaminhado em uma mensagem. Se o comprimento real de uma mensagem exceder o valor especificado, a mensagem é truncada e os dados podem ser perdidos. O tamanho padrão é de 2.048 bytes. Este campo estará disponível somente se você selecionar o formato de log do sistema no campo **Protocolo**.

5. Alterne a opção para a posição **Exportar automaticamente os eventos para o banco de dados do sistema SIEM Ativado**.

6. Clique no botão **Salvar**.

A exportação para o sistema SIEM está configurada.

Exportando eventos diretamente do banco de dados

Você pode recuperar eventos diretamente do banco de dados do Kaspersky Security Center sem ter necessidade de usar a interface Kaspersky Security Center. Você pode consultar as vistas públicas diretamente e recuperar os dados de evento, ou ainda criar as suas próprias vistas com base em vistas públicas existentes e endereçá-las para receber os dados de que precisa.

Vistas públicas

Para a sua conveniência, um conjunto de vistas públicas é fornecido no banco de dados do Kaspersky Security Center. Você pode encontrar a descrição dessas visualizações públicas no documento klakdb.chm.

A vista pública v_akpub_ev_event contém um conjunto de campos que representa os parâmetros de evento no banco de dados. No documento klakdb.chm você também pode encontrar informações sobre vistas públicas que correspondem a outras entidades do Kaspersky Security Center, por exemplo, dispositivos, aplicativos ou usuários. Você pode usar estas informações nas suas consultas.

Esta seção contém instruções para executar uma consulta SQL por meio do utilitário klsql2 e um exemplo de consulta.

Para criar consultas SQL ou vistas do banco de dados, você também pode usar qualquer outro programa para trabalhar com bancos de dados. As informações sobre como exibir os parâmetros para conectar-se ao banco de dados do Kaspersky Security Center, como o nome da instância e o nome do banco de dados, são fornecidas na seção correspondente.

Executar uma consulta SQL usando o utilitário klsql2

Este artigo descreve como baixar e usar o utilitário klsql2 e como executar uma consulta SQL usando esse utilitário.

Para usar o utilitário klsql2:

1. Localize o utilitário klsql2 na pasta de instalação do Kaspersky Security Center. O caminho de instalação padrão é <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center. Não use versões do utilitário klsql2 destinadas a versões mais antigas do Kaspersky Security Center.

2. Crie um arquivo com a extensão .sql em qualquer editor de texto e coloque o arquivo na mesma pasta do utilitário.

3. No arquivo .sql criado, digite a consulta SQL desejada e salve o arquivo.

4. No dispositivo com o Servidor de Administração do Kaspersky Security Center instalado, na linha de comando, digite o seguinte comando para executar a consulta SQL do arquivo .sql e salve os resultados no arquivo result.xml:

   ```
   klsql2 -i src.sql -u <nome de usuário> -p <senha> -o result.xml
   ```

   onde `<nome de usuário>` e `<senha>` são as credenciais da conta de usuário que tem acesso ao banco de dados.

5. Caso seja necessário, digite o login e a senha da conta de usuário que tem acesso ao banco de dados.

6. Abra os arquivos result.xml criados recentemente para exibir os resultados da consulta SQL.

É possível editar o arquivo .sql e criar qualquer consulta SQL para as visualizações públicas. Então, a partir da linha de comando, execute a consulta SQL e salve os resultados em um arquivo.

Exemplo de uma consulta SQL no utilitário klsql2

Esta seção mostra um exemplo de uma consulta SQL, executada por meio do utilitário klsql2.

O exemplo a seguir ilustra a recuperação dos eventos que ocorreram em dispositivos durante os últimos sete dias e exibe os eventos ordenados pelo horário em que ocorreram. Os eventos mais recentes são exibidos primeiro.

Exemplo:

```
SELECT

/* identificador do evento */
e.nId,

/* hora em que o evento ocorreu */
e.tmRiseTime,

/* nome interno do tipo de evento */
e.strEventType,

/* nome exibido do evento */
e.wstrEventTypeDisplayName,

/* descrição do evento exibida */
e.wstrDescription,

/* nome do grupo onde o dispositivo está localizado */
e.wstrGroupName,

/* nome exibido do dispositivo no qual o evento ocorreu */
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)) + '.' +

/* endereço IP do dispositivo no qual o evento ocorreu */
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
```

Exibir o nome de banco de dados do Kaspersky Security Center

Se você desejar acessar o banco de dados do Kaspersky Security Center por meio das ferramentas de gerenciamento de banco de dados do SQL Server, MySQL ou MariaDB deverá conhecer o nome do banco de dados para conectar-se usando o editor de script SQL.

Para exibir o nome do banco de dados do Kaspersky Security Center:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Detalhes do banco de dados atual**.

O nome do banco de dados é especificado no campo **Nome do banco de dados**. Use o nome do banco de dados para endereçar o banco de dados nas suas consultas SQL.

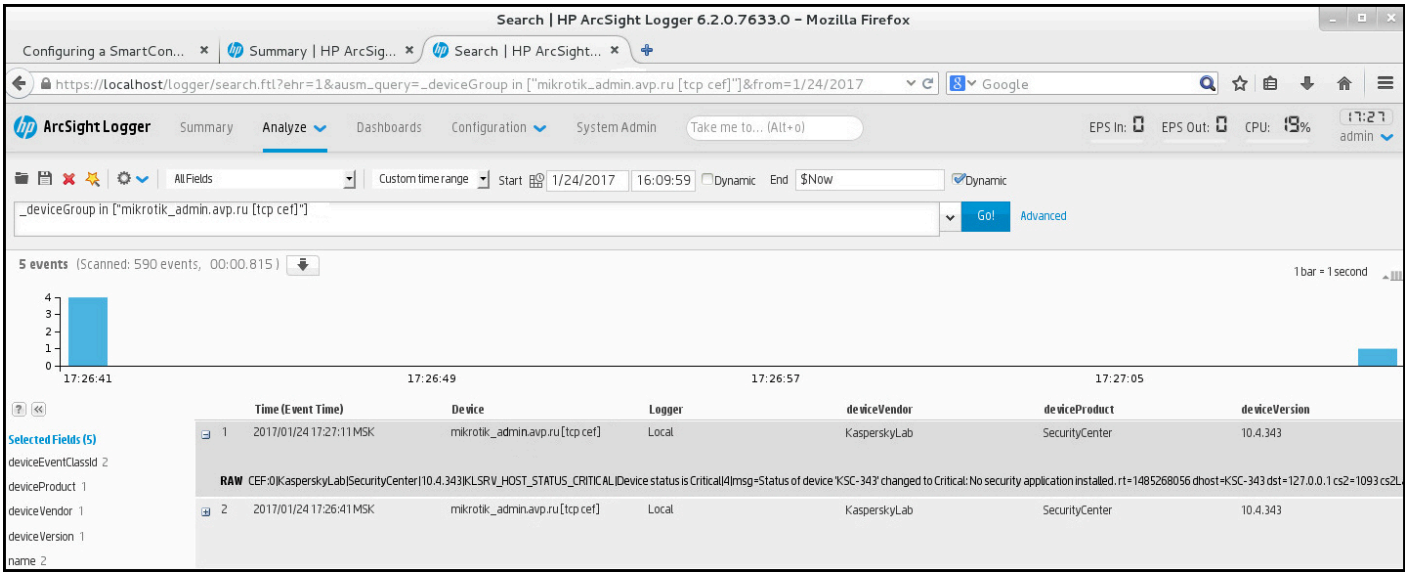
Exibir os resultados da exportação

Você pode controlar para a conclusão bem-sucedida do procedimento de exportação de eventos. Para fazer isto, verifique se as mensagens com eventos exportados são recebidas pelo seu sistema SIEM.

Se os eventos enviados do Kaspersky Security Center forem recebidos e apropriadamente analisados pelo seu sistema SIEM, a configuração nos dois lados foi feita apropriadamente. De outra forma, verifique as configurações que você especificou no Kaspersky Security Center contra a configuração no seu sistema SIEM.

A figura abaixo mostra os eventos exportados ao ArcSight. Por exemplo, o primeiro evento é crítico do Servidor de Administração: "*Status do dispositivo é crítico*".

A representação da exportação de eventos no sistema SIEM varia de acordo com o sistema SIEM que você usa.



Exemplo de eventos

Visualização de um histórico de eventos a partir de um evento

De um evento de criação ou modificação de um objeto que não tem suporte no gerenciamento de revisão, você pode alternar para o histórico de revisões do objeto.

Para visualizar o histórico de revisões de um evento:

1. Nova seleção de eventos.
2. Selecione a caixa de seleção junto ao evento necessário.
3. Clique no botão **Histórico de revisões**.

   O histórico de revisões do objeto é aberto.

Excluir os eventos

Para excluir um ou vários eventos:

1. Nova seleção de eventos.
2. Selecione as caixas de seleção junto aos eventos necessários.
3. Clique no botão **Excluir**.

   Os eventos selecionados são excluídos e não podem ser restaurados.

Configuração do termo de armazenamento de um evento

O Kaspersky Security Center lhe permite receber informações sobre os eventos que ocorrem durante a operação do Servidor de Administração e de outros aplicativos Kaspersky instalados nestes dispositivos gerenciados. As informações sobre eventos são salvas no banco de dados do Servidor de Administração. Você pode precisar armazenar alguns eventos por um período maior ou menor do que o especificado pelos valores padrão. Você pode alterar as configurações padrão do período de armazenamento de um evento.

Se não desejar em armazenar alguns eventos no banco de dados do Servidor de Administração, poderá desativar a respectiva configuração na política do Servidor de Administração e na política do aplicativo Kaspersky, ou nas propriedades do Servidor de Administração (apenas para eventos do Servidor de Administração). Isso reduzirá o número de tipos de evento no banco de dados.

Quanto mais longo o prazo de armazenamento de um evento, mais rápido o banco de dados atingirá sua capacidade máxima. No entanto, um prazo de armazenamento mais longo de um evento permite executar tarefas de monitoramento e relatório por um período maior.

Para definir o prazo de armazenamento de um evento no banco de dados do Servidor de Administração:

1. No menu principal, vá para **Dispositivos** → **Políticas e perfis**.
2. Clique no nome da política necessária.

   Você pode selecionar uma política de um aplicativo gerenciado, Agente de Rede ou Servidor de Administração da Kaspersky. No caso do Servidor de Administração, você também pode configurar o período de armazenamento de eventos clicando no ícone de configurações () correspondente ao nome do Servidor de Administração necessário.
3. Selecione a guia **Configuração de eventos**.

   Uma lista de tipos de evento relacionados à seção **Crítico** é exibida. Se necessário, você pode mover para as seções **Falha funcional**, **Advertência** ou **Informações**.
4. Na lista de tipos de eventos no painel direito, clique no link do evento cujo prazo de armazenamento deseja alterar.

   Na seção **Registro de eventos** da janela, o botão de alternância **Armazenar no banco de dados do Servidor de Administração por (dias)** está ativado.
5. Na caixa de edição abaixo desse botão de alternar, insira o número de dias para armazenar o evento.
6. Caso não deseje armazenar um evento no banco de dados do Servidor de Administração, desative a opção **Armazenar no banco de dados do Servidor de Administração por (dias)**.

   Se você configurar eventos do Servidor de Administração na janela de propriedades do Servidor de Administração e se as configurações do evento estiverem bloqueadas na política do Servidor de Administração do Kaspersky Security Center, não será possível redefinir o valor do período de armazenamento para um evento.
7. Clique em **OK** e clique no botão **Salvar** quando o painel direito for fechado.

   A janela de propriedades da política é fechada.

A partir de agora, quando o Servidor de Administração receber e armazenar os eventos do tipo selecionado, eles terão o prazo de armazenamento alterado. O Servidor de Administração não altera o prazo de armazenamento de eventos recebidos anteriormente.

Eventos dos componentes do Kaspersky Security Center

Cada componente do Kaspersky Security Center tem o seu próprio conjunto de tipos de evento. Esta seção lista tipos de eventos que ocorrem no Servidor de Administração do Kaspersky Security Center, no Agente de Rede, no Servidor de MDM do iOS e em um Servidor de dispositivos móveis do Microsoft Exchange. Os tipos de eventos que ocorrem nos aplicativos Kaspersky não são listados nesta seção.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Estrutura de dados da descrição do tipo de evento

Para cada tipo de evento, seu nome de exibição, o identificador (ID), o código alfabético, a descrição e o termo de armazenamento padrão são fornecidos.

- **Nome de exibição do tipo de evento**. Este texto é exibido no Kaspersky Security Center quando você configura eventos e quando eles ocorrem.
- **ID do tipo de evento**. Este código numérico é usado quando você processa eventos usando ferramentas de terceiros para a análise de eventos.
- **Tipo de evento** (código alfabético). Este código é usado quando você percorre e processa eventos usando vistas públicas fornecidas no banco de dados do Kaspersky Security Center e quando os eventos são exportados para um sistema SIEM.
- **Descrição**. Este texto contém as situações nas quais um evento ocorre e o que você pode fazer nesses casos.
- **Prazo de armazenamento padrão**. É o número de dias durante os quais o evento é armazenado no banco de dados do Servidor de Administração e é exibido na lista de eventos no Servidor de Administração. Após o término desse período, o evento é excluído. Se o valor do prazo de armazenamento do evento for 0, os eventos são detectados, mas não são exibidos na lista de eventos no Servidor de Administração. Se você configurou para salvar os eventos no log de eventos do sistema operacional, poderá encontrá-los nesse local.

  Você pode alterar o prazo de armazenamento de eventos:

  - Console de Administração: configuração do termo de armazenamento de um evento
  - Kaspersky Security Center Web Console: Configurar o termo de armazenamento de um evento

Outros dados podem incluir os seguintes campos:

- **event_id**: número exclusivo do evento no banco de dados, gerado e atribuído automaticamente. Não deve ser confundido com **ID do tipo de evento**.
- **task_id**: a ID da tarefa que causou o evento (se houver)
- **severity**: um dos níveis de gravidade a seguir (na ordem crescente de gravidade):

  0) nível de gravidade inválido

  1) Informativo

  2) Aviso

  3) Erro

  4) Crítico

Eventos do Servidor de Administração

Esta seção contém informações sobre os eventos relativos ao Servidor de Administração.

Eventos críticos do Servidor de Administração

A tabela abaixo mostra os tipos de eventos do Servidor de Administração do Kaspersky Security Center que têm o nível de importância **Crítico**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Caso a porta seja especificada na janela de propriedades do Servidor de Administração no Console de Administração, o **Kaspersky Security Center publicará as métricas** e os eventos críticos a serem obtidos pelo Prometheus, um sistema para monitoramento e alerta. O Prometheus obtém as métricas e os eventos críticos e, em seguida, gera os alertas para cada 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 de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O limite da licença foi excedido	4099	KLSRV_EV_LICENSE_CHECK_MORE_110	Uma vez por dia o Kaspersky Security Center verifica se um limite de licenciamento foi excedido. Eventos deste tipo ocorrem quando Servidor de Administração detectar que alguns limites de licenciamento estão excedidos pelos aplicativos da Kaspersky instalados nos dispositivos clientes e se o número de unidades de licenciamento atualmente usadas e cobertas por uma única licença exceder 110% do número total de unidades cobertas pela licença. Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. • Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração). O Kaspersky Security Center determina as regras para gerar eventos quando um limite de licenciamento for excedido.	180 dias
Surto de vírus	26 (para Proteção Contra Ameaças ao Arquivo)	GNRL_EV_VIRUS_OUTBREAK	Eventos desse tipo ocorrem quando a quantidade de objetos maliciosos detectada em diversos dispositivos gerenciados exceder o limite dentro de um curto período. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias
Surto de vírus	27 (para Proteção Contra Ameaças ao Correio)	GNRL_EV_VIRUS_OUTBREAK	Eventos desse tipo ocorrem quando a quantidade de objetos maliciosos detectada em diversos dispositivos gerenciados exceder o limite dentro de um curto período. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Surto de vírus	28 (para Firewall)	GNRL_EV_VIRUS_OUTBREAK	Eventos desse tipo ocorrem quando a quantidade de objetos maliciosos detectada em diversos dispositivos gerenciados exceder o limite dentro de um curto período. Você pode responder ao evento nas seguintes maneiras: • Você pode configurar o limite nas propriedades do Servidor de Administração. • Você também pode criar uma política mais rigorosa a ser ativada ou criar uma tarefa a ser executada no momento da ocorrência deste evento.	180 dias
O dispositivo está sem gerenciamento	4111	KLSRV_HOST_OUT_CONTROL	Eventos deste tipo ocorrem se um dispositivo gerenciado está visível na rede, mas não se conectou ao Servidor de Administração por um período específico. Descubra o que impede o funcionamento apropriado do Agente de Rede no dispositivo. As causas possíveis incluem problemas de rede e a remoção do Agente de Rede do dispositivo.	180 dias
O status do dispositivo é Crítico	4113	KLSRV_HOST_STATUS_CRITICAL	Eventos deste tipo ocorrem quando um dispositivo gerenciado é atribuído com o status *Crítico*. Você pode configurar as condições sob as quais o status do dispositivo é alterado para *Crítico*.	180 dias
O arquivo de chave foi adicionado à lista de bloqueio	4124	KLSRV_LICENSE_BLACKLISTED	Eventos deste tipo ocorrem quando a Kaspersky tiver adicionado o código de ativação ou arquivo de chave usado por você à lista de proibição. Entre em contato com o Suporte Técnico para obter mais detalhes.	180 dias
Modo de funcionalidade limitada	4130	KLSRV_EV_LICENSE_SRV_LIMITED_MODE	Eventos deste tipo ocorrem quando o Kaspersky Security Center inicia a operar com a funcionalidade básica, sem o Gerenciamento de Dispositivos Móveis e sem o Gerenciamento de patches e vulnerabilidades. A seguir se encontram as causas de, e as respostas apropriadas, do evento: • Termo da licença expirado. Forneça uma licença para usar a funcionalidade completa do Kaspersky Security Center (adicione um código de ativação ou um arquivo de chave válido no Servidor de Administração). • O Servidor de Administração gerencia mais dispositivos do que o especificado pelo limite da licença. Mover dispositivos dos grupos de administração de um Servidor de Administração para aqueles de outro Servidor (se o limite da licença do outro Servidor de Administração o permitir).	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
A licença expira em breve	4129	KLSRV_EV_LICENSE_SRV_EXPIRE_SOON	Eventos desse tipo ocorrem quando a data de expiração da licença comercial está se aproximando. Uma vez ao dia, o Kaspersky Security Center verifica se a data de expiração da licença está próxima. Eventos deste tipo são publicados 30 dias, 15 dias, 5 dias e 1 dia antes da data de expiração da licença. Você não pode alterar a quantidade de dias. Se o Servidor de Administração é desativado no dia especificado antes da data de expiração da licença, o evento não será publicado até o próximo dia. Quando a licença comercial expirar, o Kaspersky Security Center fornecerá apenas a funcionalidade básica. Você pode responder ao evento nas seguintes maneiras: • Certifique-se de que uma chave reserva de licença seja adicionada ao Servidor de Administração. • Caso use uma assinatura, certifique-se de renová-la. Uma assinatura ilimitada será automaticamente renovada, caso tenha sido pré-paga ao provedor de serviços na data devida.	180 dias
O certificado expirou	4132	KLSRV_CERTIFICATE_EXPIRED	Eventos desse tipo ocorrem quando o certificado de cliente de dispositivos móveis expira.	180 dias
As atualizações dos módulos de software da Kaspersky foram revogadas	4142	KLSRV_SEAMLESS_UPDATE_REVOKED	Eventos deste tipo ocorrem se as atualizações racionais tenham sido revogadas (o status *Revogada* é exibido para essas atualizações) pelos especialistas técnicos da Kaspersky; por exemplo, elas precisam ser atualizadas para uma versão mais nova. Este evento é relativo aos patches do Kaspersky Security Center e não relativos aos módulos dos aplicativos Kaspersky gerenciados. O evento fornece o motivo da não instalação das atualizações racionais.	180 dias

Eventos de falha funcional do Servidor de Administração

A tabela abaixo mostra os tipos de eventos do Servidor de Administração do Kaspersky Security Center que têm o nível de importância **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Erro do tempo de execução	4125	KLSRV_RUNTIME_ERROR	Eventos deste tipo ocorrem devido a problemas desconhecidos. Mais frequentemente estes são problemas de DBMS, problemas de rede e outros problemas de software e hardware. Os detalhes do evento podem ser encontrados na descrição do evento.	180 dias
O limite de instalações foi excedido para um dos grupos de aplicativos licenciados	4126	KLSRV_INVLICPROD_EXCEDED	O Servidor de Administração gera periodicamente eventos deste tipo (a cada hora). Eventos deste tipo ocorrem se no Kaspersky Security Center você gerencia chaves de licença de aplicativos de terceiros e o número de instalações excedeu o limite definido pela chave de licença do aplicativo de terceiro. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua o aplicativo de terceiro dos dispositivos nos quais o aplicativo não está em uso. • Use uma licença de terceiro para mais dispositivos. Você pode gerenciar chaves de licença de aplicativos de terceiros usando a funcionalidade de grupos de aplicativos licenciados. Um grupo de aplicativos licenciados inclui aplicativos de terceiros que atendem os critérios definidos por você.	180 dias
Falha ao amostrar o segmento da nuvem	4143	KLSRV_KLCLOUD_SCAN_ERROR	Os eventos desse tipo ocorrem quando o Servidor de Administração falha não faz a sondagem de um segmento de rede em um ambiente de nuvem. Leia os detalhes na descrição do evento e responda de acordo.	Não armazenado
Falha ao copiar as atualizações para a pasta especificada	4123	KLSRV_UPD_REPL_FAIL	Eventos deste tipo ocorrem quando as atualizações do software são copiadas para uma pasta adicional compartilhada. Você pode responder ao evento nas seguintes maneiras: • Verifique se a conta de usuário que está sendo empregada para obter o acesso às pastas tem permissão de gravação. • Verifique se um nome de usuário e/ou senha para a(s) pasta(s) foi/está alterado. • Verifique a conexão com a internet, já que isso pode ser a causa do evento. Siga as instruções para atualizar bancos de dados e módulos do software.	180 dias
Nenhum espaço livre em disco	4107	KLSRV_DISK_FULL	Eventos deste tipo ocorrem quando o disco rígido do dispositivo onde o Servidor de Administração está instalado fica sem espaço. Libere espaço em disco no dispositivo.	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
A pasta compartilhada não está disponível	4108	KLSRV_SHARED_FOLDER_UNAVAILABLE	Eventos deste tipo ocorrem se a pasta compartilhada do Servidor de Administração não estiver disponível. Você pode responder ao evento nas seguintes maneiras: • Verifique se o Servidor de Administração (onde a pasta compartilhada está localizada) está ativado e disponível. • Verifique se um nome de usuário e/ou senha para a pasta foi/está alterado. • Verifique a conexão à rede.	180 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O banco de dados do Servidor de Administração está indisponível	4109	KLSRV_DATABASE_UNAVAILABLE	Eventos deste tipo ocorrem se o banco de dados do Servidor de Administração s tornar indisponível. Você pode responder ao evento nas seguintes maneiras: • Verifique se o servidor remoto que tem o SQL Server instalado está disponível. • Visualize os registros do DBMS para descobrir o motivo da indisponibilidade de banco de dados do Servidor de Administração. Por exemplo, devido a uma manutenção preventiva de um servidor remoto com o SQL Server instalado possa estar indisponível.	180 dias
Espaço insuficiente no banco de dados do Servidor de Administração	4110	KLSRV_DATABASE_FULL	Eventos deste tipo ocorrem quando não houver nenhum espaço livre no banco de dados do Servidor de Administração. O Servidor de Administração não funciona quando seu banco de dados alcançou sua capacidade e quando o registro no banco de dados não for possível. A seguir estão as causas deste evento, dependendo do DBMS que você usa, e as respostas apropriadas ao evento: • Você usa o SQL Server Express Edition DBMS: Na documentação do SQL Server Express, verifique o limite de tamanho do banco de dados para a versão que estiver usando. Provavelmente, o banco de dados de seu Servidor de Administração excedeu o limite de tamanho. Limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração. No banco de dados do Servidor de Administração, há muitos eventos enviados pelo componente Controle de Aplicativos. Você pode alterar as configurações da política do Kaspersky Endpoint Security for Windows relacionadas ao armazenamento de eventos do Controle de Aplicativos no banco de dados do Servidor de Administração. • Você usa um DBMS diferente do SQL Server Express Edition: Não limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração. Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração. Revise as informações na seleção do DBMS.	180 dias

Eventos de aviso do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração do Kaspersky Security Center com o nível de importância **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Foi detectado um evento frequente de spam		KLSRV_EVENT_SPAM_EVENTS_DETECTED	Eventos desse tipo ocorrem quando o Servidor de Administração detecta um evento frequente em um dispositivo gerenciado. Consulte a seguinte seção para obter detalhes: Bloqueio de eventos frequentes.	90 dias
O limite da licença foi excedido	4098	KLSRV_EV_LICENSE_CHECK_100_110	Uma vez por dia o Kaspersky Security Center verifica se um limite de licença foi excedido. Eventos deste tipo ocorrem quando Servidor de Administração detectar que alguns limites de licenciamento estão excedidos pelos aplicativos da Kaspersky instalados nos dispositivos clientes e se o número de unidades de licenciamento atualmente usadas e cobertas por uma única licença exceder 100% a 110% do número total de unidades cobertas pela licença. Mesmo quando este evento ocorrer, os dispositivos clientes estão protegidos. Você pode responder ao evento nas seguintes maneiras: • Examine a lista de dispositivos gerenciados. Exclua os dispositivos que não estão em uso. • Forneça uma licença para mais dispositivos (adicione um código de ativação ou arquivo de chave válido no Servidor de Administração). O Kaspersky Security Center determina as regras para gerar eventos quando um limite de licença é excedido.	90 dias
O dispositivo permaneceu inativo na rede por muito tempo	4103	KLSRV_EVENT_HOSTS_NOT_VISIBLE	Eventos desse tipo ocorrem quando um dispositivo gerenciado fica em inatividade por algum tempo. Na maioria das vezes, isso acontece quando um dispositivo gerenciado é desativado. Você pode responder ao evento nas seguintes maneiras: • Remova manualmente o dispositivo da lista de dispositivos gerenciados. • Especifique o intervalo de tempo após o qual o evento **O dispositivo permaneceu inativo na rede por muito tempo** é criado usando o Console de Administração ou o Kaspersky Security Center Web Console. • Especifique o intervalo de tempo após o qual o dispositivo é removido automaticamente do grupo usando o Console de Administração ou o Kaspersky Security Center Web Console.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Conflito de nomes de dispositivo	4102	KLSRV_EVENT_HOSTS_CONFLICT	Eventos desse tipo ocorrem quando o Servidor de Administração considera dois ou mais dispositivos gerenciados como um único dispositivo. Na maioria das vezes, isso acontece quando um disco rígido clonado foi usado para implantação de software em dispositivos gerenciados, sem alterar o Agente de Rede para o modo de clonagem de disco dedicado em um dispositivo de referência. Para evitar este problema, altere o Agente de Rede para o modo de clonagem de disco em um dispositivo de referência antes de clonar o disco rígido desse dispositivo.	90 dias
O status do dispositivo é Advertência	4114	KLSRV_HOST_STATUS_WARNING	Eventos deste tipo ocorrem quando à um dispositivo gerenciado for atribuído o status de *Aviso*. Você pode configurar as condições sob as quais o status do dispositivo é alterado para *Aviso*.	90 dias
O limite de instalações está prestes a ser excedido para um dos grupos de aplicativos licenciados	4127	KLSRV_INVLICPROD_FILLED	Eventos deste tipo ocorrem quando o número de instalações de aplicativos de terceiros incluídos em um grupo de aplicativos licenciados atinge 90% do valor máximo permitido especificado nas propriedades da chave de licença. Você pode responder ao evento nas seguintes maneiras: • Se o aplicativo de terceiros não estiver em uso em alguns dos dispositivos gerenciados, exclua o aplicativo desses dispositivos. • Se você espera que o número de instalações do aplicativo de terceiros ultrapasse o máximo permitido em um futuro próximo, considere obter uma licença de terceiros para um número maior de dispositivos com antecedência. Você pode gerenciar chaves de licença de aplicativos de terceiros usando a funcionalidade de grupos de aplicativos licenciados.	90 dias
O certificado foi solicitado	4133	KLSRV_CERTIFICATE_REQUESTED	Eventos deste tipo ocorrem quando um certificado para Gerenciamento de Dispositivos Móveis não é reemitido automaticamente. Seguem abaixo as possíveis causas e as respostas apropriadas para o evento: • A reemissão automática foi iniciada para um certificado para o qual a opção **Reemitir o certificado automaticamente se possível** está desativada. Isso pode ser devido a um erro ocorrido durante a criação do certificado. Pode ser necessária a reemissão manual do certificado. • Se você usar uma integração com uma infraestrutura de chave pública, a causa pode ser a ausência de um atributo SAM-Account-Name na conta usada para integração com PKI e para emissão do certificado. Revise as propriedades da conta.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O certificado foi removido	4134	KLSRV_CERTIFICATE_REMOVED	Eventos deste tipo ocorrem quando um administrador remove qualquer tipo de certificado (Geral, Correio, VPN) para Gerenciamento de Dispositivos Móveis. Depois de remover um certificado, os dispositivos móveis conectados por meio deste certificado não conseguirão se conectar ao Servidor de Administração. Este evento pode ser útil ao investigar falhas associadas ao gerenciamento de dispositivos móveis.	90 dias
O certificado vai expirar	6128	ServerCertificateExpiresSoon	Eventos deste tipo ocorrem quando os certificados do Servidor de Administração para dispositivos móveis e dispositivos com UEFI expiram. Você precisa atualizar o certificado expirado.	90 dias
O certificado de APNs expirou	4135	KLSRV_APN_CERTIFICATE_EXPIRED	Eventos deste tipo ocorrem quando um certificado de APNs expira. Você precisa renovar manualmente o certificado de APNs e instalá-lo em um servidor de MDM do iOS.	Não armazenado
O certificado de APNs expira em breve	4136	KLSRV_APN_CERTIFICATE_EXPIRES_SOON	Eventos deste tipo ocorrem quando faltam menos de 14 dias para a expiração do certificado de APNs. Quando o certificado de APNs expirar, você precisará renová-lo manualmente e instalá-lo em um servidor de MDM do iOS. Recomendamos que você agende a renovação do certificado de APNs antes da data de expiração.	Não armazenado
Falha ao enviar a mensagem FCM para o dispositivo móvel	4138	KLSRV_GCM_DEVICE_ERROR	Eventos desse tipo ocorrem quando o Gerenciamento de Dispositivos Móveis está configurado para usar o Firebase Cloud Messaging (FCM) para se conectar a dispositivos móveis gerenciados com um sistema operacional Android e o Servidor FCM não consegue processar algumas das solicitações recebidas do Servidor de Administração. Isso significa que alguns dos dispositivos móveis gerenciados não receberão uma notificação push. Leia o código HTTP nos detalhes da descrição do evento e responda de acordo. Para obter mais informações sobre os códigos HTTP recebidos do Servidor FCM e erros relacionados, consulte a documentação do serviço Firebase (em especial, o capítulo "Códigos de resposta de erro de mensagens downstream").	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Ocorreu um erro de HTTP ao enviar a mensagem FCM para o servidor FCM	4139	KLSRV_GCM_HTTP_ERROR	Eventos desse tipo ocorrem quando o Gerenciamento de Dispositivos Móveis está configurado para usar o Firebase Cloud Messaging (FCM) para se conectar a dispositivos móveis gerenciados com sistema operacional Android e o Servidor FCM responde à solicitação do Servidor de Administração com um código HTTP diferente de 200 (OK). Seguem abaixo as possíveis causas e as respostas apropriadas para o evento: • Problemas no lado do servidor FCM. Leia o código HTTP nos detalhes da descrição do evento e responda de acordo. Para obter mais informações sobre os códigos HTTP recebidos do Servidor FCM e erros relacionados, consulte a documentação do serviço Firebase (em especial, o capítulo "Códigos de resposta de erro de mensagens downstream"). • Problemas no lado do servidor proxy (se estiver usando servidor proxy). Leia o código HTTP nos detalhes da descrição do evento e responda de acordo.	90 dias
Falha ao enviar a mensagem FCM para o servidor FCM	4140	KLSRV_GCM_GENERAL_ERROR	Eventos desse tipo ocorrem devido a erros inesperados no Servidor de Administração ao trabalhar com o protocolo HTTP do Firebase Cloud Messaging. Leia os detalhes na descrição do evento e responda de acordo. Se você não conseguir solucionar o problema sozinho, é recomendável entrar em contato com o Suporte Técnico da Kaspersky.	90 dias
Pouco espaço livre no disco rígido	4105	KLSRV_NO_SPACE_ON_VOLUMES	Eventos deste tipo ocorrem quando o disco rígido do dispositivo onde o Servidor de Administração está instalado fica praticamente sem espaço livre. Libere espaço em disco no dispositivo.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Resta pouco espaço livre no banco de dados do Servidor de Administração	4106	KLSRV_NO_SPACE_IN_DATABASE	Eventos deste tipo ocorrem se o espaço no banco de dados do Servidor de Administração for muito limitado. Se você não remediar a situação, em breve o banco de dados do Servidor de Administração alcançará sua capacidade e o Servidor de Administração não funcionará. A seguir estão as causas deste evento, dependendo do DBMS que estiver usando, e as respostas apropriadas ao evento. Você usa o SQL Server Express Edition DBMS: • Na documentação do SQL Server Express, verifique o limite de tamanho do banco de dados para a versão que estiver usando. Provavelmente, o banco de dados de seu Servidor de Administração está por alcançar seu limite de tamanho. • Limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração. • No banco de dados do Servidor de Administração, há muitos eventos enviados pelo componente Controle de Aplicativos. Você pode alterar as configurações da política do Kaspersky Endpoint Security for Windows relacionadas ao armazenamento de eventos do Controle de Aplicativos no banco de dados do Servidor de Administração. Você usa um DBMS diferente do SQL Server Express Edition: • Não limite o número de eventos a serem armazenados no banco de dados do Servidor de Administração • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração Revise as informações na seleção do DBMS.	90 dias
A conexão com o Servidor de Administração secundário foi interrompida	4116	KLSRV_EV_SLAVE_SRV_DISCONNECTED	Eventos deste tipo ocorrem quando uma conexão com o Servidor de Administração secundário é interrompida. Leia o Log de eventos Kaspersky no dispositivo onde o Servidor de Administração primário está instalado e responda de acordo.	90 dias
A conexão com o Servidor de Administração principal foi interrompida	4118	KLSRV_EV_MASTER_SRV_DISCONNECTED	Eventos deste tipo ocorrem quando uma conexão com o Servidor de Administração primário é interrompida. Leia o Log de eventos Kaspersky no dispositivo onde o Servidor de Administração primário está instalado e responda de acordo.	90 dias
Novas atualizações para os módulos de software da Kaspersky foram registradas	4141	KLSRV_SEAMLESS_UPDATE_REGISTERED	Eventos deste tipo ocorrem quando o Servidor de Administração registra novas atualizações para o software Kaspersky instalado em dispositivos gerenciados que requerem aprovação para instalação. Aprove ou recuse as atualizações usando o Console de Administração ou o Kaspersky Security Center Web Console.	90 dias

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
O limite de eventos no banco de dados foi excedido. A exclusão dos eventos foi iniciada	4145	KLSRV_EVP_DB_TRUNCATING	Eventos deste tipo ocorrem quando a exclusão de eventos antigos do banco de dados do Servidor de Administração começou após a capacidade do banco de dados do Servidor de Administração ter sido alcançada. Você pode responder ao evento nas seguintes maneiras: • Alterar o número máximo de eventos armazenados no banco de dados do Servidor de Administração • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração	Não armazenado
O limite de eventos no banco de dados foi excedido. Os eventos foram excluídos	4146	KLSRV_EVP_DB_TRUNCATED	Eventos deste tipo ocorrem quando a exclusão de eventos antigos do banco de dados do Servidor de Administração começou após a capacidade do banco de dados do Servidor de Administração ter sido alcançada. Você pode responder ao evento nas seguintes maneiras: • Altere o número máximo de eventos armazenados permitidos no banco de dados do Servidor de Administração • Reduza a lista de eventos a serem armazenados no banco de dados do Servidor de Administração	Não armazenado
Falha na emissão automática do certificado		KLSRV_CERTIFICATE_AUTO_ISSUE_ERROR	Esse evento ocorre em caso de erro ao criar um certificado de cliente para um dispositivo móvel (um dispositivo operando sob um protocolo móvel).	90 dias

Eventos informativos do Servidor de Administração

A tabela abaixo mostra os eventos do Servidor de Administração do Kaspersky Security Center com o nível de importância **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Para o Servidor de Administração, é possível também visualizar e configurar a lista de eventos nas propriedades do Servidor de Administração. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Servidor de Administração

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão	Observações
Mais de 90% desta chave de licença foram utilizados	4097	KLSRV_EV_LICENSE_CHECK_90	30 dias	
Novo dispositivo detectado	4100	KLSRV_EVENT_HOSTS_NEW_DETECTED	30 dias	
O dispositivo foi adicionado automaticamente ao grupo	4101	KLSRV_EVENT_HOSTS_NEW_REDIRECTED	30 dias	

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão	Observações
O dispositivo foi removido do grupo: inativo na rede por muito tempo	4104	KLSRV_INVISIBLE_HOSTS_REMOVED	30 dias	
O limite de instalações está prestes a ser excedido (mais de 95% já foram utilizados) para um dos grupos de aplicativos licenciados	4128	KLSRV_INVLICPROD_EXPIRED_SOON	30 dias	
Foram encontrados arquivos para enviar para a Kaspersky para análise	4131	KLSRV_APS_FILE_APPEARED	30 dias	
O ID da Instância FCM foi alterado neste dispositivo móvel	4137	KLSRV_GCM_DEVICE_REGID_CHANGED	30 dias	
As atualizações foram copiadas com êxito para a pasta especificada	4122	KLSRV_UPD_REPL_OK	30 dias	
A conexão com o Servidor de Administração secundário foi estabelecida	4115	KLSRV_EV_SLAVE_SRV_CONNECTED	30 dias	
A conexão com o Servidor de Administração principal foi estabelecida	4117	KLSRV_EV_MASTER_SRV_CONNECTED	30 dias	
Os bancos de dados foram atualizados	4144	KLSRV_UPD_BASES_UPDATED	30 dias	
Auditoria: a conexão com o Servidor de Administração foi estabelecida	4147	KLAUD_EV_SERVERCONNECT	30 dias	Eventos desse tipo ocorrem quando um usuário se conecta ao Servidor de Administração usando o Console de Administração ou o Kaspersky Security Center Web Console. Esses eventos incluem o endereço IP do dispositivo no qual o Console de Administração baseado em MMC ou o Kaspersky Security Center Web Console Server está instalado.
Auditoria: o objeto foi modificado	4148	KLAUD_EV_OBJECTMODIFY	30 dias	Este evento acompanha mudanças nos seguintes objetos: • Grupo de administração • Grupo de segurança • Usuário • Pacote • Tarefa • Política • Servidor • Servidor virtual
Auditoria: o status do objeto foi alterado	4150	KLAUD_EV_TASK_STATE_CHANGED	30 dias	Por exemplo, este evento ocorre quando uma tarefa falha com um erro.

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão	Observações
Auditoria: as configurações do grupo foram modificadas	4149	KLAUD_EV_ADMGROUP_CHANGED	30 dias	
Auditoria: a conexão com o Servidor de Administração foi encerrada	4151	KLAUD_EV_SERVERDISCONNECT	30 dias	
Auditoria: as propriedades do objeto foram modificadas	4152	KLAUD_EV_OBJECTPROPMODIFIED	30 dias	Este evento rastreia as mudanças nas seguintes propriedades: • Usuário • Licença • Servidor • Servidor virtual
Auditoria: as permissões do usuário foram modificadas	4153	KLAUD_EV_OBJECTACLMODIFIED	30 dias	
Auditoria: as chaves de criptografia foram importadas ou exportadas do Servidor de Administração	5100	KLAUD_EV_DPEKEYSEXPORT	30 dias	

Eventos do Agente de Rede

Esta seção contém informações sobre os eventos relativos ao Agente de Rede.

Eventos de falha funcional do Agente de Rede

A tabela abaixo mostra os tipos de eventos do Agente de Rede do Kaspersky Security Center que têm o nível de gravidade **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Descrição	Prazo de armazenamento padrão
Erro de instalação da atualização	7702	KLNAG_EV_PATCH_INSTALL_ERROR	Eventos deste tipo ocorrem se a atualização e correção automática para os componentes do Kaspersky Security Center não teve êxito. O evento não contém atualizações dos aplicativos gerenciados da Kaspersky. Leia a descrição do evento. Um problema do Windows no Servidor de Administração poderá ser o motivo desse evento. Se descrição mencionar qualquer problema da configuração do Windows, solucione o problema.	30 dias
Falha ao instalar a atualização de software de terceiros	7697	KLNAG_EV_3P_PATCH_INSTALL_ERROR	Eventos deste tipo ocorrem se os recursos de Gerenciamento de patches e vulnerabilidades e Gerenciamento de dispositivos móveis estão em uso, e se a atualização do software de terceiro não teve êxito. Verificar se o link para o software de terceiros é válido. Leia a descrição do evento.	30 dias
Falha ao instalar as atualizações do Windows Update	7717	KLNAG_EV_WUA_INSTALL_ERROR	Eventos deste tipo ocorrem se a atualizações do Windows não tiverem êxito. Configurar as atualizações do Windows em uma política de Agente de Rede. Leia a descrição do evento. Procure o erro na Base de Dados de Conhecimento da Microsoft. Entre em contato com o Suporte Técnico da Microsoft se você não conseguir resolver o problema você mesmo.	30 dias

Eventos de aviso do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center que têm o nível de gravidade **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Uma advertência foi retornada durante a instalação da atualização dos módulos de software	7701	KLNAG_EV_PATCH_INSTALL_WARNING	30 dias
A instalação da atualização do software de terceiros foi concluída com uma advertência	7696	KLNAG_EV_3P_PATCH_INSTALL_WARNING	30 dias
A instalação da atualização do software de terceiros foi adiada	7698	KLNAG_EV_3P_PATCH_INSTALL_SLIPPED	30 dias
Ocorreu um incidente	549	GNRL_EV_APP_INCIDENT_OCCURED	30 dias
Proxy da KSN iniciado. Falha ao verificar a disponibilidade da KSN	7718	KSNPROXY_STARTED_CON_CHK_FAILED	30 dias

Eventos informativos do Agente de Rede

A tabela abaixo mostra os eventos do Agente de Rede do Kaspersky Security Center que têm o nível de gravidade **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Agente de Rede

Nome de exibição do tipo de evento	ID de tipo de evento	Tipo de evento	Prazo de armazenamento padrão
A atualização dos módulos de software foi instalada com êxito	7699	KLNAG_EV_PATCH_INSTALLED_SUCCESSFULLY	30 dias
A instalação da atualização dos módulos de software foi iniciada	7700	KLNAG_EV_PATCH_INSTALL_STARTING	30 dias
Aplicativo instalado	7703	KLNAG_EV_INV_APP_INSTALLED	30 dias
Aplicativo desinstalado	7704	KLNAG_EV_INV_APP_UNINSTALLED	30 dias
O aplicativo monitorado foi instalado	7705	KLNAG_EV_INV_OBS_APP_INSTALLED	30 dias
O aplicativo monitorado foi desinstalado	7706	KLNAG_EV_INV_OBS_APP_UNINSTALLED	30 dias
O aplicativo de terceiros foi instalado	7707	KLNAG_EV_INV_CMPTR_APP_INSTALLED	30 dias
Novo dispositivo adicionado	7708	KLNAG_EV_DEVICE_ARRIVAL	30 dias
Dispositivo removido	7709	KLNAG_EV_DEVICE_REMOVE	30 dias
Novo dispositivo detectado	7710	KLNAG_EV_NAC_DEVICE_DISCOVERED	30 dias
O dispositivo foi autorizado	7711	KLNAG_EV_NAC_HOST_AUTHORIZED	30 dias
Windows Desktop Sharing: o arquivo foi lido	7712	KLUSRLOG_EV_FILE_READ	30 dias
Windows Desktop Sharing: o arquivo foi modificado	7713	KLUSRLOG_EV_FILE_MODIFIED	30 dias
Windows Desktop Sharing: aplicativo iniciado	7714	KLUSRLOG_EV_PROCESS_LAUNCHED	30 dias
Windows Desktop Sharing: iniciado	7715	KLUSRLOG_EV_WDS_BEGIN	30 dias
Windows Desktop Sharing: parado	7716	KLUSRLOG_EV_WDS_END	30 dias
A atualização do software de terceiros foi instalada com êxito	7694	KLNAG_EV_3P_PATCH_INSTALLED_SUCCESSFULLY	30 dias
A instalação da atualização de software de terceiros foi iniciada	7695	KLNAG_EV_3P_PATCH_INSTALL_STARTING	30 dias
Proxy da KSN iniciado. A verificação de disponibilidade da KSN foi concluída com êxito	7719	KSNPROXY_STARTED_CON_CHK_OK	30 dias
Proxy da KSN parado	7720	KSNPROXY_STOPPED	30 dias

Eventos do Servidor de MDM do iOS

Esta seção contém informações sobre os eventos relativos ao Servidor de MDM do iOS.

Eventos de falha funcional do Servidor de MDM do iOS

A tabela abaixo mostra os eventos do Servidor de MDM do iOS do Kaspersky Security Center com o nível de gravidade **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Servidor de MDM do iOS

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Falha ao solicitar a lista de perfis	PROFILELIST_COMMAND_FAILED	30 dias
Falha ao instalar o perfil	INSTALLPROFILE_COMMAND_FAILED	30 dias
Falha ao remover o perfil	REMOVEPROFILE_COMMAND_FAILED	30 dias
Falha ao solicitar a lista de perfis de provisionamento	PROVISIONINGPROFILELIST_COMMAND_FAILED	30 dias
Falha ao instalar o perfil de provisionamento	INSTALLPROVISIONINGPROFILE_COMMAND_FAILED	30 dias
Falha ao remover o perfil de provisionamento	REMOVEPROVISIONINGPROFILE_COMMAND_FAILED	30 dias
Falha ao solicitar lista de certificados digitais	CERTIFICATELIST_COMMAND_FAILED	30 dias
Falha ao solicitar a lista de aplicativos instalados	INSTALLEDAPPLICATIONLIST_COMMAND_FAILED	30 dias
Falha em solicitar informações gerais sobre o dispositivo móvel	DEVICEINFORMATION_COMMAND_FAILED	30 dias
Falha ao solicitar informações de segurança	SECURITYINFO_COMMAND_FAILED	30 dias
Falha em bloquear o dispositivo móvel	DEVICELOCK_COMMAND_FAILED	30 dias
Falha ao redefinir a senha	CLEARPASSCODE_COMMAND_FAILED	30 dias
Falha em limpar os dados no dispositivo móvel	ERASEDEVICE_COMMAND_FAILED	30 dias
Falha ao instalar o aplicativo	INSTALLAPPLICATION_COMMAND_FAILED	30 dias
Falha ao definir o código de resgate para o aplicativo	APPLYREDEMPTIONCODE_COMMAND_FAILED	30 dias
Falha ao solicitar a lista de aplicativos gerenciados	MANAGEDAPPLICATIONLIST_COMMAND_FAILED	30 dias
Falha ao remover o aplicativo gerenciado	REMOVEAPPLICATION_COMMAND_FAILED	30 dias
As configurações de roaming foram rejeitadas	SETROAMINGSETTINGS_COMMAND_FAILED	30 dias
Ocorreu um erro na operação do aplicativo	PRODUCT_FAILURE	30 dias
O resultado do comando contém dados inválidos	MALFORMED_COMMAND	30 dias
Falha ao enviar a notificação push	SEND_PUSH_NOTIFICATION_FAILED	30 dias
Falha em enviar o comando	SEND_COMMAND_FAILED	30 dias
Dispositivo não encontrado	DEVICE_NOT_FOUND	30 dias

Eventos de aviso do Servidor de MDM do iOS

A tabela abaixo mostra os eventos do Servidor de MDM do iOS do Kaspersky Security Center com o nível de gravidade **Advertência**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de aviso do Servidor de MDM do iOS

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Uma tentativa de conectar-se um dispositivo móvel bloqueado foi detectada	INACTICE_DEVICE_TRY_CONNECTED	30 dias
O perfil foi removido	MDM_PROFILE_WAS_REMOVED	30 dias
Uma tentativa de reutilizar um certificado cliente foi detectada	CLIENT_CERT_ALREADY_IN_USE	30 dias
Dispositivo inativo detectado	FOUND_INACTIVE_DEVICE	30 dias
Um código de resgate é necessário	NEED_REDEMPTION_CODE	30 dias
Perfil incluído em uma política removida do dispositivo	UMDM_PROFILE_WAS_REMOVED	30 dias

Eventos informativos do Servidor de MDM do iOS

A tabela abaixo mostra os eventos do Servidor de MDM do iOS do Kaspersky Security Center com o nível de gravidade **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Servidor de MDM do iOS

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Novo dispositivo móvel conectado	NEW_DEVICE_CONNECTED	30 dias
A lista de perfis foi solicitada com êxito	PROFILELIST_COMMAND_SUCCESSFULL	30 dias
O perfil foi instalado com êxito	INSTALLPROFILE_COMMAND_SUCCESSFULL	30 dias
O perfil foi removido com êxito	REMOVEPROFILE_COMMAND_SUCCESSFULL	30 dias
A lista de perfis de provisionamento foi solicitada com êxito	PROVISIONINGPROFILELIST_COMMAND_SUCCESSFULL	30 dias
O perfil de Provisionamento foi instalado com êxito	INSTALLPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dias
O perfil de provisionamento foi removido com êxito	REMOVEPROVISIONINGPROFILE_COMMAND_SUCCESSFULL	30 dias
A lista de certificados digitais foi solicitada com êxito	CERTIFICATELIST_COMMAND_SUCCESSFULL	30 dias
A lista de aplicativos instalados foi solicitada com êxito	INSTALLEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dias
As informações gerais sobre o dispositivo móvel foram solicitadas com êxito	DEVICEINFORMATION_COMMAND_SUCCESSFULL	30 dias
As informações de segurança foram solicitadas com êxito	SECURITYINFO_COMMAND_SUCCESSFULL	30 dias
O dispositivo móvel foi bloqueado com êxito	DEVICELOCK_COMMAND_SUCCESSFULL	30 dias
A senha foi redefinida com êxito	CLEARPASSCODE_COMMAND_SUCCESSFULL	30 dias
Os dados foram limpos do dispositivo móvel	ERASEDEVICE_COMMAND_SUCCESSFULL	30 dias
O aplicativo foi instalado com êxito	INSTALLAPPLICATION_COMMAND_SUCCESSFULL	30 dias
O código de resgate para o aplicativo foi definido com êxito	APPLYREDEMPTIONCODE_COMMAND_SUCCESSFULL	30 dias
A lista de aplicativos gerenciados foi solicitada com êxito	MANAGEDAPPLICATIONLIST_COMMAND_SUCCESSFULL	30 dias
O aplicativo gerenciado foi removido com êxito	REMOVEAPPLICATION_COMMAND_SUCCESSFULL	30 dias
As configurações de roaming foram aplicadas com êxito	SETROAMINGSETTINGS_COMMAND_SUCCESSFUL	30 dias

Eventos do Servidor de dispositivos móveis Microsoft Exchange

Esta seção contém informações sobre os eventos relativos a um Servidor de dispositivos móveis do Microsoft Exchange.

Eventos de falha funcional do Servidor de dispositivos móveis Exchange

A tabela abaixo mostra os eventos do Servidor de dispositivos móveis Exchange do Kaspersky Security Center com o nível de gravidade **Falha funcional**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos de falha funcional do Servidor de dispositivos móveis Exchange

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Falha em limpar os dados no dispositivo móvel	WIPE_FAILED	30 dias
Não foi possível excluir as informações sobre a conexão do dispositivo móvel da caixa de correio	DEVICE_REMOVE_FAILED	30 dias
Não é possível aplicar a política ActiveSync à caixa de correio	POLICY_APPLY_FAILED	30 dias
Erro de funcionamento do aplicativo	PRODUCT_FAILURE	30 dias
Falha ao modificar o estado da funcionalidade ActiveSync	CHANGE_ACTIVE_SYNC_STATE_FAILED	30 dias

Eventos informativos do Servidor de dispositivos móveis Exchange

A tabela abaixo mostra os eventos do Servidor de dispositivos móveis Exchange do Kaspersky Security Center com o nível de gravidade **Informações**.

Para cada evento que pode ser gerado por um aplicativo, é possível especificar as configurações de notificação e configurações de armazenamento na guia **Configuração de eventos** na política do aplicativo. Caso queira definir as configurações de notificação para todos os eventos de uma vez, defina as configurações gerais de notificação nas propriedades do Servidor de Administração.

Eventos informativos do Servidor de dispositivos móveis Exchange

Nome de exibição do tipo de evento	Tipo de evento	Prazo de armazenamento padrão
Um novo dispositivo móvel foi conectado	NEW_DEVICE_CONNECTED	30 dias
Os dados foram limpos do dispositivo móvel	WIPE_SUCCESSFULL	30 dias

Bloqueio de eventos frequentes

Esta seção fornece informações sobre como gerenciar e remover o bloqueio de eventos frequentes.

Sobre o bloqueio de eventos frequentes

Um aplicativo gerenciado, por exemplo, Kaspersky Endpoint Security for Windows, instalado em um ou vários dispositivos gerenciados, pode enviar muitos eventos do mesmo tipo ao Servidor de Administração. Receber eventos frequentes pode sobrecarregar o banco de dados do Servidor de Administração e sobrepor-se a outros eventos. O Servidor de Administração começa a bloquear os eventos mais frequentes quando o número de todos os eventos recebidos excede o limite especificado para o banco de dados.

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes. Você não pode bloquear os eventos frequentes ou escolher quais eventos bloquear.

Caso queira saber se um evento está bloqueado, é possível visualizar a lista de notificações ou visualizar se o evento está presente na seção **Bloqueando eventos frequentes** das propriedades do servidor de administração. Se o evento estiver bloqueado, você pode fazer o seguinte:

- Se deseja evitar a substituição do banco de dados, pode continuar bloqueando o recebimento desse tipo de evento.
- Se deseja, por exemplo, localizar o motivo do envio de eventos frequentes ao Servidor de Administração, pode desbloquear os eventos frequentes e continuar recebendo os eventos deste tipo de qualquer maneira.
- Se quiser continuar recebendo os eventos frequentes até que sejam bloqueados novamente, pode remover o bloqueio dos eventos frequentes.

Gerenciando o bloqueio de eventos frequentes

O Servidor de Administração bloqueia o recebimento automático de eventos frequentes, mas você pode desbloquear e continuar a recebê-los. Você também pode bloquear o recebimento de eventos frequentes que desbloqueou anteriormente.

Para gerenciar o bloqueio de eventos frequentes:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Bloqueando eventos frequentes**.
3. Na seção **Bloqueando eventos frequentes**:
   - Se deseja desbloquear o recebimento de eventos frequentes:
     a. Selecione os eventos frequentes que deseja desbloquear e clique no botão **Excluir**.
     b. Clique no botão **Salvar**.
   - Se deseja bloquear o recebimento de eventos frequentes:
     a. Selecione os eventos frequentes que deseja bloquear e clique no botão **Bloquear**.
     b. Clique no botão **Salvar**.

O Servidor de Administração recebe os eventos frequentes desbloqueados e não recebe os eventos frequentes bloqueados.

Removendo o bloqueio de eventos frequentes

Você pode remover o bloqueio de eventos frequentes e começar a recebê-los até que o Servidor de Administração os bloqueie novamente.

Para remover o bloqueio de eventos frequentes:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.

2. Na guia **Geral**, selecione a seção **Bloqueando eventos frequentes**.

3. Na seção **Bloqueando eventos frequentes**, selecione os tipos de eventos frequentes para os quais deseja remover o bloqueio.

4. Clique no botão **Remover do bloqueio**.

O evento frequente é removido da lista de eventos frequentes. O Servidor de Administração receberá eventos deste tipo.

Recebendo eventos do Kaspersky Security for Microsoft Exchange Servers

As informações sobre os eventos durante a operação de aplicativos gerenciados, como o Kaspersky Endpoint Security for Windows, são transferidas de dispositivos gerenciados e registradas no banco de dados do Servidor de Administração. Por padrão, os eventos do Kaspersky Security for Microsoft Exchange Servers versão 9.0 MR6 e anteriores não são registrados no banco de dados do Servidor de Administração. Caso o Kaspersky Security for Microsoft Exchange Servers versão 9.0 MR6 e anterior esteja instalado nos dispositivos gerenciados na sua organização e caso queira receber os eventos deste aplicativo, ative o registro de eventos para o aplicativo com o uso do utilitário klscflag.

Para habilitar o registro de eventos para o Kaspersky Security for Microsoft Exchange Servers:

1. No dispositivo do Servidor de Administração, execute o prompt de comando do Windows em uma conta com direitos de administrador.

2. Altere o diretório atual para a pasta de instalação do Kaspersky Security Center (geralmente, C:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center).

3. Execute um dos seguintes comandos:

   - Para o Servidor de Administração instalado em um cluster de failover do Windows Server:

     ```
     klscflag.exe --stp cluster -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Para o Servidor de Administração instalando em um nó de cluster de failover da Kaspersky Security Center:

     ```
     klscflag.exe --stp klfoc -fset -pv klserver -n
     KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d -v 0
     ```

   - Para o Servidor de Administração que não está funcionando em um cluster:

     ```
     klscflag.exe -fset -pv klserver -n KLSRV_EVP_ENABLE_HOST_EVENT_BODY_VALIDATION -t d
     -v 0
     ```

O registro de eventos do Kaspersky Security for Microsoft Exchange Servers está ativado.

Para o Kaspersky Security for Microsoft Exchange Servers, não é possível definir o prazo de armazenamento para os eventos ou selecionar quais eventos devem ser salvos no repositório do Servidor de Administração. É possível definir o número máximo de eventos que podem ser salvos no repositório. A configuração é aplicada aos eventos recebidos de todos os aplicativos da Kaspersky.

Notificações e status do dispositivo

Esta seção contém informações sobre como visualizar notificações, configurar a entrega de notificações, usar os status do dispositivo e habilitar a alteração de status do dispositivo.

Usar as notificações

As Notificações alertam sobre os eventos e ajudam a agilizar as respostas a estes eventos executando ações recomendadas ou ações que você considera apropriadas.

Dependendo do método de notificação selecionado, os seguintes tipos de notificações estão disponíveis:

- Notificações na tela
- Notificações por SMS
- Notificações por e-mail
- Notificações por arquivo executável ou script

Notificações na tela

As notificações na tela alertam para eventos agrupados por níveis de importância (*Crítico*, *Aviso* e *Informativo*).

A notificação na tela pode ter um de dois status:

- *Revisado*. Significa que você executou a ação recomendada para a notificação ou atribuiu esse status da notificação manualmente.
- *Não Revisado*. Significa que você não executou a ação recomendada para a notificação ou não atribuiu esse status da notificação manualmente.

Por padrão, a lista de notificações inclui notificações no status *Não Revisado*.

Você pode monitorar a rede da sua organização visualizando notificações na tela e dando resposta a elas em tempo real.

Notificações por e-mail, por SMS e por arquivo executável ou um script

O Kaspersky Security Center oferece a capacidade de controlar a rede da sua organização enviando notificações sobre qualquer evento que você considera importante. Para qualquer evento, você pode configurar notificações por e-mail, SMS ou executando um arquivo executável ou um script.

Para receber notificações por e-mail ou SMS, você pode decidir a sua resposta para um evento. Essa resposta deve ser a mais apropriada para a rede da sua organização. Executando um arquivo executável ou um script, você predefine uma resposta para um evento. Você também pode considerar a execução de um arquivo executável ou um script como uma resposta primária para um evento. Após a execução do arquivo executável, você pode tomar outras medidas para responder ao evento.

Visualização de notificações na tela

Você pode visualizar notificações na tela de três maneiras:

- Na seção **Monitoramento e relatórios** → **Notificações**. Aqui, você pode exibir notificações relacionadas a categorias predefinidas.
- Em uma janela separada que pode ser aberta, não importa qual seção está sendo usada no momento. Neste caso, você pode marcar notificações como revisadas.
- No widget **Notificações por nível de gravidade selecionado** na seção **Monitoramento e relatórios** → **Painel**. No widget, você pode exibir apenas notificações de eventos que estão nos níveis de importância *Crítico* e *Aviso*.

Você pode realizar ações, por exemplo, responder a um evento.

Para visualizar notificações de categorias predefinidas:

1. No menu principal, vá para **Monitoramento e relatórios** → **Notificações**.

   A categoria **Todas as notificações** é selecionada no painel esquerdo, e no painel direito todas as notificações são exibidas.

2. No painel esquerdo, selecione uma das categorias:

   - **Implementação**
   - **Dispositivos**
   - **Proteção**
   - **Atualizações** (esta inclui notificações sobre aplicativos Kaspersky disponíveis para download e notificações sobre atualizações de banco de dados de antivírus que foram baixadas)
   - **Prevenção de Exploit**
   - **Servidor de Administração** (esta inclui eventos relacionados apenas ao Servidor de Administração)
   - **Links úteis** (esta inclui links para recursos da Kaspersky, por exemplo, Suporte Técnico da Kaspersky, fórum da Kaspersky, página de renovação de licença ou a Enciclopédia de TI da Kaspersky)
   - **Notícias da Kaspersky** (esta inclui informações sobre versões de aplicativos Kaspersky)

Uma lista de notificações da categoria selecionada é exibida. A lista contém o seguinte:

- Ícone relacionado ao tópico da notificação: implementação (), proteção (), atualizações (), gerenciamento de dispositivo (), Prevenção de Exploits (), Servidor de Administração ().
- Nível de importância da notificação. As notificações dos seguintes níveis de importância são exibidas: **Notificações críticas** (), **Notificações de advertência** (), **Notificações de informação**. As notificações na lista são agrupadas por níveis de importância.
- **Notificação**. Contém uma descrição da notificação.
- **Ação**. Contém um link para uma ação rápida que recomendamos que você execute. Por exemplo, clicando neste link, você pode prosseguir para o repositório e instalar aplicativos de segurança em dispositivos ou visualizar uma lista de dispositivos ou uma lista de eventos. Depois que executar a ação recomendada para a notificação, essa notificação será atribuída ao status *Revisado*.
- **Status registrado**. Contém o número de dias ou horas que se passaram a partir do momento em que a notificação foi registrada no Servidor de Administração.

Para exibir notificações na tela em uma janela separada pelo nível de importância:

1. No canto superior direito do Kaspersky Security Center Web Console, clique no ícone sinalizador ().

   Caso o ícone sinalizador tenha um ponto vermelho, isso significa que há notificações que não foram analisadas.

   Uma janela é exibida listando as notificações. Por padrão, a guia **Todas as notificações** está selecionada, e as notificações estão agrupadas pelo nível de importância: *Crítico*, *Aviso* e *Informativo*.

2. Selecione a guia **Sistema**.

   A lista de notificações de níveis de importância *Crítico* () e *Advertência* () é exibida. A lista de notificações inclui o seguinte:

   - Marcador de cores. As notificações críticas estão marcadas em vermelho. As notificações de aviso estão marcadas em amarelo.
   - Ícone que indica o tópico da notificação: implementação (), proteção (), atualizações (), gerenciamento de dispositivo (), Prevenção de Exploits (), Servidor de Administração ().
   - Descrição da notificação.
   - Ícone sinalizador. O ícone sinalizador ficará cinza caso as notificações tenham recebido o status *Não Analisado*. Quando o ícone sinalizador cinza é selecionado e o status *Analisado* é atribuído para uma notificação, a cor do ícone muda para branca.
   - Link para a ação recomendada. Quando você executa a ação recomendada depois de clicar no link, a notificação ganha o status *Revisado*.
   - O número de dias que se passaram desde a data quando a notificação foi registrada no Servidor de Administração.

3. Selecione a guia **Mais**.

   A lista de notificações de nível de importância *Informativo* é exibida.

   A organização da lista é a mesma da lista na guia **Sistema** (veja a descrição acima). A única diferença é a ausência de um marcador de cores.

Você pode filtrar notificações pelo intervalo de datas quando elas tiverem sido registradas no Servidor de Administração. Use a caixa de seleção **Mostrar filtro** para gerenciar o filtro.

Para exibir notificações na tela no widget:

1. Na seção **Painel**, selecione **Adicionar ou restaurar widget da Web**.

2. Na janela exibida, clique na categoria **Outro**, selecione o widget **Notificações por nível de gravidade selecionado** e clique em Adicionar.

   O widget agora aparece na guia **Painel**. Por padrão, as notificações do nível de importância *Crítico* são exibidas no widget.

   Você pode clicar no botão **Configurações** no widget e alterar as configurações de widget para exibir notificações do nível de importância *Aviso*. Ou você pode adicionar outro widget: **Notificações por nível de gravidade selecionado**, com um nível de importância *Aviso*.

   A lista de notificações no widget é limitada pelo seu tamanho e inclui duas notificações. Essas duas notificações estão relacionadas aos eventos mais recentes.

A lista de notificações no widget inclui o seguinte:

- Ícone relacionado ao tópico da notificação: implementação ( ), proteção ( ), atualizações ( ), gerenciamento de dispositivo ( ), Prevenção de Exploits ( ), Servidor de Administração ( ).

- Descrição da notificação com um link para a ação recomendada. Quando você executa a ação recomendada depois de clicar no link, a notificação ganha o status *Revisado*.

- O número de dias ou o número de horas que se passaram desde a data quando a notificação foi registrada no Servidor de Administração.

- Link para outras notificações. Clicando nesse link, você é transferido para a visualização de notificações na seção **Notificações** em **Monitoramento e relatórios**.

Sobre os status do dispositivo

O Kaspersky Security Center atribui um status a cada dispositivo gerenciado. O status específico depende se as condições definidas pelo usuário são atendidas. Em alguns casos, ao atribuir um status a um dispositivo, o Kaspersky Security Center leva em consideração o sinalizador de visibilidade do dispositivo na rede (consulte a tabela abaixo). Se o Kaspersky Security Center não encontrar um dispositivo na rede dentro de duas horas, o sinalizador de visibilidade do dispositivo será definido como *Não visível*.

Os status são os seguintes:

- *Crítico* ou *Crítico/Visível*

- *Advertência* ou *Advertência/Visível*

- *OK* ou *OK/Visível*

A tabela abaixo lista as condições padrão que devem ser atendidas para atribuir o status *Crítico* ou *Advertência* a um dispositivo, com todos os valores possíveis.

Condições para atribuir um status a um dispositivo

Condição	Descrição da condição	Valores disponíveis
O aplicativo de segurança não está instalado	O Agente de Rede é instalado no dispositivo, mas um aplicativo de segurança não é instalado.	• O botão de alternar é ativado. • O botão de alternar é desativado.
Excesso de vírus detectados	Alguns vírus foram encontrados no dispositivo por uma tarefa de detecção de vírus, por exemplo, a tarefa de *verificação de malwares*, e o número de vírus encontrados excede o valor especificado.	Mais de 0.
O nível da proteção em tempo real é diferente do nível definido pelo administrador	O dispositivo está visível na rede, mas o nível de proteção em tempo real difere do nível definido (na condição) pelo administrador para o status do dispositivo.	• Parado. • Pausada. • Executando.
A verificação de vírus não é executada há muito tempo	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas nem a tarefa de *verificação de malware* nem a verificação local foram executadas dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 7 dias ou antes.	Mais de 1 dia.
Os bancos de dados estão desatualizados	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas os bancos de dados antivírus não foram atualizados neste dispositivo dentro do intervalo de tempo especificado. A condição é aplicável somente aos dispositivos que foram adicionados ao banco de dados do Servidor de Administração há 1 dia ou antes.	Mais de 1 dia.
Não conectado há muito tempo	O Agente de Rede está instalado no dispositivo, mas o dispositivo não se conectou a um Servidor de Administração dentro do intervalo de tempo especificado, porque o dispositivo estava desativado.	Mais de 1 dia.
Foram detectadas ameaças ativas	O número de objetos não processados na pasta **Ameaças ativas** excede o valor especificado.	Mais de 0 itens.
A reinicialização é necessária	O dispositivo está visível na rede, mas um aplicativo requer o reinício do dispositivo por mais tempo do que o intervalo de tempo especificado e para um dos motivos selecionados.	Mais de 0 minuto.
Aplicativos incompatíveis estão instalados	O dispositivo está visível na rede, mas o inventário de software executado pelo Agente de Rede detectou aplicativos incompatíveis instalados no dispositivo.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Foram detectadas vulnerabilidades de software	O dispositivo está visível na rede, e o Agente de Rede está instalado no dispositivo, mas a tarefa *Encontrar vulnerabilidades e atualizações necessárias* detectou vulnerabilidades com o nível de gravidade especificado nos aplicativos instalados no dispositivo.	• Crítico. • Alto. • Médio. • Ignorar se a vulnerabilidade não puder ser corrigida. • Ignorar se uma atualização for atribuída para instalação.
A licença expirou	O dispositivo está visível na rede, mas a licença expirou.	• O botão de alternar é desativado. • O botão de alternar é ativado.
A licença expira em breve	O dispositivo está visível na rede, mas a licença expirará no dispositivo em tempo menor que o número especificado de dias.	Valor de dias inferior a 0.
A verificação de atualizações do Windows Update não é executada há muito tempo	O dispositivo está visível na rede, mas a tarefa *executar a sincronização com o Windows Update* não foi executada dentro do intervalo de tempo especificado.	Mais de 1 dia.

Condição	Descrição da condição	Valores disponíveis
Status de criptografia inválido	O Agente de Rede está instalado no dispositivo, mas o resultado da criptografia de dispositivo é igual ao valor especificado.	• Não está em conformidade com a política devido à recusa do usuário (somente para dispositivos externos). • Não está em conformidade com a política devido a um erro. • Reiniciar é necessário ao aplicar a política. • Nenhuma política de criptografia está especificada. • Sem suporte. • Ao aplicar a política.
As configurações do dispositivo móvel não estão em conformidade com a política	As configurações do dispositivo móvel são diferentes das especificadas na política do Kaspersky Endpoint Security for Android durante a verificação das regras de conformidade.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Incidentes não processados detectados	Alguns incidentes não processados foram encontrados no dispositivo. Os incidentes podem ser criados automaticamente, através de aplicativos da Kaspersky gerenciados instalados no dispositivo cliente, ou manualmente pelo administrador.	• O botão de alternar é desativado. • O botão de alternar é ativado.
Status do dispositivo definido pelo aplicativo	O status do dispositivo é definido pelo aplicativo gerenciado.	• O botão de alternar é desativado. • O botão de alternar é ativado.
O dispositivo está com espaço em disco insuficiente	O espaço livre em disco no dispositivo é menor do que o valor especificado ou o dispositivo não pôde ser sincronizado com o Servidor de Administração. O status *Crítico* ou *Advertência* é alterado para o status *OK* quando o dispositivo é sincronizado com sucesso com o Servidor de Administração, e o espaço livre no dispositivo é maior que ou igual ao valor especificado.	Mais de 0 MB.
O dispositivo está sem gerenciamento	Durante a descoberta de dispositivos, o dispositivo foi reconhecido como visível na rede, mas houve falha em mais de três tentativas de sincronizar com o Servidor de Administração.	• O botão de alternar é desativado. • O botão de alternar é ativado.
A proteção está desativada	O dispositivo é visível na rede, mas o aplicativo de segurança no dispositivo foi desativado por um tempo mais longo do que o intervalo de tempo especificado. Nesse caso, o estado do aplicativo de segurança é *interrompido* ou *com falha* e diferente de: *iniciando*, *em execução* ou *suspenso*.	Mais de 0 minuto.
O aplicativo de segurança não está em execução	O dispositivo está visível na rede, e um aplicativo de segurança está instalado no dispositivo, mas não está em execução.	• O botão de alternar é desativado. • O botão de alternar é ativado.

O Kaspersky Security Center lhe permite definir a troca automática do status de um dispositivo em um grupo de administração quando as condições especificadas forem atendida. Quando as condições especificadas forem atendidas, ao dispositivo cliente é atribuído um dos seguintes status: *Crítico* ou *Aviso*. Quando as condições especificadas não são atendidas, o dispositivo cliente recebe o status *OK*.

Diferentes status poderão corresponder a diferentes valores de uma condição. Por exemplo, se por padrão a condição **Os bancos de dados estão desatualizados** possuir o valor **Mais de 3 dias**, o dispositivo cliente recebe o status *Advertência*. Se o valor for **Mais de 7 dias**, é atribuído o status *Crítico*.

Se você atualizar o Kaspersky Security Center da versão anterior, os valores do **Os bancos de dados estão desatualizados** condição para atribuir o status *Crítico* ou *Advertência* não mudam.

Quando o Kaspersky Security Center atribui um status a um dispositivo, para algumas condições (consulte a coluna Descrição da condição), o sinalizador de visibilidade é levado em consideração. Por exemplo, se um dispositivo gerenciado recebeu o status *Crítico* porque a condição Os bancos de dados estão desatualizados foi atendida e, mais tarde, o sinalizador de visibilidade foi definido para o dispositivo, então o dispositivo recebe o status *OK*.

Configurar a alternância dos status do dispositivo

Você pode alterar as condições para atribuir o status *Crítico* ou *Advertência* para um dispositivo.

Para ativar a alteração do status do dispositivo para Crítico:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Crítico**.
5. No painel direito, na seção **Se especificados, definir como Crítico**, ative a condição para alterar o status de um dispositivo para *Crítico*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.

9. Clique em **OK**.

Quando condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Crítico*.

Para ativar a alteração do status do dispositivo para Advertência:

1. No menu principal, vá para **Dispositivos** → **Hierarquia de grupos**.
2. Na lista de grupos que se abre, clique no link com o nome de um grupo para o qual você deseja alternar os status do dispositivo.
3. Na janela de propriedades que se abre, clique na guia **Status do dispositivo**.
4. No painel esquerdo, selecione **Advertência**.

5. No painel direito, na seção **Se especificados, definir como Advertência**, ative a condição para alterar o status de um dispositivo para *Advertência*.

   No entanto, é possível alterar as configurações que não estão bloqueadas na política principal.

6. Selecione o botão de seleção ao lado da condição na lista.
7. No canto superior esquerdo, clique no botão **Editar**.
8. Defina o valor necessário para a condição selecionada.

   Os valores não podem ser definidos e para cada condição.

9. Clique em **OK**.

Quando as condições especificadas são atendidas, o dispositivo gerenciado recebe o status *Advertência*.

Configurar a entrega de notificações

Você pode configurar a notificação sobre eventos que ocorrem no Kaspersky Security Center. Dependendo do método de notificação selecionado, os seguintes tipos de notificações estão disponíveis:

- E-mail – Sempre que ocorre um evento, Kaspersky Security Center envia uma notificação para os endereços de e-mail especificados.
- SMS – Sempre que ocorre um evento, Kaspersky Security Center envia uma notificação para os números de telefone especificados.
- Arquivo executável – sempre que ocorre um evento, o arquivo executável é executado no Servidor de Administração.

Para configurar a entrega de notificação de eventos que ocorrem no Kaspersky Security Center:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela de propriedades do Servidor de Administração é exibida com a guia **Geral** selecionada.

2. Clique na seção **Notificação** e, no painel direito, selecione a guia do método de notificação desejado:

   - **E-mail**

A guia **E-mail** permite-lhe configurar a notificação do evento por e-mail.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome da rede Windows (nome NetBIOS) do dispositivo
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Se você ativar a opção **Usar consulta de DNS MX**, pode usar vários registros MX dos endereços IP para o mesmo nome DNS do servidor SMTP. O mesmo nome DNS pode ter vários registros de MX com valores diferentes de prioridade de recebimento de mensagens de e-mail. O Servidor de Administração tenta enviar notificações por e-mail ao servidor SMTP em ordem crescente de prioridade dos registros MX.

Se você ativar **Usar consulta de DNS MX** e não ativar o uso de configurações TLS, recomendamos que use as configurações DNSSEC em seu dispositivo de servidor como uma medida adicional de proteção para o envio de notificações por e-mail.

Se você ativar a opção **Usar a autenticação ESMTP**, pode especificar as configurações de autenticação ESMTP nos campos **Nome do usuário** e **Senha**. Por padrão, a opção estiver desativada, e as configurações da autenticação ESMTP não estão disponíveis.

Você pode especificar as configurações de TLS de conexão com um servidor SMTP:

- **Não usar TLS**

Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.

- **Usar TLS se compatível com servidor SMTP**

Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.

- **Sempre usar TLS e verificar a validade do certificado do servidor**

Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se você selecionar o valor **Sempre usar TLS e verificar a validade do certificado do servidor**, pode especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar certificados para uma conexão TLS clicando no link **Especificar certificados**:

- Procurar por um arquivo de certificado do servidor SMTP:

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

- Procurar um arquivo de certificado de cliente:

Você pode usar um certificado que recebeu de qualquer fonte, por exemplo, de qualquer autoridade de certificação confiável. Você deve especificar o certificado e sua chave privada usando um dos seguintes tipos de certificado:

- Certificado X-509:

Você deve especificar um arquivo com o certificado e um arquivo com a chave privada. Ambos os arquivos não dependem um do outro e a ordem de carregamento dos arquivos não é significativa. Quando os dois arquivos são carregados, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

- Contêiner pkcs12:

Você deve carregar um único arquivo que contenha o certificado e sua chave privada. Quando o arquivo for carregado, você deve especificar a senha para decodificar a chave privada. A senha pode ter um valor vazio se a chave privada não estiver codificada.

No campo **Assunto**, especifique o assunto do e-mail. Você pode deixar este campo vazio.

Na lista suspensa **Modelo de assunto**, selecione o modelo do seu assunto. Uma variável determinada pelo modelo selecionado é colocada automaticamente no campo **Assunto**. Você pode criar um assunto de e-mail selecionando vários modelos de assunto.

No campo **Endereço de e-mail do remetente**, especifique o endereço de e-mail do remetente. Se você deixar este campo vazio, por padrão, o endereço do destinatário é usado. Não é recomendável usar endereços de e-mail fictícios.

O campo **Mensagem de notificação** contém o texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto inclui parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio. Você pode editar o texto da mensagem adicionando outros parâmetros substitutos com detalhes mais relevantes sobre o evento.

> Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clicar no link **Configurar limite numérico de notificações** permite-lhe especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

Clicar no botão **Enviar mensagem de teste** permite verificar se você configurou as notificações apropriadamente: o aplicativo envia uma notificação de teste aos endereços de e-mail que você especificou.

- SMS

A guia **SMS** permite-lhe configurar a transmissão de notificações por SMS de vários eventos para um telefone celular. As mensagens SMS são enviadas por meio de um gateway de correio.

No campo **Servidores SMTP**, especifique endereços de servidor de correio, separando-os com ponto-e-vírgula. Você pode usar os seguintes parâmetros:

- Endereço IPv4 ou IPv6
- Nome da rede Windows (nome NetBIOS) do dispositivo
- Nome de DNS do servidor SMTP

No campo **Porta do servidor SMTP**, especifique o número de uma porta de comunicação do servidor SMTP. O número da porta padrão é 25.

Caso a opção **Usar a autenticação ESMTP** seja ativada, será possível especificar as configurações de autenticação ESMTP nos campos **Nome do usuário** e **Senha**. Por padrão, a opção estiver desativada, e as configurações da autenticação ESMTP não estão disponíveis.

Você pode especificar as configurações de TLS de conexão com um servidor SMTP:

- **Não usar TLS**

Você pode selecionar esta opção se deseja desativar a criptografia de mensagens de e-mail.

- **Usar TLS se compatível com servidor SMTP**

Você pode selecionar esta opção se quiser usar uma conexão TLS com um servidor SMTP. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração conecta o servidor SMTP sem usar TLS.

- **Sempre usar TLS e verificar a validade do certificado do servidor**

Você pode selecionar esta opção se quiser usar as configurações de autenticação TLS. Se o servidor SMTP não for compatível com TLS, o Servidor de Administração não poderá conectar o servidor SMTP.

Recomendamos usar esta opção para melhor proteção da conexão com um servidor SMTP. Se você selecionar esta opção, poderá definir as configurações de autenticação para uma conexão TLS.

Se você selecionar o valor **Sempre usar TLS e verificar a validade do certificado do servidor**, pode especificar um certificado para autenticação do servidor SMTP e escolher se deseja ativar a comunicação por meio de qualquer versão de TLS ou apenas por meio de TLS 1.2 ou versões posteriores. Além disso, você pode especificar um certificado para autenticação do cliente no servidor SMTP.

Você pode especificar o arquivo de certificado do servidor SMTP clicando no link **Especificar certificados**:

Você pode receber um arquivo com a lista de certificados de uma autoridade de certificação confiável e carregá-lo para o Servidor de Administração. O Kaspersky Security Center verifica se o certificado do servidor de um servidor SMTP também está assinado por uma autoridade de certificação confiável. O Kaspersky Security Center não pode se conectar ao servidor SMTP se o certificado do servidor do servidor SMTP não foi recebido de uma autoridade de certificação confiável.

No campo **Destinatários (endereços de e-mail)**, especifique os endereços de e-mail aos quais o aplicativo enviará as notificações. Você pode especificar múltiplos endereços neste campo separando-os com o ponto-e-vírgula. As notificações serão entregues aos números de telefone associados aos endereços de e-mail especificados.

No campo **Assunto**, especifique o assunto do e-mail.

Na lista suspensa **Modelo de assunto**, selecione o modelo do seu assunto. Uma variável segundo o modelo selecionado é inserida no campo **Assunto**. Você pode criar um assunto de e-mail selecionando vários modelos de assunto.

No campo **Endereço de e-mail do remetente: se essa configuração não for especificada, o endereço do destinatário será usado em vez disso. Aviso: não é recomendável usar um endereço de e-mail fictício**, especifique o endereço de e-mail do remetente. Se você deixar este campo vazio, por padrão, o endereço do destinatário é usado. Não é recomendável usar endereços de e-mail fictícios.

No campo **Números de telefone dos destinatários de mensagens SMS**, especifique os números de celular dos destinatários da notificação de SMS.

O campo **Mensagem de notificação**, especifique um texto padrão com informações sobre o evento que o aplicativo envia quando ocorrer um evento. Este texto pode incluir parâmetros substitutos, como o nome do evento, nome do dispositivo e nome do domínio.

Se o texto de notificação contiver um sinal de %, você tem de especificá-lo duas vezes em uma linha para permitir o envio da mensagem. Por exemplo, "A carga de CPU é de 100%%".

Clique no link **Configurar limite numérico de notificações** para especificar a quantidade máxima de notificações que o aplicativo pode enviar ao longo do intervalo de tempo especificado.

Clique em **Enviar mensagem de teste** para verificar se você configurou as notificações adequadamente: o aplicativo envia uma notificação de teste ao destinatário especificado.

- **Arquivo executável a ser executado**

  Se este método de notificação estiver selecionado, no campo de entrada, você pode especificar o aplicativo que será iniciado quando ocorre um evento.

  No campo **O arquivo executável que será executado no Servidor de Administração quando um evento ocorrer**, especifique a pasta e o nome do arquivo a ser executado. Antes de especificar o arquivo, prepare-o e especifique os espaços reservados que definem os detalhes do evento a serem enviados na mensagem de notificação. A pasta e o arquivo especificados devem estar localizados no Servidor de Administração.

  Clicar no link **Configurar limite numérico de notificações** permite-lhe especificar o número máximo de notificações que o aplicativo pode enviar durante o intervalo de tempo especificado.

3. Na guia, defina as configurações de notificação.

4. Clique no botão **OK** para fechar a janela Propriedades do Servidor de Administração.

   As configurações de entrega de notificação salvas são aplicadas a todos os eventos que ocorrem no Kaspersky Security Center.

Você pode ignorar as configurações de entrega de notificações para certos eventos na seção **Configuração de eventos** das configurações do Servidor de Administração, de uma política ou de um aplicativo.

Notificações de evento exibidas executando um arquivo executável

O Kaspersky Security Center pode notificar o administrador sobre os eventos nos dispositivos cliente, executando um arquivo executável. O arquivo executável deve conter outro arquivo executável com marcadores de posição do evento para enviar ao administrador (consulte a tabela abaixo).

Marcadores de posição para descrever um evento

Marcador de posição	Descrição do marcador de posição
%SEVERITY%	Gravidade do evento. Valores possíveis: • **Informações** • **Advertência** • **Erro** • **Crítico**
%COMPUTER%	Nome do dispositivo onde ocorreu o evento. O comprimento máximo do nome do dispositivo é de 256 caracteres.
%DOMAIN%	Nome de domínio do dispositivo onde o evento ocorreu.
%EVENT%	Nome do tipo de evento. O comprimento máximo do nome do tipo de evento é de 50 caracteres.
%DESCR%	Descrição de evento. O comprimento máximo da descrição é de mil caracteres.
%RISE_TIME%	Tempo de criação do evento.
%KLCSAK_EVENT_TASK_DISPLAY_NAME%	Nome da tarefa. O comprimento máximo do nome da tarefa é de 100 caracteres.
%KL_PRODUCT%	Nome do aplicativo.
%KL_VERSION%	Número da versão do aplicativo.
%KLCSAK_EVENT_SEVERITY_NUM%	Número da gravidade do evento. Valores possíveis: • 1 - **Informações** • 2 - **Advertência** • 3 - **Erro** • 4 - **Crítico**
%HOST_IP%	Endereço IP do dispositivo onde o evento ocorreu.
%HOST_CONN_IP%	Endereço IP da conexão do dispositivo onde o evento ocorreu.

Exemplo:
As notificações de eventos são enviadas através de um arquivo executável (como script1.bat) dentro do qual outro arquivo executável (como script2.bat) com o marcador de posição %COMPUTER% é executado. Quando um evento ocorrer, o arquivo script1.bat é executado no dispositivo do administrador, o qual, por sua vez, executa o arquivo script2.bat com o marcador de posição %COMPUTER%. O administrador recebe o nome do dispositivo no qual o evento ocorreu.

Novidades da Kaspersky

Esta seção descreve como usar, configurar e desativar o recebimento de Novidades da Kaspersky.

Sobre as Novidades Kaspersky

A seção Novidades Kaspersky (**Monitoramento e relatórios → Novidades Kaspersky**) apresenta as últimas novidades sobre a sua versão do Kaspersky Security Center e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. O Kaspersky Security Center atualiza periodicamente as informações da seção, removendo informações antigas e adicionando novas.

O Kaspersky Security Center mostra apenas os anúncios da Kaspersky relacionados ao Servidor de Administração conectado atualmente e aos aplicativos Kaspersky instalados nos dispositivos gerenciados deste Servidor de Administração. Os anúncios são mostrados individualmente para qualquer tipo de Servidor de Administração, seja principal, secundário ou virtual.

O Servidor de Administração deve ter uma conexão com a internet para receber os informativos da Kaspersky.

Os informativos incluem informações dos seguintes tipos:

- Comunicados relacionados à segurança

  Os informativos relacionados à segurança têm como objetivo manter os aplicativos da Kaspersky instalados em sua rede atualizados e totalmente funcionais. Os informativos podem incluir informações sobre atualizações críticas para aplicativos da Kaspersky, correções para vulnerabilidades encontradas e maneiras de corrigir outros problemas em aplicativos da Kaspersky. Informativos relacionados à segurança são ativados por padrão. Se não deseja receber informações sobre novidades da Kaspersky, pode desativar este recurso.

  Para mostrar a você as informações que correspondem à sua configuração de proteção de rede, o Kaspersky Security Center envia dados para os servidores em nuvem da Kaspersky e recebe apenas os informativos relacionados aos aplicativos Kaspersky instalados na rede. O conjunto de dados que pode ser enviado aos servidores é descrito no Contrato de Licença do Usuário Final aceito por você ao instalar o Servidor de Administração do Kaspersky Security Center.

- Informativos de marketing

  Informativos de marketing incluem informações sobre ofertas especiais para os aplicativos da Kaspersky, anúncios e notícias da Kaspersky. Informativos de marketing estão desativados por padrão. Você recebe esse tipo de informativo apenas se ativou a Kaspersky Security Network (KSN). Você pode desativar os informativos de marketing desativando a KSN.

  Para que você visualize apenas informações relevantes que podem ser úteis na proteção de seus dispositivos de rede e em suas tarefas diárias, o Kaspersky Security Center envia dados para os servidores Kaspersky na nuvem e coleta os informativos apropriados. O conjunto de dados que pode ser enviado aos servidores é descrito na seção Dados Processados do Declaração da KSN.

As novas informações são divididas nas seguintes categorias, de acordo com a importância:

1. Informações críticas
2. Notícias importantes
3. Advertência
4. Informação

Quando as novas informações são exibidas na seção Novidades Kaspersky, o Kaspersky Security Center Web Console exibe um rótulo com uma notificação correspondente ao nível de importância da informação. Você pode clicar no rótulo para ver a notícia na seção Novidades Kaspersky.

Você pode especificar as configurações de Novidades Kaspersky, incluindo as categorias de informações que deseja receber e onde exibir o rótulo de notificação.

Especificando configurações para receber as Novidades Kaspersky

Na seção Novidades Kaspersky, você pode especificar as configurações de Novidades Kaspersky, incluindo as categorias de notícias que deseja receber e onde exibir o rótulo de notificação.

Para desativar o recebimento das Novidades Kaspersky:

1. No menu principal, vá para **Monitoramento e relatórios → Novidades Kaspersky**.
2. Clique no link **Configurações**.

   A janela de configurações de Novidades Kaspersky é aberta.
3. Especificar as seguintes configurações:

   - Selecione o nível de importância para as novidades que você deseja ver. As novidades sobre outras categorias não serão exibidas.
   - Selecione onde você deseja que o rótulo de notificação seja exibido. O rótulo pode ser exibido em todas as seções do console ou na seção **Monitoramento e relatórios** e suas subseções.
4. Clique no botão **OK**.

   As configurações da seção Novidades Kaspersky estão especificadas.

Desativando o recebimento de Novidades Kaspersky

A seção Novidades Kaspersky (**Monitoramento e relatórios → Novidades Kaspersky**) apresenta as últimas novidades sobre a sua versão do Kaspersky Security Center e sobre aplicativos gerenciados instalados nos dispositivos gerenciados. Se não deseja receber informações de novidades sobre a Kaspersky, pode desativar este recurso.

Os informativos da Kaspersky incluem dois tipos de informações: informativos relacionados à segurança e de marketing. Você pode desativar os informativos de cada tipo separadamente.

Para desativar informativos relacionados à segurança:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.
2. Na guia **Geral**, selecione a seção **Novidades Kaspersky**.
3. Alterne o botão para a posição **Comunicados relacionados à segurança Desativado**.
4. Clique no botão **Salvar**.

   O recebimento de novidades sobre a Kaspersky está desativado.

Informativos de marketing estão desativados por padrão. Você recebe informativos de marketing apenas se ativou a Kaspersky Security Network (KSN). Você pode desativar este tipo de informativo desativando a KSN.

Para desativar os informativos de marketing:

1. No menu principal, clique no ícone de configurações ( ) ao lado do nome do Servidor de Administração necessário.

   A janela Propriedades do Servidor de Administração é aberta.
2. Na guia **Geral**, selecione a seção **Configurações de Proxy da KSN**.

3. Desative a opção **Usar a Kaspersky Security Network Ativado**.

4. Clique no botão **Salvar**.

   Os informativos de marketing estão desativados.

Visualizando informações sobre detecção de ameaças

É possível ativar ou desativar a exibição de informações sobre alertas.

*Para ativar ou desativar a exibição da seção **Alertas** no menu principal:*

1. No menu principal, acesse as configurações da conta e selecione **Opções da interface.**

2. Na janela aberta de **opções de interface**, ative ou desative a opção **Exibir alertas EDR**.

3. Clique em **Salvar**.

O console exibe a subseção **Alertas** na seção **Monitoramento e relatórios** do menu principal. Na subseção **Alertas**, você pode ver informações sobre a detecção de ameaças nos dispositivos de endpoints. Se você adicionar uma chave de licença para EDR Optimum, o Kaspersky Security Center Web Console exibe automaticamente a subseção **Alertas** na seção **Monitoramento e relatórios** do menu principal. Além disso, você pode adicionar um widget que exibe informações sobre alertas.

A subseção **Alertas** será exibida automaticamente somente se você tiver adicionado a chave de licença do EDR Optimum antes de ativar a opção **Exibir alertas EDR**. Se tiver sido adicionada a chave de licença depois de ativar a opção **Exibir alertas EDR**, a subseção **Alertas** será exibida somente após você ativar esta opção novamente.

Para exibir corretamente informações detalhadas sobre ameaças detectadas no cartão de alerta, é necessário selecionar o plug-in EDR Optimum na lista de plug-ins disponíveis e, então, atualizá-lo. Além disso, é necessário instalar o plug-in do Kaspersky Endpoint Agent e a versão compatível do plug-in do Kaspersky Endpoint Security (Kaspersky Endpoint Security for Linux 12.1 ou posterior, Kaspersky Endpoint Security for Mac 12.1 ou posterior, ou Kaspersky Endpoint Security for Windows 12.6 ou posterior).

Use o menu **Filtro** para filtrar alertas por data e valores de campo.

O campo **Tipo de objeto** contém os seguintes valores:

- desconhecido
- Link de phishing
- vírus
- Cavalo de Troia
- ferramenta maliciosa
- backdoor
- worm

- outro aplicativo
- Adware
- Pornware
- Programa perigoso empacotado
- Comportamento perigoso

O campo **Resposta automática** contém os seguintes valores:

- Objeto malicioso detectado
- Objeto excluído
- Objeto desinfectado
- Falha ao desinfectar o objeto
- Objeto colocado em quarentena
- Arquivo comprimido protegido por senha detectado
- Vírus detectado

Baixando e excluindo arquivos da quarentena e backup

Esta seção fornece informações sobre como baixar e excluir arquivos da quarentena e backup no Kaspersky Security Center Web Console.

Baixando arquivos da quarentena e backup

É possível baixar os arquivos da quarentena e backup apenas se uma das duas condições a seguir for atendida: a opção **Não desconectar do Servidor de Administração** estiver ativada nas configurações do dispositivo ou se um gateway da conexão estiver em uso. Caso contrário, o download não será possível.

Para salvar uma cópia do arquivo da Quarentena ou Backup para o disco rígido:

1. Execute uma das seguintes ações:
   - Caso queira salvar uma cópia do arquivo da Quarentena, No menu principal, vá para **Operações** → **Repositórios** → **Quarentena**.
   - Caso queira salvar uma cópia do arquivo a partir do Backup, No menu principal, vá para **Operações** → **Repositórios** → **Backup**.
2. Na janela que se abre, selecione um arquivo que deseja baixar e clique em **Baixar**.

   O download é iniciado. Uma cópia do arquivo que foi colocado em Quarentena no dispositivo cliente é salva na pasta especificada.

Registro da atividade do Kaspersky Security Center Web Console

O registro em log de atividades do Kaspersky Security Center Web Console pode ajudar a investigar as causas de um defeito de software. Quando você contata o Suporte Técnico da Kaspersky sobre um defeito do Kaspersky Security Center Web Console, os especialistas de Suporte Técnico da Kaspersky podem solicitar os arquivos de log do Kaspersky Security Center Web Console a você. Os arquivos de log do Kaspersky Security Center Web Console são armazenados na <pasta de instalação do Kaspersky Security Center Web Console>/logs todo o tempo que você usar o aplicativo. Os arquivos de registro não são enviados a especialistas de Suporte Técnico da Kaspersky automaticamente.

Para ativar o registro da atividade do Kaspersky Security Center Web Console,

Marque a caixa de seleção **Ativar registro de log das atividades do Kaspersky Security Center Web Console** na janela **Configurações de conexão do Kaspersky Security Center Web Console** do Assistente de instalação do Kaspersky Security Center Web Console.

Os arquivos de registro estão no formato de texto.

Os nomes de arquivo de registro estão nos registros de formato-<nome do componente>. <nome do dispositivo>-<número de revisão do arquivo>.AAAA-MM-DD, em que:

- <nome do componente> é o nome do componente do Kaspersky Security Center ou é o nome do plugin de gerenciamento do Kaspersky Security Center Web Console.
- <nome de dispositivo> é o nome do dispositivo no qual o <nome do componente> está em execução.
- <número de revisão de arquivo> é o número do arquivo de registro criado para o <nome do componente> que está na operação no <nome do dispositivo>. Em um dia, vários arquivos de registro do mesmo <nome do componente> e <nome do dispositivo> podem ser criados. O tamanho máximo de um arquivo de registro é de 50 megabytes (MB). Quando o tamanho máximo do arquivo for atingido, um novo arquivo de registro será criado. Um novo arquivo de registro <número de revisão de arquivo> é aumentado em 1.
- AAAA, MM e DD são o ano, o mês e o dia quando o registro foi criado pela primeira vez. Quando um novo dia inicia, é criado um novo arquivo de registro.

Integração entre o Kaspersky Security Center e outras soluções

Esta seção descreve como configurar o acesso a partir do Kaspersky Security Center Web Console a outro aplicativo Kaspersky, como o Kaspersky Managed Detection and Response. Esta seção também descreve como configurar a exportação para sistemas SIEM.

Configurar o acesso ao Console da Web KATA/KEDR

O Kaspersky Anti Targeted Attack (KATA) e o Kaspersky Endpoint Detection and Response (KEDR) são dois blocos funcionais da Kaspersky Anti Targeted Attack Platform. Você pode gerenciar esses blocos funcionais através do Console da Web da Kaspersky Anti Targeted Attack Platform (KATA / KEDR Web Console). Se você usar o Kaspersky Security Center Web Console e o KATA / KEDR Web Console, poderá configurar o acesso ao KATA / KEDR Web Console diretamente da interface do Kaspersky Security Center Web Console.

Para configurar o acesso ao KATA / KEDR Web Console:

1. No menu principal, vá para **Configurações do console** → **Integração**.
2. Na guia **Integração**, selecione a seção **KATA**.
3. Digite a URL do Console da Web KATA/KEDR no campo **URL para KATA/KEDR Web Console**.
4. Clique no botão **Salvar**.

A lista suspensa **Gerenciamento avançado** é adicionada à parte superior da janela principal do aplicativo. Você pode usar este menu para abrir o KATA / KEDR Web Console. Depois de clicar em **Advanced Cybersecurity Platform**, uma nova guia é aberta no navegador com a URL especificada.

Estabelecendo uma conexão em segundo plano

Para permitir que o Kaspersky Security Center Web Console execute as tarefas em segundo plano, é preciso estabelecer uma conexão em segundo plano entre o Kaspersky Security Center Web Console e o Servidor de Administração. Você pode estabelecer uma conexão somente se sua conta tiver o direito de **Modificar ACLs** de objeto na área funcional **Recursos gerais: Permissões de usuário**.

Caso o plug-in do Kaspersky Endpoint Security for Windows 12.3 seja instalado ou caso o plug-in do Kaspersky Endpoint Security for Windows seja atualizado a partir de uma versão anterior a 11.7 e uma conexão em segundo plano ainda não tenha sido estabelecida, uma notificação será exibida informando que é necessário estabelecer uma conexão em segundo plano. Além disso, você terá que conceder à conta de serviço os direitos da área funcional **Recursos gerais: Operações no Servidor de Administração**.

Para estabelecer uma conexão em segundo plano:

1. No menu principal, vá para **Configurações do console** → **Integração**.
2. Na guia **Integração**, alterne o botão de alternância para estabelecer uma conexão em segundo plano para a posição: **Estabelecer uma conexão em segundo plano para integração Ativado**.
3. Na seção aberta **O serviço que estabelece uma conexão em segundo plano será iniciado no Kaspersky Security Center Web Console Server está instalado**, clique no botão **OK**.

A conexão de segundo plano entre o Kaspersky Security Center Web Console e o Servidor de Administração é estabelecida. O Servidor de Administração cria uma conta para a conexão em segundo plano e essa conta é usada como uma conta de serviço para manter a interação entre o Kaspersky Security Center e outro aplicativo ou solução Kaspersky. O nome desta conta de serviço contém o prefixo NWCSvcUser.

Por motivos de segurança, o Servidor de Administração muda automaticamente a senha da conta de serviço a cada 30 dias. Você não pode excluir a conta de serviço manualmente. O Servidor de Administração exclui esta conta automaticamente se você desativar uma conexão entre serviços. O Servidor de Administração cria uma única conta de serviço para cada Console de Administração e atribui todas as contas de serviço ao grupo de segurança com o nome ServiceNwcGroup. O Servidor de Administração cria este grupo de segurança automaticamente durante o processo de instalação do Kaspersky Security Center. Você não pode excluir este grupo de segurança manualmente.

Trabalhar com o Kaspersky Security Center Web Console em um ambiente de nuvem

Esta seção fornece informações sobre os recursos do Kaspersky Security Center Web Console relacionados à implementação e manutenção do Kaspersky Security Center em ambientes em nuvem, como Amazon Web Services, Microsoft Azure ou Google Cloud.

Para trabalhar em um ambiente em nuvem, é necessária uma licença especial. Se você não tiver essa licença, os elementos da interface relacionados aos dispositivos na nuvem não serão exibidos.

Configuração de ambiente em nuvem no Kaspersky Security Center Web Console

Para configurar o Kaspersky Security Center com o uso deste ambiente, é necessário ter o seguinte:

- Credenciais específicas para um ambiente em nuvem:
  - Uma função do IAM a qual foi concedida o direito de criar uma sondagem do segmento da nuvem ou uma conta de usuário IAM a qual foi concedida o direito de criar uma sondagem do segmento da nuvem (para uso com Amazon Web Services)
  - ID do Aplicativo Azure, senha e assinatura (para uso com Microsoft Azure)
  - E-mail do cliente do Google, ID do projeto e chave privada (para uso com o Google Cloud)
- Pacotes de instalação:
  - Agente de Rede para Windows
  - Agente de Rede para Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in da Web para o Kaspersky Endpoint Security for Linux
- Pelo menos um dos seguintes itens:
  - Pacote de instalação e plug-in da Web para o Kaspersky Endpoint Security for Windows (recomendado)
  - O pacote de instalação e o plugin da Web para o Kaspersky Security for Windows Server

O assistente Configurar o ambiente em nuvem inicia automaticamente na primeira conexão com o Servidor de Administração pelo Console de Administração caso o Kaspersky Security Center seja implementado a partir de uma imagem pronta para usar. Também é possível iniciar o assistente de início rápido manualmente a qualquer momento.

Para iniciar o assistente Configurar o ambiente em nuvem manualmente,

No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Configurar ambiente em nuvem**.

O assistente é iniciado.

A média da sessão de trabalho para configuração do ambiente em nuvem é de aproximadamente 15 minutos.

Etapa 1. Verificação dos plug-ins e pacotes de instalação necessários

Essa etapa não será exibida caso tenha todos os plug-ins da Web e pacotes de instalação necessários e listados abaixo.

Para configurar um ambiente na nuvem, é necessário ter os seguintes componentes:

- Pacotes de instalação:
  - Agente de Rede para Windows
  - Agente de Rede para Linux
  - Kaspersky Endpoint Security for Linux
- Plug-in da Web para o Kaspersky Endpoint Security for Linux
- Pelo menos um dos seguintes itens:
  - Pacote de instalação e plug-in da Web para o Kaspersky Endpoint Security for Windows (recomendado)
  - O pacote de instalação e o plugin da Web para o Kaspersky Security for Windows Server

    Recomendamos usar o Kaspersky Endpoint Security for Windows em vez do Kaspersky Security for Windows Server.

O Kaspersky Security Center detecta automaticamente os componentes possuídos e lista apenas os que estão faltando. Baixe os componentes listados clicando no botão **Selecionar os aplicativos para download** e, em seguida, selecione os plug-ins e pacotes de instalação necessários. Depois de baixar um componente, será possível usar o botão **Atualizar** para atualizar a lista de componentes ausentes.

Etapa 2. Licenciar o aplicativo

Esta etapa será exibida apenas se você estiver usando uma BYOL AMI e não tiver ativado o aplicativo com uma licença do Kaspersky Security for Virtualization ou uma licença do Kaspersky Hybrid Cloud Security.

Especifique a chave de licença e clique em **Avançar** para continuar.

A chave de licença é adicionada ao armazenamento do Servidor de Administração.

Se você executar o assistente novamente, essa etapa não será exibida.

Etapa 3. Seleção do ambiente em nuvem e autorização

Esta seção descreve os recursos aplicáveis apenas ao Kaspersky Security Center 12.1 ou a uma versão posterior.

Especificar as seguintes configurações:

- Ambiente em nuvem

  Selecione o ambiente em nuvem no qual você está implementando o Kaspersky Security Center: AWS, Azure ou Google Cloud.

  Caso planeje trabalhar com mais de um ambiente em nuvem, selecione um ambiente e execute o assistente novamente.

- Nome da conexão

  Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

  Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

  Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

Insira suas credenciais para receber autorização no ambiente em nuvem que especificou.

AWS

Se você selecionou AWS como tipo de segmento da nuvem, precisará de uma função do IAM ou de uma chave de acesso AWS IAM para amostragem adicional do segmento da nuvem.

- **Função do AWS IAM atribuída à instância EC2**

  Selecione esta opção caso tenha uma função do IAM com os direitos necessários para o Servidor de Administração.

- **usuário do AWS IAM**

  Selecione esta opção caso tenha uma chave de acesso AWS IAM. Insira os dados da sua chave:

  - **ID da chave de acesso**

    A ID da chave de acesso IAM é uma sequência de caracteres alfanuméricos. Você recebeu a ID da chave quando você criou a conta de usuário IAM.

    O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

  - **Chave secreta**

    A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

    Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

    O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

    Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

Azure

Se você selecionou Azure como o tipo de segmento da nuvem, especifique as seguintes configurações para a conexão que será usada para sondagem adicional do segmento da nuvem:

- **ID do aplicativo Azure**

  Você criou este ID do aplicativo no portal do Azure.

  É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **ID da assinatura do Azure**

  Você criou a assinatura no portal do Azure.

- **Senha do aplicativo Azure**

  Você recebeu a senha quando criou o ID do aplicativo.

  Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

- **Nome da conta de armazenamento do Azure**

  Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center.

- **Chave de acesso ao armazenamento do Azure**

  Você recebeu uma senha (chave) quando criou a conta de armazenamento Azure para uso com o Kaspersky Security Center.

  A chave está disponível na seção "Visão geral da conta de armazenamento Azure", na subseção "Chaves."

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

Google Cloud

Se você selecionou Google Cloud como o tipo de segmento da nuvem, especifique as seguintes configurações para a conexão que será usada para sondagem adicional do segmento da nuvem:

- **Endereço de e-mail do cliente**

  O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

- **ID do projeto**

  O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

A conexão especificada é salva nas configurações do aplicativo.

O assistente Configurar o ambiente em nuvem permite especificar apenas um segmento. Posteriormente, você poderá especificar mais conexões para gerenciar outros segmentos da nuvem.

Clique em **Avançar** para prosseguir.

Etapa 4. Amostragem de segmentos, configuração da sincronização com a Nuvem e seleção de ações adicionais

Neste passo, a sondagem de segmentos da nuvem é iniciada e um grupo de administração especial para dispositivos na nuvem é criado automaticamente. Os dispositivos detectados durante a sondagem são colocados neste grupo. O agendamento de sondagem de segmentos da nuvem é configurado (a cada 5 minutos, por padrão; é possível alterar essa configuração posteriormente).

Uma regra automática para mover **Sincronizar com a Nuvem** também é criada. Para cada verificação subsequente da rede na nuvem, os dispositivos virtuais detectados serão movidos ao subgrupo correspondente dentro do grupo **Dispositivos gerenciados\Cloud**.

Defina as seguintes configurações:

- **Sincronizar grupos de administração com estrutura de nuvem**

  Se essa opção é ativada, o grupo **Nuvem** é automaticamente criado dentro do grupo **Dispositivos gerenciados** e uma descoberta de dispositivos na nuvem é iniciada. As instâncias e máquinas virtuais detectadas durante cada verificação da rede na nuvem são colocadas no grupo Nuvem. A estrutura dos subgrupos de administração dentro deste grupo corresponde à estrutura do seu segmento da nuvem (no AWS, as zonas de disponibilidade e os grupos de posicionamento não são representados na estrutura; no Azure, as sub-redes não são representadas na estrutura). Os dispositivos que não foram identificados como instância no ambiente nuvem estão no grupo **Dispositivos não atribuídos**. Esta estrutura de grupo permite usar tarefas de instalação de grupo para instalar aplicativos antivírus nas instâncias, assim como definir políticas diferentes para grupos diferentes.

  Se esta opção estiver desativada, o grupo **Nuvem** também será criado, e a descoberta de dispositivos de nuvem também será iniciada; contudo, os subgrupos que correspondem à estrutura do segmento da nuvem não serão criados no grupo. Todas as instâncias detectadas estão no grupo de administração **Nuvem**, portanto elas são exibidos em uma lista única. Se o seu trabalho com o Kaspersky Security Center necessitar da sincronização, você pode modificar as propriedades da regra **Sincronizar com a nuvem** e forçá-la. Forçar esta regra alterará a estrutura dos subgrupos no grupo Nuvem para que ele coincida com a estrutura do seu segmento da nuvem.

  Por padrão, esta opção está desativada.

- **Implementar a proteção**

  Se esta opção estiver selecionada, o assistente cria uma tarefa para instalar aplicativos de segurança nas instâncias. Após a conclusão do assistente, o Assistente de implementação da proteção automaticamente inicia nos dispositivos em seus segmentos da nuvem, e você será capaz de instalar o Agente de Rede e aplicativos de segurança neles.

  O Kaspersky Security Center pode executar a implementação com suas ferramentas nativas. Se você não tiver permissões para instalar os aplicativos nas instâncias do EC2 ou nas máquinas virtuais do Azure, você pode configurar a tarefa de **Instalação remota** manualmente e especificar uma conta com as permissões necessárias. Neste caso, a tarefa de Instalação remota não funcionará para os dispositivos descobertos usando API AWS ou Azure. Essa tarefa só funcionará para os dispositivos descobertos usando a sondagem do Active Directory, de domínios do Windows ou de conjuntos de IPs.

  Se esta opção não está selecionada, o Assistente de Implementação da Proteção não é iniciado e as tarefas para instalar aplicativos de segurança nas instâncias não são criadas. Você pode executar manualmente ambas estas ações em outro momento.

Se você selecionar a opção Implementar a proteção, a seção **Reiniciando dispositivos** fica disponível. Nesta seção, você deverá escolher o que fazer quando o sistema operacional de um dispositivo de destino precisar ser reiniciado. Selecione se as instâncias deverão ser reiniciadas caso o sistema operacional precise ser reiniciado durante a instalação de aplicativos:

- **Não reiniciar**

  Se esta opção for selecionada, o dispositivo não será reiniciado após a instalação do aplicativo de segurança.

- **Reiniciar**

  Se esta opção for selecionada, o dispositivo será reiniciado após a instalação do aplicativo de segurança.

Clique em **Avançar** para prosseguir.

Para o Google Cloud, você só pode executar a implementação com as ferramentas nativas do Kaspersky Security Center. Se você selecionou o Google Cloud, a opção **Implementar a proteção** não está disponível.

Etapa 5. Seleção de um aplicativo para criar uma política e tarefas

Essa etapa só é exibida caso tenha pacotes de instalação e plug-ins para o Kaspersky Endpoint Security for Windows e o Kaspersky Security for Windows Server. Caso tenha um plugin e um pacote de instalação para apenas um desses aplicativos, essa etapa será ignorada e o Kaspersky Security Center criará uma política e tarefas para o aplicativo existente.

Selecione um aplicativo para o qual deseja criar uma política e tarefas:

- Kaspersky Endpoint Security for Windows
- Kaspersky Security for Windows Server

Etapa 6. Configurar o Kaspersky Security Network para o Kaspersky Security Center

Especifique as configurações para encaminhar informações sobre as operações do Kaspersky Security Center à Base de conhecimento da Kaspersky Security Network (KSN). Selecione uma das seguintes opções:

- **Concordo em usar a Kaspersky Security Network**

  O Kaspersky Security Center e os aplicativos gerenciados instalados nos dispositivos cliente transferem automaticamente seus detalhes de operação para o Kaspersky Security Network. A participação na Kaspersky Security Network assegura atualizações mais rápidas dos bancos de dados que contêm informações sobre vírus e outras ameaças, que assegura uma resposta mais rápida a ameaças de segurança emergentes.

- **Não concordo em usar a Kaspersky Security Network**

  O Kaspersky Security Center e os aplicativos gerenciados não fornecerão informações ao Kaspersky Security Network.

  Se você selecionar esta opção, o uso da Kaspersky Security Network será desativado.

A Kaspersky recomenda a participação na Kaspersky Security Network.

Os contratos da KSN para aplicativos gerenciados também podem ser exibidos. Se você concordar em usar a Kaspersky Security Network, o aplicativo gerenciado enviará dados para a Kaspersky. Se você não concordar em participar da Kaspersky Security Network, o aplicativo gerenciado não enviará dados para a Kaspersky. (Você pode alterar essa configuração posteriormente na política do aplicativo.)

Clique em **Avançar** para prosseguir.

Etapa 7. Criar uma configuração inicial de proteção

Você poderá verificar a lista de políticas e tarefas que foram criadas.

Aguarde a conclusão da criação de políticas e tarefas e, em seguida, clique em **Avançar** para prosseguir. Na última página do assistente, clique no botão **Concluir** para sair.

Amostragem do segmento de rede por meio do Kaspersky Security Center Web Console

As informações sobre a estrutura da rede (e de seus dispositivos) são recebidas pelo Servidor de Administração por meio da amostragem regular de segmentos da nuvem usando as ferramentas AWS API, Azure API ou Google API. O Kaspersky Security Center usa estas informações para atualizar o conteúdo das pastas Dispositivos não atribuídos e Dispositivos gerenciados. Se você tiver configurado dispositivos a ser movidos automaticamente para grupos de administração, os dispositivos detectados são incluídos nos grupos de administração.

Para permitir que o Servidor de Administração faça amostragem dos segmentos da nuvem, você deve ter os direitos correspondentes fornecidos com uma função do IAM ou conta de usuário IAM (no AWS), com um ID do Aplicativo e senha (no Azure) ou com um e-mail de cliente Google, ID de projeto Google e chave privada (no Google Cloud).

Você pode adicionar e excluir conexões, assim como definir o agendamento da sondagem, para cada segmento da nuvem.

Adicionar conexões para a sondagem do segmento da nuvem

Para adicionar uma conexão para a sondagem do segmento da nuvem para a lista de conexões disponíveis:

1. No menu principal, vá para **Descoberta e implementação** → **Descoberta** → **Nuvem**.
2. Na janela que se abre, clique em **Propriedades**.
3. Na janela **Configurações** que se abre, clique em **Adicionar**.

   A janela **Configurações de segmento da nuvem** se abre.
4. Especifique o nome do ambiente em nuvem para a conexão que será usada para a sondagem adicional do segmento da nuvem:

   - **Ambiente em nuvem**

     Selecione o ambiente em nuvem no qual você está implementando o Kaspersky Security Center: AWS, Azure ou Google Cloud.

     Caso planeje trabalhar com mais de um ambiente em nuvem, selecione um ambiente e execute o assistente novamente.

   - **Nome da conexão**

     Digite um nome para a conexão. O nome de um perfil não pode conter mais do que 256 caracteres. Somente caracteres Unicode são permitidos.

     Esse nome também será usado para o grupo de administração para os dispositivos em nuvem.

     Se você planeja trabalhar com mais de um ambiente em nuvem, inclua o nome do ambiente no nome da conexão, por exemplo, "Segmento do Azure", "Segmento AWS" ou "Segmento Google".

5. Insira suas credenciais para receber autorização no ambiente em nuvem que especificou.

- Se você selecionou AWS, especifique as seguintes configurações:

  - **Usar função do AWS IAM**

    Selecione esta opção se você já tiver criado uma função do IAM para o Servidor de Administração para usar os serviços AWS.

  - **Credenciais de conta de usuário IAM AWS**

    Selecione esta opção se você tiver uma conta de Usuário do IAM com as permissões necessárias e será possível inserir uma ID da chave e uma chave secreta.

    Se você especificou que tem Credenciais de conta de usuário IAM AWS, especifique o seguinte:

    - **ID da chave de acesso**

      A ID da chave de acesso IAM é uma sequência de caracteres alfanuméricos. Você recebeu a ID da chave quando você criou a conta de usuário IAM.

      O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

    - **Chave secreta**

      A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

      Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

      O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

    Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

- Se você selecionou o Azure, especifique as seguintes configurações:

  - **ID do aplicativo Azure**

    Você criou este ID do aplicativo no portal do Azure.

    É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

  - **ID da assinatura do Azure**

    Você criou a assinatura no portal do Azure.

  - **Senha do aplicativo Azure**

Você recebeu a senha quando criou o ID do aplicativo.

Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

- **Nome da conta de armazenamento Azure**

  Você criou o nome da conta de armazenamento do Azure para trabalhar com o Kaspersky Security Center.

- **Chave de acesso do armazenamento Azure**

  Você recebeu uma senha (chave) quando criou a conta de armazenamento Azure para uso com o Kaspersky Security Center.

  A chave está disponível na seção "Visão geral da conta de armazenamento Azure", na subseção "Chaves."

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

Se você selecionou o Google Cloud, especifique as seguintes configurações:

- **Endereço de e-mail do cliente**

  O e-mail do cliente é o endereço usado para registrar o seu projeto no Google Cloud.

- **ID do projeto**

  O ID do projeto é o código recebido no ato do registro do seu projeto no Google Cloud.

- **Chave privada**

  A chave privada é a sequência de caracteres recebida como sua chave privada ao registrar o seu projeto no Google Cloud. Você pode copiar e colar esta sequência para evitar erros.

  Para ver os caracteres digitados, clique e pressione o botão **Exibir**.

6. Se quiser, clique em **Definir agendamento da sondagem** e altere as configurações padrão.

A conexão é salva nas configurações do aplicativo.

Após o novo segmento na nuvem ter sido amostrado pela primeira vez, um subgrupo que corresponde àquele segmento aparece no grupo de administração **Dispositivos gerenciados\Cloud**.

Se você especificar as credenciais incorretas, nenhuma instância será encontrada durante a amostragem do segmento na nuvem e um novo subgrupo não aparecerá no grupo de administração **Dispositivos gerenciados\Cloud**.

Excluindo uma conexão para sondagem do segmento da nuvem

Se não for mais necessário sondar um segmento da nuvem específico, é possível excluir a conexão correspondente àquele segmento da lista de conexões disponíveis. Também é possível excluir uma conexão se, por exemplo, as permissões para sondar um segmento da nuvem tiverem sido transferidas para o outro usuário com credenciais diferentes.

Para excluir uma conexão:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Nuvem**.
2. Na janela que se abre, clique em **Propriedades**.
3. Na janela **Configurações** que se abre, clique no nome do segmento que deseja excluir.
4. Clique em **Excluir**.
5. Na janela que se abre, clique no botão **OK** para confirmar a sua seleção.

A conexão é excluída. Os dispositivos no segmento da nuvem correspondentes a essa conexão são excluídos automaticamente dos grupos de administração.

Configurar o agendamento da amostragem por meio do Kaspersky Security Center Web Console

A amostragem do segmento da nuvem é executada segundo um agendamento. Você pode definir a frequência de sondagem.

A frequência de sondagem é automaticamente definida em 5 minutos nas definições Configurar o ambiente em nuvem. É possível alterar esse valor a qualquer momento e definir outro agendamento. Contudo, não é recomendado configurar a execução da sondagem mais frequentemente do que a cada 5 minutos porque isso pode levar a erros na operação da API.

Para configurar um agendamento da sondagem do segmento da nuvem:

1. No menu principal, vá para **Descoberta e implementação → Descoberta → Nuvem**.
2. Na janela que se abre, clique em **Propriedades**.
3. Na janela **Configurações** que se abre, clique no nome do segmento para o qual deseja configurar um agendamento de sondagem.

   Isso abre a janela **Configurações de segmento da nuvem**.

4. Na janela **Configurações de segmento da nuvem**, clique no botão **Definir agendamento da sondagem**. Isso abre a janela **Agendamento**.

5. Na janela **Agendamento**, defina as seguintes configurações:

- **Início agendado**

  Opções de agendamento da sondagem:

  - A cada N dias

    A sondagem é executada regularmente, com o intervalo especificado em dias, iniciando na data e hora especificadas.

    Por padrão, a sondagem é executada todos os dias, iniciando na data e hora atuais do sistema.

  - A cada N minutos

    A sondagem é executada regularmente, com o intervalo especificado em minutos, iniciando na hora especificada.

    Por padrão, a sondagem é executada a cada cinco minutos, iniciando na hora atual do sistema.

  - Por dias da semana

    A sondagem é executada regularmente, nos dias da semana e na hora especificados.

    Por padrão, a sondagem é executada todas as sextas-feiras às 18h.

  - Todos os meses em dias especificados das semanas selecionadas

    A sondagem é executada regularmente, nos dias de cada mês e na hora especificados.

    Por padrão, nenhum dia do mês é selecionado; a hora de início padrão é 18h.

- Intervalo de início (min.)

  Especifique o valor de N (para minutos ou dias).

- A partir das

  Especifique quando iniciar a primeira sondagem.

- Executar tarefas ignoradas

  Se o Servidor de Administração estiver desligado ou indisponível durante o tempo no qual a sondagem está agendada, o Servidor de Administração pode iniciar a sondagem imediatamente após ser ligado ou esperar até a próxima vez em que a sondagem estiver agendada.

  Se esta opção estiver ativada, o Servidor de Administração inicia a sondagem imediatamente após ser ligado.

  Se esta opção estiver desativada, o Servidor de Administração espera até a próxima em que a sondagem estiver agendada.

  Por padrão, esta opção está ativada.

6. Clique em **Salvar** para salvar as alterações.

O agendamento da sondagem para o segmento foi configurado e salvo.

Visualizar os resultados da amostragem de segmentos da nuvem por meio do Kaspersky Security Center Web Console

Você pode visualizar os resultados da amostragem de segmentos da nuvem, ou seja, visualizar a lista de dispositivos em nuvem gerenciados pelo Servidor de Administração.

Para visualizar os resultados da sondagem de segmentos da nuvem,

No menu principal, vá para **Descoberta e implementação → Descoberta → Nuvem**.

Isso exibe os segmentos de nuvem disponíveis para sondagem.

Visualizar as propriedades dos dispositivos na nuvem por meio do Kaspersky Security Center Web Console

É possível visualizar as propriedades de cada dispositivo na nuvem.

Para visualizar as propriedades de um dispositivo na nuvem:

1. No menu principal, vá para **Dispositivos** → **Dispositivos gerenciados**.
2. Clique no nome do dispositivo cujas propriedades deseja visualizar.

   Uma janela de propriedades é exibida com a seção **Geral** selecionada.
3. Caso queira visualizar as propriedades específicas de dispositivos na nuvem, selecione a seção **Sistema** na janela de propriedades.

   As propriedades são exibidas dependendo da plataforma na nuvem do dispositivo.

   Para os dispositivos na AWS, as seguintes propriedades são exibidas:

   - **Dispositivo descoberto usando API** (valor: **AWS**)
   - **Região da nuvem**
   - **VPC da nuvem**
   - **Zona de disponibilidade da nuvem**
   - **Subrede da nuvem**
   - **Cloud Placement Group** (essa unidade será exibida apenas se a instância pertencer a um grupo de colocação; caso contrário, não será exibida)

   Para os dispositivos no Azure, as seguintes propriedades são exibidas:

   - **Dispositivo descoberto usando API** (valor: **Microsoft Azure**)
   - **Região da nuvem**
   - **Subrede da nuvem**

   Para os dispositivos no Google Cloud, as seguintes propriedades são exibidas:

   - **Dispositivo descoberto usando API** (valor: **Google Cloud**)
   - **Região da nuvem**
   - **VPC da nuvem**
   - **Zona de disponibilidade da nuvem**
   - **Subrede da nuvem**

Sincronização com a nuvem: configuração da regra móvel

Durante a operação de Configurar o ambiente em nuvem, a regra sincronizar com a nuvem é criada automaticamente. Esta regra permite mover automaticamente os dispositivos detectados em cada sondagem, do grupo Dispositivos não atribuídos para o grupo Dispositivos gerenciados\Nuvem para tornar estes dispositivos disponíveis para o gerenciamento centralizado. Por padrão, a regra está ativa após ter sido criada. Você pode desativar, modificar ou forçar a regra a qualquer momento.

Para editar as propriedades da regra de Sincronizar com a nuvem e/ou forçar a regra:

1. No menu principal, vá para **Descoberta e implementação → Implementação e atribuição → Regras de migração**.

   Isso abre uma lista de regras de movimentação.

2. Na lista de regras de movimentação, selecione **Sincronizar com a nuvem**.

   Isso abre a janela de propriedades da regra.

3. Se necessário, especifique as seguintes configurações na guia **Condições da regra**, na guia **Segmentos da nuvem**:

- **O dispositivo está no segmento da nuvem**

  A regra só é aplicada aos dispositivos que estão no segmento da nuvem selecionado. Caso contrário, a regar se aplica a todos os dispositivos que tenham sido descobertos.

  Por padrão, esta opção está selecionada.

- **Incluir objetos secundários**

  A regra se aplica a todos os dispositivos no segmento selecionado e em todas as subsecções da nuvem aninhadas. Caso contrário, a regra só é aplicada aos dispositivos que estão no segmento raiz.

  Por padrão, esta opção está selecionada.

- **Migrar dispositivos de objetos aninhados para os subgrupos correspondentes**

  Se essa opção é ativada, os dispositivos de objetos aninhados são automaticamente movidos aos subgrupos que correspondem à sua estrutura.

  Se essa opção é desativada, os dispositivos de objetos aninhados são automaticamente movidos para a raiz do subgrupo Nuvem sem nenhuma ramificação adicional.

  Por padrão, esta opção está ativada.

- **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente**

  Se esta opção estiver ativada, quando a estrutura do grupo **Dispositivos gerenciados\Nuvem** não tiver nenhum subgrupo que corresponda à seção que contém o dispositivo, o Kaspersky Security Center criará os subgrupos. Por exemplo, se uma nova sub-rede for descoberta durante a descoberta de dispositivos, um novo grupo com o mesmo nome será criado abaixo do grupo **Dispositivos gerenciados\Nuvem**.

  Se esta opção estiver desativada, o Kaspersky Security Center não criará nenhum novo subgrupo. Por exemplo, se uma nova sub-rede for descoberta durante a sondagem da rede, um novo grupo com o mesmo nome não será criado sob o grupo **Dispositivos gerenciados\Nuvem**, e os dispositivos naquela sub-rede serão movidos para o grupo **Dispositivos gerenciados\Nuvem**.

  Por padrão, esta opção está ativada.

- **Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem**

  Se esta opção estiver ativada, o aplicativo excluirá do grupo Nuvem todos os subgrupos que não correspondem a nenhum dos objetos da nuvem existentes.

  Se esta opção estiver desativada, os subgrupos que não correspondem a nenhum dos objetos da nuvem existentes serão mantidos.

  Por padrão, esta opção está ativada.

Caso tenha ativado a opção **Sincronizar grupos de administração com estrutura de nuvem** ao usar Configurar o ambiente em nuvem, a regra **Sincronizar com a nuvem** é criada com as opções **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente** e **Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem** ativadas.

Se você não ativou a opção **Sincronizar grupos de administração com estrutura de nuvem**, a regra **Sincronizar com a nuvem** é criada com essas opções desativadas (desmarcadas). Se o seu trabalho com o Kaspersky Security Center precisar que a estrutura de subgrupos no subgrupo **Dispositivos gerenciados\Nuvem** coincida com a estrutura dos segmentos da nuvem, ative as opções **Criar subgrupos que correspondem a contêineres de dispositivos detectados recentemente** e **Excluir subgrupos sem correspondências encontradas nos segmentos da nuvem** nas propriedades da regra e, a seguir, force a regra.

4. Na lista suspensa **Dispositivo detectado usando a API**, selecione um dos seguintes valores:

   - **Não**. O dispositivo não pode ser detectado usando AWS, Azure ou Google API, ou seja, está fora do ambiente em nuvem ou está no ambiente em nuvem, mas não pode ser detectado usando uma API por algum motivo.
   - **AWS**. O dispositivo é descoberto usando AWS API, ou seja, o dispositivo está definitivamente no ambiente nuvem do AWS.
   - **Azure**. O dispositivo é descoberto usando Azure API, ou seja, o dispositivo está definitivamente no ambiente nuvem do Azure.
   - **Google Cloud**. O dispositivo é descoberto usando Google API, ou seja, o dispositivo está definitivamente no ambiente nuvem do Google.
   - Nenhum valor. Este critério não pode ser aplicado.

5. Se necessário, defina outras propriedades da regra nas outras seções.

A regra de movimentação é configurada.

Instalação remota de aplicativos nas máquinas virtuais do Azure

Você deve ter uma licença válida para instalar aplicativos nas máquinas virtuais do Microsoft Azure.

O Kaspersky Security Center suporta os seguintes cenários:

- Um dispositivo cliente é detectado via API do Azure. A instalação é executada por meio de uma API. Usar a API do Azure significa que será possível instalar os seguintes aplicativos:
  - Kaspersky Endpoint Security for Linux
  - Kaspersky Endpoint Security for Windows
  - Kaspersky Security for Windows Server
- Um dispositivo cliente é detectado por meio da Azure API. A instalação é realizada por meio de ponto de distribuição ou, se não houver um ponto de distribuição, manualmente, usando pacotes de instalação independente. Você pode instalar qualquer aplicativo compatível com o Kaspersky Security Center desta forma.

Para criar uma tarefa para instalação remota do aplicativo nas máquinas virtuais do Azure:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.
3. Siga as instruções do assistente:

   a. Selecionar **Instalar o aplicativo remotamente** como o tipo de tarefa.

   b. Na página **Pacotes de instalação**, selecione **Instalação remota pela API do Microsoft Azure**.

   c. Ao selecionar a conta para acessar os dispositivos, use uma conta existente do Azure ou clique em **Adicionar** e insira as credenciais de sua conta do Azure:

   - **Nome da conta do Azure**

     Digite qualquer nome para as credenciais que você está especificando. Este nome será exibido na lista das contas a executarem a tarefa.

   - **ID do aplicativo Azure**

     Você criou este ID do aplicativo no portal do Azure.

     É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

   - **Senha do aplicativo Azure**

     Você recebeu a senha quando criou o ID do aplicativo.

     Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

   d. Selecione os dispositivos relevantes no grupo **Dispositivos gerenciados\Nuvem**.

Após a conclusão do assistente, a tarefa para a instalação remota do aplicativo aparece na lista de tarefas.

Criação da tarefa de Backup dos dados do Servidor de Administração usando um DBMS na nuvem

Tarefas de Backup são tarefas do Servidor de Administração. Você cria uma tarefa de backup se desejar usar um DBMS localizado em um ambiente de nuvem (AWS ou Azure).

Para criar uma tarefa de backup de dados do Servidor de Administração:

1. No menu principal, vá para **Dispositivos** → **Tarefas**.
2. Clique em **Adicionar**.

   O Assistente para novas tarefas inicia.

3. Na primeira página do assistente, na lista **Aplicativo**, selecione **Kaspersky Security Center 14.2**, e na lista **Tipo de tarefa**, selecione **Backup de dados do Servidor de Administração**.

4. Na página correspondente do assistente, especifique as seguintes informações:

   - Se estiver trabalhando com um banco de dados no AWS:

     - **Nome do bucket S3**

       O nome do S3 bucket que você criou para o Backup.

     - **ID da chave de acesso**

       Você recebeu o ID da chave (sequência de caracteres alfanuméricos) quando criou a Conta de Usuário do IAM para uso com a instância de armazenamento do S3 bucket.

       O campo está disponível se você selecionou o banco de dados RDS em um S3 bucket.

     - **Chave secreta**

       A chave secreta que você recebeu com o ID da chave de acesso quando criou a Conta de Usuário do IAM.

       Os caracteres da chave secreta são exibidos como asteriscos. Após você começa a inserir a chave secreta, o botão **Exibir** é exibido. Mantenha pressionado este botão pelo tempo necessário para exibir os caracteres que você inseriu.

       O campo está disponível se você selecionou uma chave de acesso a AWS IAM para a autorização em vez de uma função do IAM.

   - Se estiver trabalhando com um banco de dados no Microsoft Azure:

     - **Nome da conta de armazenamento do Azure**

       Você criou o nome da conta de armazenamento do Azure para uso com o Kaspersky Security Center.

     - **ID de assinatura do Azure**

       Você criou a assinatura no portal do Azure.

     - **Senha do Azure**

       Você recebeu a senha quando criou o ID do aplicativo.

       Os caracteres da senha são exibidos como asteriscos. Após você começar a inserir a senha, o botão **Exibir** se torna disponível. Mantenha pressionado este botão para exibir os caracteres que você inseriu.

     - **ID do aplicativo Azure**

Você criou este ID do aplicativo no portal do Azure.

É possível fornecer somente um ID do aplicativo Azure para sondagem e outros fins. Se quiser criar a sondagem de outro segmento do Azure, primeiro exclua a conexão Azure existente.

- **Nome do servidor Azure SQL**

  O nome e o grupo do recurso estão disponíveis nas propriedades do Azure SQL Server.

- **Grupo de recursos do servidor Azure SQL**

  O nome e o grupo do recurso estão disponíveis nas propriedades do Azure SQL Server.

- **Chave de acesso ao armazenamento do Azure**

  Disponível nas propriedades da conta de armazenamento, na seção Chaves de Acesso. Você pode usar qualquer uma das chaves (key1 ou key2).

A tarefa é criada e exibida na lista de tarefas. Caso a opção **Abrir detalhes da tarefa quando a criação for concluída** seja habilitada, será possível modificar as configurações padrão da tarefa imediatamente após a criação. Se você não ativar esta opção, a tarefa será criada com as configurações padrão. Você pode modificar as configurações padrão depois, a qualquer momento.

Diagnóstico remoto de dispositivos cliente

É possível usar o diagnóstico remoto para execução remota das seguintes operações nos dispositivos clientes:

- Ativar e desativar o rastreamento, alterar o nível de rastreamento e baixar o arquivo de rastreamento
- Download de informações do sistema e de configurações do aplicativo
- Download de registros de eventos
- Gerar um arquivo de dump para um aplicativo
- Início do diagnóstico e download de seus relatórios
- Início, interrupção e reinício de aplicativos

Você pode usar registros de eventos e relatórios de diagnóstico baixados de um dispositivo cliente para resolver problemas. Além disso, ao entrar em contato com o Suporte Técnico da Kaspersky, um especialista de Suporte Técnico pode pedir que você faça download de arquivos de rastreamento, arquivos de despejo, logs de eventos e relatórios de diagnóstico de um dispositivo cliente para análise adicional na Kaspersky.

O diagnóstico remoto é realizado usando o Servidor de Administração.

Abertura da janela de diagnóstico remoto

Para executar diagnóstico remoto em um dispositivo cliente, é necessário abrir a janela de diagnóstico remoto.

Para abrir a janela de diagnóstico remoto:

1. Para selecionar o dispositivo para o qual você deseja abrir a janela de diagnóstico remoto, execute um dos seguintes procedimentos:

   - Caso o dispositivo pertença a um grupo de administração, No menu principal, vá para **Dispositivos → Dispositivos gerenciados**.

   - Caso o dispositivo pertença ao grupo de dispositivos não atribuídos, No menu principal, vá para **Descoberta e implementação → Dispositivos não atribuídos**.

2. Clique no nome do dispositivo necessário.

3. Na janela de propriedades do dispositivo exibida, selecione a guia **Avançado**.

4. Na janela que se abre, clique em **Diagnóstico remoto**.

   Isso abre a janela de **Diagnóstico remoto** do dispositivo cliente.

Ativação e desativação do rastreamento para aplicativos

É possível ativar e desativar o rastreamento para aplicativos, incluindo o rastreamento do Xperf.

Ativação e desativação do rastreamento

Para ativar ou desativar o rastreamento em um dispositivo remoto:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto, clique em **Diagnóstico remoto**.

3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.

   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.

4. Na lista de aplicativos, selecione o aplicativo para o qual deseja ativar ou desativar o rastreamento.

   A lista de opções de diagnóstico remoto é exibida.

5. Se desejar ativar o rastreamento:

   a. Na seção **Rastreamento** da lista, clique em **Ativar rastreamento**.

   b. Na janela **Modificar nível de rastreamento** que se abre, recomendamos que você mantenha os valores padrões das configurações. Quando necessário, um especialista de Suporte Técnico orientará você através do processo de configuração. Estão disponíveis as seguintes configurações:

   - **Nível de rastreamento**

     O nível de rastreamento define o volume de detalhes que o arquivo de rastreamento contém.

   - **Rastreamento baseado em rotatividade**

     O aplicativo sobrescreve as informações de rastreamento para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o número máximo de arquivos a serem usados para armazenar as informações de rastreamento e o tamanho máximo de cada arquivo. Se o número máximo de arquivos de rastreamento com o tamanho máximo estiver gravado, o arquivo de rastreamento mais antigo será excluído para que um novo arquivo possa ser gravado.

     Essa configuração está disponível apenas para o Kaspersky Endpoint Security.

   c. Clique em **Salvar**.

   O rastreamento está ativado para o aplicativo selecionado. Em alguns casos, um aplicativo de segurança e sua tarefa devem ser reiniciados para que seja possível ativar o rastreamento.

6. Caso deseje desativar o rastreamento para o aplicativo selecionado, clique em **Desabilitar rastreamento**.

   O rastreamento está desativado para o aplicativo selecionado.

Ativação do rastreamento do Xperf

Para o Kaspersky Endpoint Security, um especialista de Suporte Técnico pode solicitar que você ative o rastreamento do Xperf para obter informações sobre o desempenho do sistema.

Para ativar e configurar o rastreamento do Xperf:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.

   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.
4. Na lista de aplicativos, selecione Kaspersky Endpoint Security for Windows.

   A lista de opções de diagnóstico remoto do Kaspersky Endpoint Security for Windows é exibida.

5. Na seção **Rastreamento do Xpref** da lista, clique em **Ativar rastreio do Xperf**.

   Se o rastreamento do Xperf já estiver ativado, o botão **Desativar rastreamento Xperf** é exibido.

6. Na janela **Alterar nível de rastreamento Xperf** que se abre, dependendo da solicitação do especialista de Suporte Técnico, faça o seguinte:

   a. Selecione um dos seguintes níveis de rastreamento:

   - **Nível leve**

     Um arquivo de rastreamento deste tipo contém a quantidade mínima de informações sobre o sistema.

     Por padrão, esta opção está selecionada.

   - **Nível profundo**

     Um arquivo de rastreamento deste tipo contém informações mais detalhadas do que as dos arquivos de rastreamento do tipo *Superficial* e podem ser solicitadas pelos especialistas de Suporte Técnico quando um arquivo de rastreamento do tipo *Superficial* não for suficiente para a avaliação de desempenho. Um arquivo de rastreamento *Profundo* contém informações técnicas sobre o sistema, como as informações sobre hardware, sistema operacional, lista de processos e aplicativos iniciados e concluídos, eventos usados para avaliação de desempenho e eventos da Ferramenta de Avaliação de Sistema do Windows.

   b. Selecione um dos seguintes tipos de rastreamento do Xperf:

   - **Tipo básico**

     As informações de rastreamento são recebidas durante a operação do aplicativo Kaspersky Endpoint Security.

     Por padrão, esta opção está selecionada.

   - **Tipo na reinicialização**

     As informações de rastreamento são recebidas quando o sistema operacional é iniciado no dispositivo gerenciado. Esse tipo de rastreamento é eficaz quando o problema que afeta o desempenho do sistema ocorre depois que o dispositivo é ligado e antes da inicialização do Kaspersky Endpoint Security.

   Você também pode receber a solicitação de ativar a opção **Tamanho do arquivo de rotatividade, em MB** para impedir o aumento excessivo no tamanho do arquivo de rastreamento. Especifique o tamanho máximo do arquivo de rastreamento. Quando o arquivo atingir o tamanho máximo, as informações de rastreamento mais antigas serão substituídas por novas informações.

   c. Defina o tamanho do arquivo de rotação.

   d. Clique em **Salvar**.

O rastreamento do Xperf está ativado e configurado.

Para desativar o rastreamento do Xperf:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.

   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.
4. Na lista de aplicativos, selecione Kaspersky Endpoint Security for Windows.

   As opções de rastreamento do Kaspersky Endpoint Security for Windows são exibidas.
5. Na seção **Rastreamento do Xpref** da lista, clique em **Desativar rastreamento Xperf**.

   Se o rastreamento do Xperf já estiver desativado, o botão **Ativar rastreamento Xperf** é exibido.

O rastreamento do Xperf está desativado.

Download de arquivos de rastreamento de um aplicativo

Para fazer download do arquivo de rastreamento de um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.

   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.

   Na seção **Rastreamento**, clique no botão **Arquivos de rastreamento**.

   Assim, a janela **Registros de rastreamento do dispositivo** é aberta, onde uma lista de arquivos de rastreamento é exibida.
4. Na lista de arquivos de rastreamento, selecione o arquivo desejado.
5. Execute uma das seguintes ações:

   - Faça o download do arquivo selecionado clicando em **Baixar todo o arquivo**.
   - Baixe uma parte do arquivo selecionado:

     a. Clique em **Baixar uma parte**.

     b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada, de acordo com suas necessidades.

     c. Clique em **Baixar**.

O arquivo selecionado, ou sua parte, é baixado no local especificado.

Exclusão de arquivos de rastreamento

É possível excluir arquivos de rastreamento que não sejam mais necessários.

Para excluir um arquivo de rastreamento:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto exibida, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, verifique se a seção **Registros do sistema operacional** está selecionada.
4. Na seção **Arquivos de rastreamento**, clique no botão **Logs do Windows Update** ou **Logs de instalação remota**, dependendo de quais arquivos de rastreamento deseja excluir.

   Isso abre a lista de arquivos de rastreio.
5. Na lista de arquivos de rastreamento, selecione o arquivo que deseja excluir.
6. Clique no botão **Remover**.

O arquivo de rastreamento selecionado é excluído.

Download das configurações do aplicativo

Para baixar as configurações do aplicativo a partir de um dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto exibida, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** que se abre, certifique-se de que o **Registros do sistema operacional** esteja selecionado no painel direito.

   - Na seção **Informações do sistema**, clique no botão **Baixar arquivo** para baixar as informações do sistema sobre o dispositivo cliente.
   - Na seção **Configurações do aplicativo**, clique no botão **Baixar arquivo** para baixar informações sobre as configurações dos aplicativos instalados no dispositivo.

As informações são baixadas no local especificado como um arquivo.

Download de registros de eventos

Para baixar um log de eventos a partir de um dispositivo remoto:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, clique em **Logs do dispositivo**.

3. Na janela **Todos os logs do dispositivo**, selecione o log relevante.

4. Execute uma das seguintes ações:

   - Baixe o log selecionado clicando em **Baixar todo o arquivo**.

   - Baixe uma parte do log selecionado:

     a. Clique em **Baixar uma parte**.

     b. Na janela exibida, especifique o nome e a parte do arquivo a ser baixada, de acordo com suas necessidades.

     c. Clique em **Baixar**.

O log de eventos selecionado, ou uma parte dele, é baixado no local especificado.

Início, interrupção e reinício do aplicativo

É possível iniciar, parar e reiniciar aplicativos em um dispositivo cliente.

Para iniciar, interromper ou reiniciar um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto, clique em **Diagnóstico remoto**.

3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.
   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.

4. Na lista de aplicativos, selecione o aplicativo que deseja iniciar, parar ou reiniciar.

5. Selecione uma ação clicando em um dos seguintes botões:

   - **Parar aplicativo**
     Esse botão está disponível apenas se o aplicativo estiver em execução no momento.

   - **Reiniciar aplicativo**
     Esse botão está disponível apenas se o aplicativo estiver em execução no momento.

   - **Iniciar aplicativo**
     Esse botão está disponível apenas se o aplicativo não estiver em execução no momento.

Dependendo da ação selecionada, o aplicativo necessário é iniciado, parado ou reiniciado no dispositivo cliente.

Se o Agente de Rede for reiniciado, será exibida uma mensagem informando que a conexão atual do dispositivo com o Servidor de Administração será perdida.

Execução do diagnóstico remoto do Agente de Rede do Kaspersky Security Center e download dos resultados

Para iniciar o diagnóstico do Agente de Rede do Kaspersky Security Center em um dispositivo remoto e baixar os resultados:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Aplicativos Kaspersky**.

   Isso abre a lista de aplicativos da Kaspersky instalados no dispositivo.
4. Na lista de aplicativos, selecione **Agente de Rede do Kaspersky Security Center**.

   A lista de opções de diagnóstico remoto é exibida.
5. Na seção **Relatório de diagnóstico** da lista, clique no botão **Executar diagnósticos**.

   Isso inicia o processo de diagnóstico remoto e gera um relatório de diagnóstico. Quando o processo de diagnóstico estiver concluído, o botão **Baixar o relatório de diagnóstico** ficará disponível.
6. Baixe o relatório clicando no botão **Baixar o relatório de diagnóstico**.

O relatório é baixado no local especificado.

Execução de um aplicativo em um dispositivo cliente

Você pode ter que executar um aplicativo no dispositivo cliente se solicitado por um especialista de Suporte Técnico da Kaspersky.

Não será necessário instalar o aplicativo no dispositivo.

Para executar um aplicativo no dispositivo cliente:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.
2. Na janela de diagnóstico remoto exibida, clique em **Diagnóstico remoto**.
3. Na janela **Status e logs** exibida, selecione a seção **Executando um aplicativo remoto**.

4. Na janela **Executando um aplicativo remoto**, na seção **Arquivos do aplicativo**, siga um destes procedimentos, de acordo com o que o especialista da Kaspersky solicitar que você faça:

   - Selecione um arquivo comprimido contendo o aplicativo que deseja executar no dispositivo cliente clicando no botão **Procurar**.

     O arquivo comprimido deve incluir a pasta do utilitário. Essa pasta contém o arquivo executável a ser executado em um dispositivo remoto.

   - Especifique um aplicativo de linha de comando e seus argumentos, se necessário. Para fazer isso, preencha os campos **Arquivo executável em um arquivo comprimido para ser executado em um dispositivo remoto** e os campos **Argumentos da linha de comando**.

5. Clique no botão **Carregar e executar** para executar o aplicativo especificado em um dispositivo cliente.

6. Siga as instruções do especialista.

Gerar um arquivo de dump para um aplicativo

Um arquivo de despejo de aplicativo permite visualizar os parâmetros do aplicativo em execução em um dispositivo cliente em um determinado momento. Esse arquivo também contém informações sobre os módulos que foram carregados para um aplicativo.

Não há suporte para a coleta de despejo de dispositivos baseados em Linux.

Para coletar despejos por meio do diagnóstico remoto, o utilitário kldumper é usado. Esse utilitário foi desenvolvido para coletar os dumps de processos dos aplicativos da Kaspersky mediante solicitação de especialistas do suporte técnico. Informações detalhadas sobre os requisitos para usar o utilitário kldumper são fornecidas na base de conhecimento do Kaspersky Security Center.

Para criar um arquivo de despejo para um aplicativo:

1. Abra a janela de diagnóstico remoto de um dispositivo cliente.

2. Na janela de diagnóstico remoto exibida, clique no botão **Abrir**.

3. Na janela **Status e logs** exibida, selecione a seção **Executando um aplicativo remoto**.

4. Na seção **Gerando o arquivo de dump do processo**, especifique o arquivo executável do aplicativo para o qual deseja gerar um arquivo de despejo.

5. Clique no botão **Baixar arquivo de dump**.

   Um arquivo comprimido com o arquivo de despejo para o aplicativo especificado é baixado.

   Caso o aplicativo especificado não esteja em execução no dispositivo cliente, a pasta "resultado" contida no arquivo comprimido baixado estará vazia.

   Caso o aplicativo especificado esteja em execução, mas o download falhe com um erro ou a pasta "resultado" contida no arquivo comprimido baixado esteja vazia, consulte a base de conhecimento do Kaspersky Security Center.

Alteração do idioma da interface do Kaspersky Security Center Web Console

É possível selecionar o idioma da interface do Kaspersky Security Center Web Console.

Para alterar o idioma da interface:

1. No menu principal, acesse as configurações da conta e, a seguir, selecione **Idioma**.
2. Selecione um dos idiomas compatíveis com a localização.

Guia de referência de API

Este guia de referência da OpenAPI do Kaspersky Security Center foi projetado para ajudar nas seguintes tarefas:

- Automação e personalização. É possível automatizar tarefas que pode não querer tratar manualmente usando o Console de Administração. Você também pode implementar cenários personalizados que ainda não são compatíveis no Console de Administração. Por exemplo, como administrador, é possível usar o Kaspersky Security Center OpenAPI para criar e executar scripts que facilitarão o desenvolvimento da estrutura dos grupos de administração e manterão essa estrutura atualizada.

- Desenvolvimento personalizado. Por exemplo, é possível desenvolver um Console de Administração baseado em MMC alternativo para seus clientes, que permite um conjunto limitado de ações.

No Guia de referência da OpenAPI, é possível usar o campo de pesquisa à direita da tela para localizar as informações necessárias.

GUIA DE REFERÊNCIA DA OPENAPI

Exemplos de scripts

O guia de referência do OpenAPI contém exemplos dos scripts Python listados na tabela abaixo. Os exemplos mostram como você pode chamar métodos OpenAPI e realizar automaticamente várias tarefas para proteger sua rede, por exemplo, criar uma hierarquia "principal/secundária", executar tarefas no Kaspersky Security Center ou atribuir pontos de distribuição. Você pode executar as amostras como estão ou criar seus próprios scripts com base nos exemplos.

Para chamar os métodos OpenAPI e executar scripts:

1. Baixe o arquivo KlAkOAPI.tar.gz. Este arquivo inclui o pacote e exemplos KlAkOAPI (você pode copiá-los do arquivo ou do guia de referência OpenAPI). O arquivo KlAkOAPI.tar.gz também está localizado na pasta de instalação do Kaspersky Security Center.

2. Instale o pacote KlAkOAPI do arquivo KlAkOAPI.tar.gz em um dispositivo onde o Servidor de Administração está instalado.

   Você poderá chamar os métodos OpenAPI, executar os exemplos e seus próprios scripts somente em dispositivos onde o Servidor de Administração e o pacote KlAkOAPI estiverem instalados.

Correspondência entre cenários de usuário e exemplos de métodos de OpenAPI do Kaspersky Security Center

Exemplo	Objetivo do exemplo	Cenário
Log KlAkParams	É possível extrair e processar dados usando a estrutura de dados `KlAkParams`. O exemplo mostra como trabalhar com essa estrutura de dados. A saída, nesse exemplo, pode estar presente de maneiras diferentes. É possível obter os dados para enviar um método HTTP ou para usar em seu código.	Monitoramento e relatórios
Criar e excluir uma hierarquia primária/secundária	Você pode adicionar um Servidor de Administração secundário e estabelecer uma hierarquia "primária/secundária". Como alternativa, é possível desconectar o Servidor de Administração secundário da hierarquia.	• Criar uma hierarquia de Servidores de Administração: adicionar um Servidor de Administração secundário • Excluir uma hierarquia de Servidores de Administração
Criar a hierarquia do grupo com uma estrutura baseada na unidade do Active Directory	É possível pesquisar a unidade do Active Directory e formar uma hierarquia de grupos de dispositivos descobertos.	Criação de grupos de administração
Criar a hierarquia do grupo com uma estrutura baseada na unidade do Active Directory em cache	É possível formar uma hierarquia dos grupos de dispositivos gerenciados com base na unidade do Active Directory pesquisada anteriormente. Se novos dispositivos aparecerem no Active Directory após a última pesquisa, eles não serão adicionados ao grupo porque não estão nos resultados de pesquisa salvos.	Criação de grupos de administração
Baixar arquivos de lista de rede por meio do gateway de conexão para o dispositivo especificado	É possível conectar o Agente de Rede no dispositivo necessário usando um gateway de conexão e depois baixar um arquivo com a lista de redes no computador.	Ajuste de pontos de distribuição e gateways de conexão
Instalar uma chave de licença armazenada no repositório principal do Servidor de Administração nos Servidores de Administração secundários	É possível se conectar ao Servidor de Administração principal, baixar uma chave de licença necessária a partir dele e transmitir essa chave para todos os Servidores de Administração secundários incluídos em uma hierarquia.	Licenciamento de aplicativos gerenciados
Criar um relatório de direitos efetivos do usuário	É possível criar relatórios diferentes. Por exemplo, é possível gerar o relatório dos direitos efetivos do usuário usando este exemplo. Este relatório descreve os direitos de um usuário, dependendo do seu grupo e função. É possível baixar o relatório no formato HTML, PDF ou Excel.	Como gerar e visualizar um relatório
Iniciar uma tarefa para um dispositivo	É possível se conectar ao Agente de Rede no dispositivo necessário usando um gateway de conexão e executar na sequência a tarefa necessária.	Como iniciar uma tarefa manualmente

Exemplo	Objetivo do exemplo	Cenário
Criar subredes IP com base no site e nos serviços do Active Directory	É possível criar uma subrede IP com base na unidade do Active Directory usada por você. No exemplo, é iniciada a pesquisa do intervalo de IP especificado, excluindo as subredes descobertas para evitar conflito com uma nova subrede. Portanto, não execute as operações desse exemplo em uma rede onde é importante salvar subredes. Após a pesquisa, o exemplo é referenciado no Active Directory, examina todos os dispositivos nele e cria a subrede IP. Para tanto, no exemplo são usadas máscaras e endereços IP de todos os dispositivos.	Configuração da proteção da rede
Registrar os pontos de distribuição para dispositivos em um grupo	É possível atribuir dispositivos gerenciados como pontos de distribuição (anteriormente conhecidos como agentes de atualização).	Atualização dos bancos de dados e dos aplicativos da Kaspersky
Enumerar todos os grupos	É possível executar as seguintes ações nos grupos de administração: No exemplo é mostrado como fazer o seguinte: • Obtenha um identificador do grupo raiz "Dispositivos gerenciados" • Percorra a hierarquia do grupo • Recupere a hierarquia completa e expandida de grupos, junto com seus nomes e aninhamento	Configurando o Servidor de Administração
Enumerar tarefas, consultar estatísticas de tarefas e executar uma tarefa	É possível descobrir as seguintes informações: • Histórico de progresso da tarefa • Status da tarefa atual • Número de tarefas em diferentes status É possível também executar uma tarefa. Por padrão, a amostra executa uma tarefa depois de gerar estatísticas.	Monitoramento de execução de tarefa
Criar e executar uma tarefa	É possível criar uma tarefa. Especifique os seguintes parâmetros de tarefa no exemplo: • Tipo • Método de execução • Nome • Grupo de dispositivos para o qual a tarefa será usada Por padrão, no exemplo é criada uma tarefa do tipo "Mostrar mensagem". É possível executar esta tarefa para todos os dispositivos gerenciados do Servidor de Administração. Se necessário, é possível especificar seus próprios parâmetros de tarefa.	Criar uma tarefa
Enumerar chaves de licença	É possível obter uma lista de todas as chaves de licença ativas para os aplicativos Kaspersky instalados em dispositivos gerenciados do Servidor de Administração. A lista contém dados detalhados sobre cada chave de licença, como nome, tipo ou data de expiração.	Visualizando de informações sobre chaves de licença em uso
Criar e encontrar um usuário interno	É possível criar uma conta para trabalhos futuros.	Selecionar a conta para iniciar o Servidor de Administração
Criar uma categoria personalizada	É possível criar a categoria do aplicativo com os parâmetros necessários.	Criar uma categoria de aplicativos com conteúdo adicionado manualmente
Enumerar usuários usando SrvView	É possível usar a classe SrvView para solicitar informações detalhadas do Servidor de Administração. Por exemplo, é possível obter uma lista de usuários usando este exemplo.	Como gerenciar contas de usuário

Aplicativos que interagem com o Kaspersky Security Center via OpenAPI

Alguns aplicativos interagem com o Kaspersky Security Center via OpenAPI. Esses aplicativos incluem, por exemplo, Kaspersky Anti Targeted Attack Platform ou Kaspersky Security for Virtualization. Também pode ser um aplicativo cliente personalizado, desenvolvido por terceiros, baseado em OpenAPI.

Os aplicativos que interagem com o Kaspersky Security Center via OpenAPI conectam-se ao Servidor de Administração. Caso tenha configurado uma lista de permissão de endereços IP para se conectar ao Servidor de Administração, adicione os endereços IP de dispositivos nos quais os aplicativos que usam o Kaspersky Security Center OpenAPI estão instalados. Para saber se o aplicativo usado funciona por OpenAPI, consulte a Ajuda do aplicativo.

Práticas recomendadas para Provedores de Serviços

Esta seção fornece informações sobre como configurar e usar o Kaspersky Security Center.

Esta seção contém recomendações sobre como implementar, configurar e usar o aplicativo, assim como descreve os modos para solucionar problemas típicos na operação do aplicativo.

Planejar a implementação do Kaspersky Security Center

Ao planejar a implementação dos componentes do Kaspersky Security Center em uma rede da organização você deve levar em conta o tamanho e o escopo do projeto; especificamente, os seguintes fatores:

- Número total de dispositivos
- Número de clientes MSP

Um Servidor de Administração pode suportar um máximo de 100.000 dispositivos. Se o número total de dispositivos na rede de uma organização exceder 100.000, múltiplos Servidores de Administração devem ser implementados no provedor de serviços e combinados em uma hierarquia para o gerenciamento centralizado conveniente.

Até 500 servidores virtuais podem ser criados em um único Servidor de Administração, portanto um Servidor de Administração individual é necessário para cada um dos 500 clientes MSP.

Na etapa do planejamento da implementação, a atribuição do certificado especial X.509 ao Servidor de Administração deve considerada. A atribuição do certificado X.509 ao Servidor de Administração pode ser útil nos seguintes casos (lista parcial):

- Inspecionar tráfego da camada do soquete seguro (SSL) por meio de um proxy de terminação SSL
- Especificação dos valores necessários nos campos do certificado
- Fornecer a força de criptografia necessária de um certificado

Fornecer acesso à Internet ao Servidor de Administração

Para permitir que os dispositivos na rede cliente acessem o Servidor de Administração pela Internet, é necessário tornar as seguintes portas do Servidor de Administração disponíveis:

- Porta 13000 TCP – TLS do Servidor de Administração para conectar Agentes de Rede implementados na rede cliente
- Porta 8061 TCP – HTTPS para publicar pacotes independentes usando ferramentas do Console de Administração

- Porta 8060 TCP – HTTP para publicar pacotes independentes usando ferramentas do Console de Administração

- Porta 13292 TCP – Porta TLS somente é necessária se houver dispositivos móveis que precisam de ser gerenciados

Caso tenha de fornecer aos clientes as opções básicas de administração de rede pelo Kaspersky Security Center Web Console, será necessário também abrir a porta TCP 8080 (porta HTTPS) do Kaspersky Security Center Web Console.

Configuração padrão do Kaspersky Security Center

Um ou diversos Servidores de Administração são implementados nos servidores MSP. O número de Servidores de Administração pode ser selecionado com base no hardware disponível ou no número total clientes MSP servidos ou no número total de dispositivos gerenciados.

Um Servidor de Administração pode suportar até 100.000 dispositivos. Você deve considerar a possibilidade de aumentar o número de dispositivos gerenciados no futuro próximo: pode ser útil conectar um número ligeiramente menor de dispositivos a um único Servidor de Administração.

Até 500 servidores virtuais podem ser criados em um único Servidor de Administração, portanto um Servidor de Administração individual é necessário para cada um dos 500 clientes MSP.

Se múltiplos servidores forem usados, recomenda-se que você os combine em uma hierarquia. Usar uma hierarquia de Servidores de Administração permite-lhe evitar políticas e tarefas duplicadas, tratar todo o conjunto de dispositivos gerenciados como se eles fossem gerenciados por um único Servidor de Administração: ou seja, procura por dispositivos, criação de seleções de dispositivos e criação de relatórios.

Em cada servidor virtual correspondente a um cliente MSP, é necessário atribuir um ou diversos ponto(s) de distribuição. Se os clientes MSP e o Servidor de Administração forem vinculados por meio da Internet, pode ser útil criar uma tarefa *Baixar atualizações para os repositórios de pontos de distribuição* referente aos pontos de distribuição, para que baixem as atualizações diretamente dos servidores da Kaspersky e não do Servidor de Administração.

Se alguns dispositivos na rede cliente MSP não tiverem acesso direto à Internet, você tem de trocar os pontos de distribuição para o modo de gateway de conexão. Nesse caso, os Agentes de Rede em dispositivos na rede cliente MSP serão conectados, para a sincronização adicional, ao Servidor de Administração – mas através do gateway, não diretamente.

Como o Servidor de Administração provavelmente não será capaz de amostrar a rede cliente MSP, pode ser útil passar essa função para um ponto de distribuição.

O Servidor de Administração não será capaz de enviar notificações para a porta 15000 UDP para dispositivos gerenciados localizados além da NAT na rede cliente MSP. Para solucionar este problema, pode ser útil ativar o modo de conexão contínua para o Servidor de Administração nas propriedades dos dispositivos que atuam como pontos de distribuição e sendo executados no modo de gateway de conexão (caixa de seleção **Não desconectar do Servidor de Administração**). Este modo de conexão contínua está disponível se o número total de pontos de distribuição não exceder 300.

Sobre os pontos de distribuição

Um dispositivo com o Agente de Rede instalado pode ser usado como um ponto de distribuição. Neste modo, o Agente de Rede pode executar as seguintes funções:

- Transfira arquivos para dispositivos clientes, incluindo:
  - Atualizações de bancos de dados e módulos de software da Kaspersky

    As atualizações podem ser recuperadas do Servidor de Administração ou dos servidores da Kaspersky. Nesse caso, a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* deve ser criada para o dispositivo que serve como ponto de distribuição.
  - Atualizações de softwares de terceiros
  - Pacotes de instalação
  - Atualizações do Windows ao usar o Servidor de Administração como servidor WSUS
- Instalar software (incluindo a implementação inicial dos Agentes de Rede) em outros dispositivos.
- Faça a sondagem da rede para detectar novos dispositivos e para atualizar as informações sobre os existentes. Um ponto de distribuição pode aplicar os mesmos métodos de localização dos dispositivos que os do Servidor de Administração.

A implementação de pontos de distribuição em uma rede da organização busca os seguintes objetivos:

- Reduzir a carga do Servidor de Administração se ele funcionar como a fonte de atualização.
- Otimizar o tráfego da Internet, já que, nesse caso, cada dispositivo na rede cliente MSP não precisa acessar os servidores da Kaspersky ou o Servidor de Administração para obter as atualizações.
- Fornecer ao Servidor de Administração o acesso aos dispositivos além do NAT (relativo ao Servidor de Administração) da rede cliente MSP, que permite ao Servidor de Administração executar as seguintes ações:
  - Enviar notificações para dispositivos por UDP na rede IPv4 ou IPv6
  - Sondar a rede IPv4 ou IPv6
  - Executar a implementação inicial
  - Atuar como um servidor push

Um ponto de distribuição é atribuído para um grupo de administração. Neste caso, o escopo do ponto de distribuição inclui todos os dispositivos dentro do grupo de administração e todos dos seus subgrupos. No entanto, o dispositivo que atua como o ponto de distribuição não precisa estar incluído no grupo de administração ao qual foi atribuído.

Você pode criar uma função de ponto de distribuição como um gateway de conexão. Neste caso, os dispositivos no escopo desse ponto de distribuição serão conectados ao Servidor de Administração por meio do gateway, não diretamente. É possível usar esse modo em cenários que não permitem o estabelecimento de uma conexão direta entre dispositivos com o Agente de Rede e um Servidor de Administração.

Os dispositivos que funcionam como pontos de distribuição devem ser protegidos contra violação da integridade física e de qualquer acesso não autorizado.

Hierarquia de Servidores de Administração

Um MSP pode executar múltiplos Servidores de Administração. Pode ser inconveniente administrar diversos Servidores de Administração separados, portanto uma hierarquia pode ser aplicada. Uma configuração de "principal / secundário" para dois Servidores de Administração fornece as seguintes opções:

- Um Servidor de Administração secundário herda as políticas e tarefas do Servidor de Administração principal, prevenindo assim a duplicação das configurações.
- As seleções de dispositivos no Servidor de Administração principal podem incluir dispositivos de Servidores de Administração secundários.
- Os Relatórios no Servidor de Administração principal podem conter dados (incluindo informações detalhadas) de Servidores de Administração secundários.

O Servidor de Administração principal somente recebe dados de Servidores de Administração secundários não virtuais dentro do escopo das opções listadas acima. Essa limitação não se aplica aos Servidores de Administração virtuais, que compartilham o banco de dados com seu Servidor de Administração principal.

Servidores de Administração virtual

Com base em um Servidor de Administração físico, múltiplos Servidores de Administração virtuais podem ser criados, que serão semelhantes a Servidores de Administração secundários. Em comparação com o modelo de acesso discricionário, que tem base em listas de controle de acesso (ACLs), o modelo de Servidor de Administração virtual é mais funcional e fornece um maior grau de isolamento. Além de uma estrutura dedicada de grupos de administração para dispositivos atribuídos com políticas e tarefas, cada Servidor de Administração virtual apresenta seu próprio grupo de dispositivos não atribuídos, conjuntos próprios de relatórios, dispositivos e eventos selecionados, pacotes de instalação, regras de movimentação etc. Para isolamento mútuo máximo de clientes MSP, recomendamos que escolha Servidores de Administração virtuais como a funcionalidade a ser usada. Além disso, criar um Servidor de Administração virtual para cada cliente MSP permite-lhe fornecer opções básicas clientes da administração da rede através do Kaspersky Security Center Web Console.

Os Servidores de Administração virtuais são muito semelhantes aos Servidores de Administração secundários, mas com as seguintes distinções:

- Em um Servidor de Administração virtual falta a maior parte das configurações globais e as suas próprias portas TCP.
- Um Servidor de Administração virtual não tem Servidores de Administração secundários.
- Um Servidor de Administração virtual não tem outros Servidores de Administração virtuais.
- Um Servidor de Administração físico exibe dispositivos, grupos, eventos e objetos em dispositivos gerenciados (itens em Quarentena, registro de aplicativos e etc.) de todos os seus Servidores de Administração virtuais.
- Um Servidor de Administração virtual somente pode verificar a rede com pontos de distribuição conectados.

Gerenciar dispositivos móveis com o Kaspersky Endpoint Security for Android

Os dispositivos móveis com o Kaspersky Endpoint Security for Android™ instalado (aqui referidos como dispositivos KES) são gerenciados por meio do Servidor de Administração. O Kaspersky Security Center oferece suporte aos seguintes recursos para gerenciar dispositivos do KES:

- Tratar dispositivos móveis como dispositivos cliente:
  - Associação em grupos de administração
  - Monitoramento, como visualização de status, eventos e relatórios
  - Modificar as configurações locais e atribuir políticas para o Kaspersky Endpoint Security for Android
- Enviar comandos em modo centralizado
- Instalar pacotes de aplicativos móveis remotamente

O Servidor de Administração gerencia dispositivos KES por meio de TLS, pela porta TCP 13292.

Implementação e configuração inicial

O Kaspersky Security Center é um aplicativo distribuído. O Kaspersky Security Center suporta os seguintes aplicativos:

- Servidor de Administração – o componente principal, projetado para gerenciar os dispositivos de uma organização e armazenar dados em um DBMS.
- Console de Administração – A ferramenta básica do administrador. A Console de Administração é fornecido junto com o Servidor de Administração, mas também pode ser instalado individualmente em um ou diversos dispositivos executados pelo administrador.
- Kaspersky Security Center Web Console – Uma interface da Web para o Servidor de Administração projetado para operações básicas. Você pode instalar este componente em qualquer dispositivo que atende aos requisitos de hardware e software.
- Agente de Rede: projetado para gerenciar o aplicativo de segurança instalado em um dispositivo, assim como obter informações sobre aquele dispositivo. Os Agentes de Rede são instalados em dispositivos de uma organização.

A implementação do Kaspersky Security Center em uma rede da organização é executada como segue:

- Instalação do Servidor de Administração
- Instalação do Kaspersky Security Center Web Console
- Instalação do Console de Administração no dispositivo do administrador
- Instalação do Agente de Rede e do aplicativo de segurança em dispositivos da empresa

Recomendações sobre a instalação do Servidor de Administração

Esta seção contém recomendações sobre como instalar o Servidor de Administração. Esta seção também fornece cenários para usar uma pasta compartilhada no dispositivo do Servidor de Administração para implementar o Agente de Rede em dispositivos cliente.

Criar contas para os serviços do Servidor de Administração em um cluster para falhas

Por padrão, o instalador automaticamente cria contas não-privilegiadas para os serviços do Servidor de Administração. Este comportamento é o mais conveniente para a instalação do Servidor de Administração em um dispositivo comum.

No entanto, a instalação do Servidor de Administração em um cluster de correção de falha necessita de um cenário diferente:

1. Crie contas de domínio não privilegiado para os serviços do Servidor de Administração e torne-as membros de um grupo de segurança de domínio global denominado KLAdmins.

2. No instalador do Servidor de Administração, especifique as contas de domínio que foram criadas para os serviços.

Selecionar um DBMS

Ao selecionar um sistema de gerenciamento de banco de dados (DBMS) a ser usado por um Servidor de Administração, você deve levar em conta o número de dispositivos cobertos por um Servidor de Administração.

A tabela a seguir lista as opções válidas de DBMS, assim como as recomendações e restrições quanto ao seu uso.

Recomendações e restrições no DBMS

DBMS	Recomendações e restrições
SQL Server Express Edition 2012 ou posterior	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 10.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Você pode limitar o número máximo de eventos no repositório de eventos para evitar a sobrecarga do banco de dados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados. O uso simultâneo do SQL Server Express Edition DBMS pelo Servidor de Administração e outro aplicativo é estritamente proibido. O banco de dados Microsoft SQL Express não é compatível com a tarefa **Executar a sincronização com o Windows Update**.
Edição local do SQL Server, que não seja a Express, 2014 ou posterior	Nenhuma limitação.

DBMS	Recomendações e restrições
Edição remota do SQL Server, que não seja a Express, 2014 ou posterior	Válido somente se ambos os dispositivos estiverem no mesmo domínio do Windows®; se os domínios forem diferentes, uma relação de confiança bidirecional deve ser estabelecida entre eles.
MySQL 5.5, 5.6 ou 5.7 local ou remoto (as versões 5.5.1, 5.5.2, 5.5.3, 5.5.4 e 5.5.5 do MySQL não têm mais suporte)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 10.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.
MySQL 8.0.20 remoto ou local, e versões posteriores	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.
MariaDB local ou remoto (visualizar as versões compatíveis)	Use esse DBMS se quiser que um Servidor de Administração único funcione para menos de 20.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.
PostgreSQL, Postgres Pro (ver versões compatíveis)	Use um desses DBMS se quiser que um Servidor de Administração único funcione para menos de 50.000 dispositivos. Recomendamos desativar a tarefa de inventário de software e desativar (nas configurações de política do Kaspersky Endpoint Security) as notificações do Servidor de Administração em aplicativos iniciados. Consulte o seguinte tópico para obter detalhes: Cálculo do espaço do banco de dados.

Caso um DBMS PostgreSQL, MariaDB ou MySQL seja usado, a guia **Eventos** poderá exibir uma lista incompleta de eventos para o dispositivo cliente selecionado. Isso ocorre quando o DBMS armazena uma quantidade muito grande de eventos. É possível aumentar o número de eventos exibidos com a execução de um dos seguintes procedimentos:

- Remoção de eventos desnecessários.
- Redução do prazo de armazenamento para eventos desnecessários.

Para ver uma lista completa de eventos registrados no Servidor de Administração para o dispositivo, use Relatórios.

Se estiver usando o SQL Server 2019 como um DBMS e não tiver o patch cumulativo CU12 ou posterior, será necessário fazer o seguinte após instalar o Kaspersky Security Center:

1. Conecte-se ao SQL Server usando o SQL Management Studio.
2. Execute os seguintes comandos (se escolher um nome diferente para o banco de dados, use esse nome em vez do KAV):

   ```
   USE KAV
   GO
   ALTER DATABASE SCOPED CONFIGURATION SET TSQL_SCALAR_UDF_INLINING = OFF
   GO
   ```

3. Reinicie o serviço SQL Server 2019.

Caso contrário, usando Servidor SQL 2019 pode resultar em erros com "Há memória de sistema suficientes no pool de recursos 'internos' para executar esta consulta."

Especificar o endereço do Servidor de Administração

Ao instalar o Servidor de Administração, você deve especificar o endereço externo do Servidor de Administração. Este endereço será usado como o endereço padrão ao criar pacotes de instalação do Agente de Rede. Após isso, você será capaz de modificar o endereço do host do Servidor de Administração usando as ferramentas do Console de Administração; o endereço não se modificará automaticamente em pacotes de instalação do Agente de Rede que já tiverem sido criados.

Configurar a proteção em uma rede da organização cliente

Após a instalação de Servidor de Administração ter sido concluída, o Console de Administração é iniciado e lhe solicita executar a configuração inicial através do Assistente relevante. Quando o Assistente de início rápido estiver em execução, as seguintes políticas e as tarefas são criadas no grupo de administração raiz:

- Política do Kaspersky Endpoint Security
- Tarefa de grupo para atualizar o Kaspersky Endpoint Security
- Tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security
- Política de Agente de Rede
- Tarefa de verificação de vulnerabilidades (tarefa do Agente de Rede)
- Tarefa de instalação de atualizações e correção de vulnerabilidades (tarefa do Agente de Rede)

As políticas e tarefas são criadas com as configurações padrão, que podem resultar em sub-ótimas ou até inadmissíveis para a organização. Portanto, você deve verificar as propriedades dos objetos que foram criados e os modificá-las manualmente, se necessário.

Esta seção contém informações sobre a configuração manual de políticas, tarefas e outras configurações do Servidor de Administração, e as informações sobre o ponto de distribuição, criando uma estrutura de grupo de administração e a hierarquia de tarefas e outras configurações.

Configuração manual da política do Kaspersky Endpoint Security

Esta seção fornece recomendações sobre como configurar a política do Kaspersky Endpoint Security, que é criada pelo Assistente de início rápido. Você pode executar a configuração na janela de propriedades da política.

Ao editar uma configuração, tenha em mente que é necessário clicar no ícone de cadeado acima da configuração pertinente para permitir usar o seu valor em uma estação de trabalho.

Configurar a política na seção Proteção Avançada Contra Ameaças

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Proteção Avançada Contra Ameaças**, é possível configurar o uso da Kaspersky Security Network para o Kaspersky Endpoint Security for Windows. Você também pode configurar os módulos do Kaspersky Endpoint Security for Windows, tal como a Detecção de Comportamento, Prevenção de Exploit, Prevenção de Intrusão do Host e Mecanismo de Correção.

Na subseção **a Kaspersky Security Network**, recomendamos a ativação da opção **Kaspersky Security Network**. Use esse recurso para redistribuir e otimizar o tráfego na rede. Se a opção **Kaspersky Security Network** estiver desativada, será possível ativar o uso direto de servidores KSN.

Configurar a política na seção Proteção Essencial Contra Ameaças

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Proteção Essencial Contra Ameaças** da janela de propriedades da política, recomendamos que especifique configurações adicionais nas subseções **Firewall** e **Proteção Contra Ameaças ao Arquivo**.

A subseção **Firewall** contém configurações que permitem controlar a atividade de rede dos aplicativos nos dispositivos cliente. Um dispositivo cliente usa uma rede à qual um dos seguintes status é atribuído: pública, local ou confiável. Dependendo do status da rede, o Kaspersky Endpoint Security pode permitir ou negar atividade de rede em um dispositivo. Ao adicionar uma nova rede à sua organização, você deve atribuir um status de rede apropriado a ela. Por exemplo, se o dispositivo cliente for um laptop, recomendamos que esse dispositivo use a rede pública ou confiável, porque o laptop nem sempre está conectado à rede local. Na subseção **Firewall**, é possível verificar se foram atribuídos corretamente os status às redes usadas na organização.

Para verificar a lista de redes:

1. Nas propriedades de política, acesse **Proteção Essencial Contra Ameaças** → **Firewall**.
2. Na seção **Redes disponíveis**, clique no botão **Configurações**.
3. Na janela **Firewall** que se abre, vá para a guia **Redes** para visualizar a lista de redes.

Na subseção **Proteção Contra Ameaças ao Arquivo**, é possível desativar a verificação de unidades de rede. A verificação das unidades de rede pode colocar uma carga significativa nas unidades de rede. É mais conveniente executar a verificação indireta em servidores de arquivos.

Para desativar a verificação de unidades de rede:

1. Nas propriedades de política, acesse **Proteção Essencial Contra Ameaças → Proteção Contra Ameaças ao Arquivo**.

2. Na seção **Nível de segurança**, clique no botão **Configurações**.

3. Na janela **Proteção Contra Ameaças ao Arquivo** que é aberta, na guia **Geral**, desmarque a caixa de seleção **Todas as unidades de rede**.

Configurar a política na seção Configurações Gerais

Para uma descrição completa das configurações nesta seção, consulte a documentação do Kaspersky Endpoint Security for Windows.

Na seção **Configurações gerais** da janela de propriedades da política, recomendamos que especifique configurações adicionais nas subseções **Relatórios e armazenamento** e **Interface**.

Na subseção **Relatórios e armazenamento**, vá para a seção **Transferência de dados para o Servidor de Administração**. A caixa de seleção **Sobre os aplicativos iniciados** especifica se o banco de dados do Servidor de Administração salvará as informações sobre todas as versões de todos os módulos do software nos dispositivos em rede. Se esta caixa de seleção for marcada, as informações salvas poderão necessitar de uma quantidade significativa do espaço disponível em disco para o banco de dados do Kaspersky Security Center (dúzias de gigabytes). Desmarque a caixa de seleção **Sobre os aplicativos iniciados** se estiver selecionada na política de nível superior.

Caso o Console de Administração gerencie a proteção contra ameaças na rede da organização no modo centralizado, desative a exibição da interface do usuário do Kaspersky Endpoint Security for Windows nas estações de trabalho. Para fazer isso, na subseção **Interface**, acesse a seção **Interação com o usuário** e, em seguida, marque a opção **Não exibir interface do usuário**.

Para ativar a proteção por senha nas estações de trabalho, na subseção **Interface**, acesse a seção **Proteção por senha**, clique no botão **Configurações** e, em seguida, marque a caixa de seleção **Ativar a proteção por senha**.

Configurando a política na seção Configuração de eventos

Na seção **Configuração de eventos**, é necessário desativar a função de salvar quaisquer eventos no Servidor de Administração, exceto os seguintes:

- Na guia **Crítico**:
  - *A execução automática do aplicativo está desativada*
  - *Acesso negado*
  - *Proibida a inicialização do aplicativo*
  - *Não é possível desinfectar*
  - *O Contrato de Licença do Usuário Final foi violado*
  - *Não foi possível carregar o módulo de criptografia*
  - *Não é possível iniciar duas tarefas simultaneamente*
  - *Ameaça ativa detectada. A Desinfecção avançada deve ser iniciada*
  - *Ataque de rede detectado*
  - *Nem todos os componentes foram atualizados*
  - *Erro de ativação*
  - *Erro ao ativar o modo portátil*
  - *Erro de interação com o Kaspersky Security Center*
  - *Erro ao desativar o modo portátil*
  - *Erro ao alterar componentes do aplicativo*
  - *Erro na aplicação das regras de criptografia/descriptografia do arquivo*
  - *A política não pode ser aplicada*
  - *Processo encerrado*
  - *Atividade de rede bloqueada*
- Na guia **Falha funcional**: *Configurações de tarefa inválidas. Configurações não aplicadas*

- Na guia **Advertência**:
  - *A Autodefesa está desativada*
  - *Chave de reserva inválido*
  - *O usuário optou por cancelar a política de criptografia*
- Na guia **Informações**: *Proibida a inicialização do aplicativo em modo de teste*

Configuração manual da tarefa de atualização de grupo para o Kaspersky Endpoint Security

Se o Servidor de Administração atuar como a fonte de atualização, a opção de agendamento ideal e recomendada para o Kaspersky Endpoint Security é **Quando novas atualizações são baixadas no repositório** com a caixa de seleção **Usar atraso randomizado automaticamente para início da tarefas**.

Se uma tarefa local para baixar as atualizações dos servidores da Kaspersky para o repositório que for criado em cada ponto de distribuição, o agendamento periódico será ótimo e recomendado para a tarefa de atualização em grupo do Kaspersky Endpoint Security. Neste caso, o valor de intervalo de randomização deve ser estabelecido em 1 hora.

Configuração manual da tarefa de grupo para verificar um dispositivo com o Kaspersky Endpoint Security

O Assistente de início rápido cria uma tarefa de grupo para verificar um dispositivo. Por padrão, à tarefa é atribuído um agendamento **Executar às sextas-feiras as 19:00** com aleatorização automática e se a caixa de seleção **Executar tarefas ignoradas** estiver desmarcada.

Isto significa que se os dispositivos em uma organização são desligados às sextas-feiras, por exemplo, às 18:30, a tarefa de verificação de dispositivo nunca será executada. Você deve definir o agendamento mais conveniente para esta tarefa com base nas regras do local de trabalho adotadas na organização.

Agendar a tarefa Encontrar vulnerabilidades e atualizações necessárias

O Assistente de início rápido cria a tarefa *Encontrar vulnerabilidades e atualizações necessárias* para o Agente de Rede. Por padrão, à tarefa é atribuído um agendamento **Executar às terças-feiras as 19:00** com aleatorização automática e se a caixa de seleção **Executar tarefas ignoradas** estiver marcada.

Se as regras do local de trabalho da organização proverem o desligamento de todos os dispositivos nessa hora, a tarefa *Encontrar vulnerabilidades e atualizações necessárias* será executada após os dispositivos serem novamente ligados, ou seja, na quarta-feira pela manhã. Tal atividade pode ser indesejável porque uma verificação de vulnerabilidades pode aumentar a carga de subsistemas de disco e da CPU. Você deve definir o agendamento mais conveniente para a tarefa com base nas regras do local de trabalho adotadas na organização.

Configuração manual da tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades

O Assistente de início rápido cria uma tarefa de grupo para a instalação de atualizações e correção de vulnerabilidades para o Agente de Rede. Por padrão, a tarefa é configurada para ser executada todos os dias à 1h, com randomização automática, e a opção **Executar tarefas perdidas** não está habilitada.

Se as regras do local de trabalho da organização proverem o desligamento dos dispositivos durante a noite, a instalação da atualização nunca será executada. Você deve definir o agendamento mais conveniente da tarefa de verificação de vulnerabilidades com base nas regras do local de trabalho adotadas na organização. Também é importante ter em mente que a instalação das atualizações pode necessitar o reinício do dispositivo.

Criação de uma estrutura de grupos de administração e atribuir pontos de distribuição

Uma estrutura de grupos de administração no Kaspersky Security Center executa as seguintes funções:

- Define o escopo das políticas.

  Há um modo alternativo para aplicar configurações relevantes nos dispositivos, usando perfis de política. Neste caso, o escopo das políticas é definido, por exemplo, com tags, localizações de dispositivos nas unidades organizacionais do Active Directory, associação nos grupos de segurança do Active Directory.

- Define o escopo de tarefas de grupo.

  Há uma abordagem para definir o escopo da tarefas de grupo que não tem base em uma hierarquia de grupos de administração: uso de tarefas para seleções de dispositivos e tarefas para dispositivos específicos.

- Define os direitos de acesso aos dispositivos, Servidores de Administração virtuais e Servidores de Administração secundários.

- Atribui os pontos de distribuição.

Ao criar a estrutura de grupos de administração, você deve levar em conta a topologia da rede da organização para a atribuição ótima de pontos de distribuição. A distribuição ótima dos pontos de distribuição permite poupar tráfego na rede da organização.

Dependendo do organograma da empresa e da topologia da rede adotado pelo MSP cliente, as seguintes configurações padrão podem ser aplicadas à estrutura de grupos de administração:

- Escritório único

- Múltiplos pequenos escritórios desanexados

Configuração de cliente MSP padrão: escritório único

Em uma configuração de "escritório único" padrão, todos os dispositivos estão dentro da rede da organização, portanto eles podem se "ver" mutuamente. A rede da organização pode consistir em algumas partes separadas (redes ou segmentos de rede) vinculadas por canais estreitos.

Os seguintes métodos de criar a estrutura de grupos de administração são possíveis:

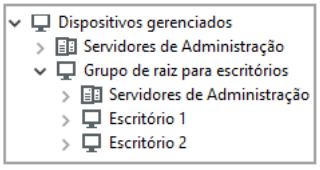
- Criar uma estrutura de grupos de administração levando em consideração a topologia da rede. A estrutura de grupos de administração pode não refletir a topologia da rede com uma precisão absoluta. Uma coincidência entre as partes separadas da rede e determinados grupos de administração seria suficiente. Você pode usar a atribuição automática de pontos de distribuição ou atribui-los manualmente.

- Criar uma estrutura de grupos de administração não levando em consideração a topologia da rede. Neste caso, você deve desativar a atribuição automática de pontos de distribuição e, a seguir, atribuir um ou diversos dispositivos para atuar como pontos de distribuição de um grupo de administração raiz em cada uma das partes separadas da rede, por exemplo, para o grupo **Dispositivos gerenciados**. Todos os pontos de distribuição estarão no mesmo nível e apresentarão a mesma expansão de escopo para todos os dispositivos na rede da organização. Neste caso, cada um dos Agentes de Rede irá conectar-se ao ponto de distribuição que tenha a rota mais curta. A rota para um ponto de distribuição pode ser traçada com o utilitário tracert.

Configuração de cliente MSP padrão: múltiplos pequenos escritórios remotos

Esta configuração padrão provê um número de pequenos escritórios remotos, que podem ser comunicados com a sede por meio da Internet. Cada escritório remoto é localizado além da NAT, ou seja, a conexão de um escritório remoto ao outro não é possível porque os escritórios estão isolados entre si.

A configuração deve ser refletida na estrutura de grupos de administração: um grupo de administração separado deve ser criado para cada escritório remoto (grupos **Escritório 1** e **Escritório 2** na figura abaixo).



Os escritórios remotos estão incluídos na estrutura do grupo de administração

Um ou múltiplos pontos de distribuição deve ser atribuído à cada grupo de administração que corresponda a um escritório. Os pontos de distribuição devem ser dispositivos nos escritórios remotos que têm espaço livre suficiente em disco. Os dispositivos implementados no grupo **Escritório 1**, por exemplo, acessarão os pontos de distribuição atribuídos ao grupo de administração **Escritório 1**.

Se alguns usuários se moverem entre escritórios fisicamente, com os seus computadores portáteis, você deve selecionar dois ou mais dispositivos (além dos pontos de distribuição existentes) em cada escritório remoto e atribui-los para atuar como pontos de distribuição para um grupo de administração de nível superior (**Grupo de raiz para escritórios** na figura acima).

Exemplo: Um computador portátil é implementado no grupo de administração **Escritório 1** e então é movido fisicamente para o escritório que corresponde ao grupo de administração **Escritório 2**. Após o computador portátil ter sido movido, o Agente de Rede tenta acessar os pontos de distribuição atribuídos ao grupo **Escritório 1**, mas aqueles pontos de distribuição estão indisponíveis. Então, O Agente de Rede começa a tentar acessar os pontos de distribuição que foram atribuídos ao **Grupo de raiz para escritórios**. Como os escritórios remotos estão isolados entre si, as tentativas de acessar os pontos de distribuição atribuídos ao grupo de administração **Grupo raiz para escritórios** somente terão êxito quando o Agente de Rede tentar acessar os pontos de distribuição no grupo **Escritório 2**. Ou seja, o computador portátil permanecerá no grupo de administração que corresponde ao escritório inicial, mas o computador portátil usará o ponto de distribuição do escritório onde estiver fisicamente localizado no momento.

Hierarquia de políticas, usando perfis de política

Essa seção fornece informações sobre como aplicar políticas aos dispositivos em grupos de administração. Esta seção também fornece informações sobre os perfis da política.

Hierarquia de políticas

No Kaspersky Security Center, você usa políticas para definir uma coleção única de configurações para múltiplos dispositivos. Por exemplo, o escopo do aplicativo P definido para o grupo de administração G inclui dispositivos gerenciados com o aplicativo P instalado o que foi implementado no grupo G e em todos dos seus subgrupos, exceto para os subgrupos onde a caixa de seleção **Herdar do grupo de origem** estiver desmarcada nas propriedades.

Uma política se diferencia de qualquer configuração local pelos ícones de cadeado (🔒) ao lado de suas configurações. Se uma configuração (ou um grupo de configurações) estiver bloqueada nas propriedades da política, será necessário, em primeiro lugar, usar essa configuração (ou o grupo de configurações) ao criar configurações efetivas e, em segundo lugar, salvar as configurações ou o grupo de configurações no fluxo abaixo da política.

A criação das configurações efetivas em um dispositivo pode ser descrita como se segue: os valores de todas as configurações que não foram bloqueadas são tiradas da política, então elas são sobregravadas com os valores das configurações locais, e então a coleção resultante é sobregravada com os valores de configurações bloqueadas tiradas da política.

As políticas do mesmo aplicativo se afetam entre si através da hierarquia de grupos de administração: as configurações bloqueadas da política de fluxo acima substituem as mesmas políticas do fluxo abaixo.

Há uma política especial para usuários fora do escritório. Esta política entra em vigor em um dispositivo quando o dispositivo muda para o modo de fora do escritório. As políticas de ausência não afetam outras políticas através da hierarquia de grupos de administração.

Perfis da política

Aplicar políticas aos dispositivos somente através da hierarquia de grupos de administração pode ser inconveniente em muitas circunstâncias. Pode ser necessário criar diversas instâncias de uma política única que se diferem em uma ou duas configurações para diferentes grupos de administração e que sincronizam os conteúdos destas políticas no futuro.

Para ajudar você a evitar tais problemas, o Kaspersky Security Center suporta os *perfis da política*. Um perfil da política é um subconjunto denominado como configurações da política. Este subconjunto é distribuído em dispositivos alvo em conjunto com a política, complementando-a em uma condição específica denominada como *condição de ativação do perfil*. Os perfis somente contêm configurações que se diferenciam da política "básica", que está ativa no dispositivo cliente (computador ou dispositivo móvel). A ativação de um perfil modifica as configurações da política que estavam ativas no dispositivo antes do perfil ser ativado. Essas configurações assumem valores que foram especificados no perfil.

As seguintes restrições são atualmente impostas aos perfis da política:

- Uma política pode incluir no máximo 100 perfis.
- Um perfil da política não pode conter outros perfis.
- Uma política não pode conter configurações de notificação.

Conteúdo de um perfil

Um perfil da política contém as seguintes partes constituintes:

- Nome. Os perfis com nomes idênticos afetam um ao outro por meio da hierarquia de grupos de administração com regras comuns.
- Subconjunto de configurações da política. Diferente da política, que contém todas as configurações, um perfil somente contém configurações que são de fato necessárias (configurações bloqueadas).
- Condição de ativação é uma expressão lógica com as propriedades do dispositivo. Um perfil está ativo (complementa a política) somente quando a condição de ativação de perfil se torna verdadeira. Em todos os outros casos, o perfil está inativo e é ignorado. As seguintes propriedades de dispositivo podem estar incluídas naquela expressão lógica:
  - Status do modo ausente.
  - Propriedades do ambiente de rede: nome da regra ativa para a conexão do Agente de Rede.
  - Presença ou ausência de identificadores especificados no dispositivo.
  - A alocação do dispositivo em uma unidade organizacional (UO) do Active Directory: explícita (o dispositivo está diretamente na UO especificada), ou implícito (o dispositivo está em uma UO, que está dentro da UO especificada em qualquer nível de aninhamento).
  - A associação do dispositivo no grupo de segurança do Active Directory (explícita ou implícita).
  - A associação do proprietário do dispositivo no grupo de segurança do Active Directory (explícita ou implícita).
- Desativando a caixa de seleção Perfil. Os perfis desativados sempre serão ignorados e as suas respetivas condições de ativação não serão verificadas.
- Prioridade do perfil. As condições de ativação de perfis diferentes são independentes, portanto vários perfis podem ser ativados simultaneamente. Se os perfis ativos contiverem coleções de configurações não de sobreposição, nenhum problema surgirá. No entanto, se dois perfis ativos contiverem valores diferentes da mesma configuração, uma ambiguidade ocorrerá. Esta ambiguidade deve ser evitada através das prioridades do perfil: o valor da variável ambígua será tomado do perfil que tiver a prioridade mais alta (aquele que é classificado como mais alto na lista de perfis).

O comportamento de perfis quando as políticas afetam uma a outra através da hierarquia

Os perfis com o mesmo nome são mesclados de acordo com as regras de mesclagem de política. Os perfis de uma política com fluxo acima têm uma prioridade mais alta do que os perfis de uma política de fluxo abaixo. Se a edição das configurações for proibida na política de fluxo acima (está bloqueada), a política de fluxo abaixo usa as condições de ativação da política de fluxo acima. Se a edição das configurações for permitida na política de fluxo acima, as condições de ativação do perfil da política de fluxo abaixo são usadas.

Como um perfil da política pode conter a propriedade **O dispositivo está offline** em sua condição de ativação, os perfis substituem completamente as políticas de usuário ausente, que não são mais compatíveis.

Uma política de usuário ausente pode conter perfis, mas os seus perfis somente podem ser ativados após que o dispositivo muda para o modo ausente.

Tarefas

O Kaspersky Security Center gerencia os aplicativos de segurança da Kaspersky instalados nos dispositivos cliente criando e executando *tarefas*. As tarefas são necessárias para a instalação, inicialização e interrupção de aplicativos, verificação de arquivos, atualização de bancos de dados e módulos de software e para a realização de outras ações em aplicativos.

As tarefas de um aplicativo específico podem ser criadas apenas se o plugin de gerenciamento desse aplicativo estiver instalado.

As tarefas podem ser realizadas no Servidor de Administração e em dispositivos.

As seguintes tarefas que são realizadas no Servidor de Administração:

- Distribuição automática de relatórios
- Baixar atualizações no repositório do Servidor de Administração
- Backup de dados do Servidor de Administração
- Manutenção do banco de dados
- Sincronização com o Windows Update
- Criação de um pacote de instalação com base na imagem do sistema operacional (SO) de um dispositivo de referência

Os seguintes tipos de tarefas são executados nos dispositivos:

- *Tarefas locais* – Tarefas que são executadas em um dispositivo específico

  As tarefas locais podem ser modificadas pelo administrador, usando as ferramentas do Console de Administração ou por um usuário de um dispositivo remoto (por exemplo, através da interface do aplicativo de segurança). Se uma tarefa local tiver sido modificada simultaneamente pelo administrador e pelo usuário de um dispositivo gerenciado, as modificações feitas pelo administrador entrarão em vigor porque elas têm uma maior prioridade.

- *Tarefas de grupo* – Tarefas que são executadas em todos os dispositivos de um grupo específico

  Salvo de especificado de outra maneira nas propriedades de tarefa, uma tarefa de grupo também afeta todos os subgrupos do grupo selecionado. Uma tarefa de grupo também afeta (opcionalmente) os dispositivos que foram conectados aos Servidores de Administração secundários e virtuais implementados no grupo ou em algum dos seus subgrupos.

- *Tarefas globais* – Tarefas que são realizadas em um conjunto de dispositivos, independentemente se os mesmos estão incluídos em qualquer grupo

Para cada aplicativo, você pode criar qualquer número de tarefas de grupo, tarefas globais ou tarefas locais.

Você pode efetuar alterações nas configurações de tarefas, exibir o andamento das tarefas, copiar, exportar, importar e excluir tarefas.

Uma tarefa é iniciada em um dispositivo cliente somente se um aplicativo para o qual a tarefa foi criada estiver sendo executado.

Os resultados das tarefas são salvos no log de eventos do Microsoft Windows e no log de eventos do Kaspersky Security Center, tanto centralmente no Servidor de Administração como localmente em cada dispositivo.

Não inclua dados privados nas configurações da tarefa. Por exemplo, evite especificar a senha do administrador do domínio.

Regras de migração de dispositivos

Recomendamos que você automatize a alocação de dispositivos aos grupos de administração no servidor virtual que corresponde a um cliente MSP, usando *regras para mover dispositivo*. Uma regra para migrar dispositivo compõe-se de três partes principais: um nome, uma condição de execução (expressão lógica com os atributos de dispositivo) e um grupo de administração alvo. Uma regra move um dispositivo para o grupo de administração alvo se os atributos do dispositivo atendam a condição de execução da regra.

Todas as regras para migrar dispositivo têm prioridades. O Servidor de Administração verifica os atributos do dispositivo quanto a se eles atendem a condição de execução de cada regra, na ordem ascendente da prioridade. Se os atributos do dispositivo atenderem a condição de execução de uma regra, o dispositivo é movido para o grupo alvo, portanto o processamento de regra é completo para este dispositivo. Se os atributos do dispositivo atenderem as condições de múltiplas regras, o dispositivo é movido para o grupo alvo da regra com a prioridade mais alta (ou seja, ele tem a classificação mais alta na lista de regras).

As regras para migrar dispositivo podem ser criadas implicitamente. Por exemplo, nas propriedades de um pacote de instalação ou de uma tarefa de instalação remota, você pode especificar o grupo de administração para o qual o dispositivo deve ser movido após que Agente de Rede seja instalado nele. Também, as regras para migrar dispositivos podem ser criadas explicitamente pelo administrador do Kaspersky Security Center na lista de regras para mover. A lista está localizada no Console de Administração, nas propriedades do grupo **Dispositivos não atribuídos**.

Por padrão, uma regra para mover dispositivo é destinada para a alocação inicial de uma só vez de dispositivos aos grupos de administração. A regra move os dispositivos do grupo **Dispositivos não atribuídos** somente uma vez. Se um dispositivo foi movido uma vez por esta regra, a regra nunca mais o moverá novamente, mesmo se você devolver o dispositivo ao grupo **Dispositivos não atribuídos** manualmente. Esta é a forma recomendada de aplicar regras para mover.

Você pode migrar dispositivos que já foram alocados à alguns dos grupos de administração. Para fazer isto, nas propriedades de uma regra, desmarque a caixa de seleção **Somente mover os dispositivos que não pertencem a um grupo de administração**.

Aplicar regras para mover aos dispositivos que já foram alocados à alguns dos grupos de administração, aumenta significativamente a carga do Servidor de Administração.

Você pode criar uma regra para mover que iria afetar um único dispositivo repetidamente.

Nós recomendamos com ênfase que você evite mover um dispositivo único de um grupo para outro repetidamente (por exemplo, para poder aplicar uma política especial àquele dispositivo, executar uma tarefa de grupo especial, ou atualizar o dispositivos através de um ponto de distribuição específico).

Tais cenários não são compatíveis, porque eles aumentam a carga no Servidor de Administração e o tráfego da rede para um grau extremo. Estes cenários também estão em conflito com os princípios operacionais do Kaspersky Security Center (em particular na área de direitos de acesso, eventos e relatórios). Outra solução deve ser encontrada, por exemplo, por meio do uso de perfis de política, tarefas para seleções de dispositivo, atribuição de Agentes de Rede de acordo com o cenário padrão, e assim por diante.

Categorização de software

A ferramenta principal para monitorar a execução dos aplicativos são as *categorias da Kaspersky* (aqui referidas como *categorias da KL*). As categorias da KL ajudam os administradores do Kaspersky Security Center a simplificar o suporte da categorização de software e minimizar o tráfego indo para os dispositivos gerenciados.

As categorias de usuário somente devem ser criadas para aplicativos que não podem ser classificados em nenhuma das categorias da KL existentes (por exemplo, para o software criado de forma personalizada). As categorias de usuário são criadas com base em um pacote de instalação do aplicativo (MSI) ou uma pasta com pacotes de instalação.

Se uma grande coleção de software estiver disponível, que não foi categorizada através de categorias da KL, pode ser útil criar uma categoria automaticamente atualizada. Os checksums de arquivos executáveis serão automaticamente adicionados a esta categoria em cada modificação da pasta que contém os pacotes de distribuição.

Não crie categorias de software atualizadas automaticamente para as pastas Meus Documentos, %windir%, %ProgramFiles% e %ProgramFiles(x86)%. O conjunto de arquivos nestas pastas está sujeito a modificações frequentes, que conduz a um aumento da no Servidor de Administração e no aumento do tráfego da rede. Você deve criar uma pasta dedicada com a coleção de software e periodicamente adicionar-lhe novos itens.

Sobre os aplicativos para múltiplos usuários

O Kaspersky Security Center permite que os administradores de provedores de serviço e administradores de usuários usem os aplicativos Kaspersky com o suporte para múltiplos usuários. Após um aplicativo da Kaspersky para múltiplos usuários ter sido instalado na infraestrutura de um provedor de serviços, os usuários podem começar a usar o aplicativo.

Para separar as tarefas e políticas relativas a diferentes usuários, você precisa criar um Servidor de Administração virtual no Kaspersky Security Center para cada usuário. Todas as tarefas e políticas para aplicativos de múltiplos usuários sendo executadas para um usuário devem ser criadas para o grupo de administração Dispositivos gerenciados do Servidor de Administração virtual correspondente àquele usuário. As tarefas criadas para os grupos de administração relativos ao Servidor de Administração principal não afetam os dispositivos dos tenants.

Diferente dos administradores do provedor de serviços, um administrador de usuários pode criar e exibir tarefas e políticas do aplicativo somente para os dispositivos do usuário correspondente. Os conjuntos de configurações de tarefas e políticas disponíveis para os administradores do provedor de serviços e para os administradores de usuários são diferentes. Algumas das configurações de tarefas e políticas não estão disponíveis para os administradores de usuários.

Na estrutura hierárquica de um usuário, as políticas criadas para aplicativos para múltiplos usuários são herdadas de grupos de administração de nível mais baixo, assim como de grupos de administração de nível superior: a política é propagada à todos os dispositivos cliente que pertencem ao usuário.

Cópia backup e restauração das configurações do Servidor de Administração

O backup das configurações do Servidor de Administração e de seu banco de dados é executado pela tarefa de backup e com o utilitário klbackup. Uma cópia backup inclui todas as principais configurações e objetos pertencentes ao Servidor de Administração, como certificados, chaves primárias para criptografia de unidades em dispositivos gerenciados, chaves para várias licenças, estrutura de grupos de administração com todo o seu conteúdo, tarefas, políticas etc. Com uma cópia backup, é possível recuperar a operação de um Servidor de Administração o mais rápido possível, gastando de uma dúzia de minutos a algumas horas nisso.

Se nenhuma cópia backup estiver disponível, uma falha pode levar a uma perda irrevogável de certificados e de todas as configurações do Servidor de Administração. Isto exigirá reconfigurar o Kaspersky Security Center do zero e executar a implementação inicial do Agente de Rede novamente na rede da organização. Todas as chaves primárias para a criptografia das unidades em dispositivos gerenciados também serão perdidas, arriscando a perda irrevogável dos dados criptografados nos dispositivos com Kaspersky Endpoint Security. Portanto, não negligencie os backups regulares do Servidor de Administração usando a tarefa de backup padrão.

O Assistente de Início Rápido cria a tarefa de backup para as configurações do Servidor de Administração e o configura para ser executado diariamente, às 4h. As cópias de backup são salvas por padrão na pasta %ALLUSERSPROFILE%\Application Data\KasperskySC.

Se uma instância do Microsoft SQL Server instalado em outro dispositivo for usado como o DBMS, você deve modificar a tarefa de backup especificando um caminho UNC, que está disponível para gravar tanto pelo serviço Servidor de Administração como pelo serviço SQL Server, como a pasta para armazenar as cópias backup. Este requisito deriva de um recurso especial do backup no Microsoft SQL Server DBMS.

Se uma instância local do Microsoft SQL Server for usada como DBMS, também recomendamos salvar as cópias de backup em uma mídia dedicada para assegurar que elas estejam protegidas contra danos, em conjunto com o Servidor de Administração.

Como uma cópia backup contém dados importantes, a tarefa de backup e o utilitário klbackup fornecem a proteção por senha das cópias backup. Por padrão, a tarefa de backup é criada com uma senha em branco. Você deve definir uma senha nas propriedades da tarefa de backup. Negligenciar este requisito causa uma situação em que todas as chaves de certificados do Servidor de Administração, as chaves para as licenças e as chaves primárias para a criptografia de unidades em dispositivos gerenciados permanecem não criptografadas.

Além do backup regular, você também deve criar uma cópia backup antes de cada mudança significativa, incluindo a instalação de atualizações e patches do Servidor de Administração.

Se você usar o Microsoft SQL Server como DBMS, poderá minimizar o tamanho das cópias de backup. Para isso, ative a opção **Compactar o backup** nas configurações do SQL Server.

A restauração de uma cópia backup é executada com o utilitário klbackup em uma instância operável do Servidor de Administração que acaba de ser instalado e que tenha a mesma versão (ou posterior) para o qual a cópia backup foi criada.

A instância do Servidor de Administração no qual a restauração deve ser executada, deve usar um DBMS do mesmo tipo (por exemplo, o mesmo SQL Server ou MariaDB) e a mesma versão ou posterior. A versão do Servidor de Administração pode ser a mesma (com uma correção idêntica ou posterior), ou posterior.

Esta seção descreve os cenários padrão para restaurar as configurações e objetos do Servidor de Administração.

Um dispositivo com o Servidor de Administração está inoperável

Se um dispositivo com o Servidor de Administração estiver inoperável devido a uma falha, você é recomendado a executar as seguintes ações:

- Ao novo Servidor de Administração deve ser atribuído o mesmo endereço: nome NetBIOS, FQDN ou IP estático (dependendo de qual deles foi definido quando os Agentes de Rede foram implementados).
- Instale o Servidor de Administração, usando um DBMS do mesmo tipo ou da mesma (ou posterior) versão. Você pode instalar a mesma versão do Servidor com a mesma (ou posterior) correção ou uma versão posterior. Após a instalação, não execute a configuração inicial por meio do assistente.
- No menu **Iniciar**, execute o utilitário klbackup e execute a restauração.

As configurações do Servidor de Administração ou o do banco de dados estão corrompidas

Se o Servidor de Administração estiver inoperável devido a configurações ou aos bancos de dados corrompidas (p. ex., após uma oscilação de corrente), você é recomendado a usar o seguinte cenário de restauração:

1. Verifique o sistema de arquivos no dispositivo danificado.
2. Desinstale a versão inoperável do Servidor de Administração.
3. Reinstale o Servidor de Administração usando um DBMS do mesmo tipo e da mesma (ou posterior) versão. Você pode instalar a mesma versão do Servidor com a mesma (ou posterior) correção ou uma versão posterior. Após a instalação, não execute a configuração inicial por meio do assistente.
4. No menu **Iniciar**, execute o utilitário klbackup e execute a restauração.

É proibido restaurar o Servidor de Administração usando qualquer outro modo que não seja através do utilitário klbackup.

Qualquer tentativa de restaurar o Servidor de Administração através de software de terceiros levará inevitavelmente a dessincronização dos dados nos nós do aplicativo Kaspersky Security Center distribuído e, consequentemente, ao funcionamento impróprio do aplicativo.

Implementar o Agente de Rede e o aplicativo de segurança

Para gerenciar dispositivos em uma organização, você deve instalar o Agente de Rede em cada um deles. A implementação do Kaspersky Security Center distribuído nos dispositivos corporativos normalmente começa com a instalação do Agente de Rede neles.

No Microsoft Windows XP, o Agente de Rede pode não executar as seguintes operações corretamente: baixar atualizações diretamente dos servidores da Kaspersky (como um ponto de distribuição); funcionar como servidor proxy da KSN (como um ponto de distribuição); e detectar vulnerabilidades de terceiros (caso o Gerenciamento de patches e vulnerabilidades seja usado).

Implementação inicial

Se um Agente de Rede já tiver sido instalado em um dispositivo, a instalação remota de aplicativos naquele dispositivo é executada através deste Agente de Rede. O pacote de distribuição de um aplicativo a ser instalado é transferido através de canais de comunicação entre Agentes de Rede e o Servidor de Administração, junto com as configurações de instalação definidas pelo administrador. Para transferir o pacote de distribuição, é possível usar nós de distribuição de transmissão, ou seja, pontos de distribuição, entrega multicast, etc. Para obter mais detalhes sobre como instalar aplicativos em dispositivos gerenciados com o Agente de Rede já instalado, consulte o conteúdo a seguir nesta seção.

Você pode executar a instalação inicial do Agente de Rede em dispositivos que executam o Windows, usando um dos seguintes métodos:

- Com ferramentas de terceiros para a instalação remota de aplicativos.
- Com políticas de grupo do Windows: usar ferramentas padrão de gerenciamento do Windows para políticas de grupo.
- No modo forçado, usando opções especiais na tarefa de instalação remota do Kaspersky Security Center.
- Enviando aos usuários de dispositivo links para pacotes independentes pelo Kaspersky Security Center. Os pacotes independentes são módulos executáveis que contêm os pacotes de distribuição de aplicativos selecionados com as suas configurações definidas.
- Manualmente, executando os instaladores do aplicativo em dispositivos.

Em plataformas outras do que o Microsoft Windows, você tem de executar a instalação inicial do Agente de Rede em dispositivos gerenciados através da ferramentas de terceiros existentes, ou manualmente, enviando aos usuários um arquivo compactado com um pacote de distribuição pré-configurado. Você pode fazer um upgrade do Agente de Rede para uma nova versão ou instalar outros aplicativos Kaspersky em plataformas que não sejam o Windows, usando Agentes de Rede (já instalado em dispositivos) para executar tarefas de instalação remotas. Neste caso, a instalação é idêntica a nos dispositivos que executam o Microsoft Windows.

Ao selecionar um método e uma estratégia para a implementação de aplicativos em uma rede gerenciada, é necessário considerar um número de fatores (lista parcial):

- Configuração da rede corporativa
- Número total de dispositivos

- A presença de domínios do Windows na rede gerenciada, com a possibilidade de modificar as políticas de grupo do Active Directory nesses domínios

- A ciência das contas de usuário com direitos de administrador locais em dispositivos nos quais a implementação inicial de aplicativos Kaspersky foi planejada (ou seja, a disponibilidade de uma conta de usuário de domínio com direitos de administrador local ou a presença de contas de usuários locais unificadas com direitos de administrador naqueles dispositivos)

- Tipo de conexão e a banda larga de canais de rede entre o Servidor de Administração e redes cliente MSP, assim como a banda larga de canais dentro daquelas redes

- Configurações de segurança aplicadas em dispositivos remotos no início da implementação (tal como o uso do modo UAC e de Compartilhamento de arquivo simples)

Configurar os instaladores

Antes da implementação inicial de aplicativos Kaspersky em uma rede, você deve especificar as configurações de instalação, ou seja, as definidas durante a instalação do aplicativo. Ao instalar o Agente de Rede, você deve especificar, no mínimo, um endereço para a conexão ao Servidor de Administração e as configurações proxy; algumas configurações avançadas também podem ser necessárias. Dependendo do método Instalação que você selecionou, poderá definir configurações de diferentes maneiras. No caso mais simples (instalação interativa manual em um dispositivo selecionado), todas as configurações relevantes podem ser definidas através da interface de usuário do Instalador, portanto, em alguns casos, a implementação inicial pode até ser executada enviando aos usuários um link ao pacote de distribuição do Agente de Rede junto com as configurações (endereço de Servidor de Administração, etc.) que o usuário deve inserir na interface do Instalador.

Este método não é recomendado para uso, já que é inconveniente para os usuários, implicando um alto risco de erros ao definir as configurações manualmente; também é não é utilizável com a instalação silenciosa de aplicativos em grupos de dispositivos. Em geral, o administrador deve especificar os valores das configurações no modo centralizado; estes valores podem ser posteriormente usados para a criação de pacotes independentes. Os pacotes independentes são arquivos compactados de auto-extração que contêm pacotes de distribuição com configurações definidas pelo administrador. Os pacotes autônomos podem ser localizados em recursos que permitam baixar pelos usuários finais (por exemplo, no Servidor Web do Kaspersky Security Center) e pela instalação silenciosa em dispositivos em rede selecionados.

Pacotes de instalação

O primeiro e principal método de definir as configurações da instalação de aplicativos é útil para muitas finalidades e assim adequado para todos os métodos de instalação, para os métodos de instalação com as ferramentas do Kaspersky Security Center e com a maior parte de ferramentas de terceiros. Este método consiste na criação de pacotes de instalação de aplicativos no Kaspersky Security Center.

Os pacotes de Instalação são gerados usando os seguintes métodos:

- Automaticamente, a partir de pacotes de distribuição especificados, com base em *descritores* incluídos (arquivos com a extensão .kud que contêm regras para a instalação e análise de resultados e outras informações)

- A partir dos arquivos executáveis de instaladores ou de instaladores no formato do Microsoft Windows Installer (MSI) são para aplicativos padrão ou suportados

Os pacotes de instalação gerados são organizados hierarquicamente como pastas com subpastas e arquivos. Além do pacote de distribuição original, um pacote de instalação contém configurações editáveis (incluindo as configurações do instalador e as regras para processar os casos tal como necessidade de reiniciar o sistema operacional para concluir a instalação), assim como os módulos auxiliares secundários.

Os valores das configurações de instalação que são específicos para um aplicativo selecionado a ser suportado podem ser especificados na interface do usuário do Console de Administração ao criar um pacote de instalação (mais configurações podem ser encontradas nas propriedades de um pacote de instalação que já foi criado). Ao executar a instalação remota de aplicativos através das ferramentas do Kaspersky Security Center, os pacotes de instalação são entregues aos dispositivos alvo para que ao executar o instalador de um aplicativo, torna todas as configurações definidas pelo administrador à disposição daquele aplicativo. Ao usar as ferramentas de terceiros para a instalação de aplicativos Kaspersky, você somente tem de assegurar a disponibilidade de todo o pacote de instalação no dispositivo alvo, ou seja, a disponibilidade do pacote de distribuição e de suas configurações. Os pacotes de Instalação são criados e armazenados pelo Kaspersky Security Center em uma subpasta dedicada da pasta de dados compartilhados.

Não especifique nenhum detalhe de contas privilegiadas nos parâmetros dos pacotes de instalação.

Para obter instruções sobre a utilização deste método de configuração para aplicativos Kaspersky antes da implementação através de ferramentas de terceiros, consulte a seção "Implementar usando políticas de grupo do Microsoft Windows".

Imediatamente após a instalação do Kaspersky Security Center, alguns pacotes de instalação são automaticamente gerados; eles estão prontos para a instalação e incluem pacotes de Agente de Rede e pacotes de aplicativos de segurança para o Microsoft Windows.

Em alguns casos, a utilização de pacotes de instalação para a implementação de aplicativos em uma rede cliente MSP implica na necessidade de criar pacotes de instalação em Servidores virtuais que correspondam aos clientes MSP. A criação de pacotes de instalação em Servidores virtuais permite usar diferentes configurações de instalação para diferentes clientes MSP. Na primeira instância, isso é útil ao manusear pacotes de instalação de Agente de Rede, já que os Agentes de Rede implementados nas redes de diferentes clientes MSP usam diferentes endereços para conectar-se ao Servidor de Administração. De fato, o endereço de conexão determina o Servidor ao qual o Agente de Rede se conecta.

Além da possibilidade de criar novos pacotes de instalação imediatamente em um Servidor de Administração virtual, o modo de operação principal para os pacotes de instalação em Servidores de Administração virtuais é a "distribuição" de pacotes de instalação do Servidor de Administração principal para os virtuais. Você pode distribuir pacotes de instalação selecionados (ou todos) aos Servidores de Administração virtuais selecionados (incluindo todos os Servidores com um grupo de administração selecionado) utilizando a tarefa de Servidor de Administração correspondente. Você também pode selecionar a lista de pacotes de instalação do Servidor de Administração principal criando um novo Servidor de Administração virtual. Os pacotes selecionados serão imediatamente distribuídos a um Servidor de Administração virtual recentemente criado.

Ao distribuir um pacote de instalação, seu conteúdo não é inteiramente copiado. O repositório de arquivo em um Servidor de Administração virtual, que corresponde ao pacote de instalação sendo distribuído, somente armazena arquivos de configurações que são específicos para aquele Servidor virtual. A parte principal do pacote de instalação (incluindo o pacote de distribuição do aplicativo sendo instalado) permanece inalterada e é somente armazenada no repositório do Servidor de Administração principal. Isto permite aumentar o desempenho do sistema drasticamente e reduzir o volume de disco necessário. Ao tratar pacotes de instalação distribuídos aos Servidores de Administração virtuais (ou seja, executando tarefas de instalação remotas ou criando pacotes de instalação independentes), os dados do pacote de instalação original do Servidor de Administração principal são "mesclados" com os arquivos de configurações, que correspondem ao pacote distribuído no Servidor de Administração virtual.

Embora a chave de licença para um aplicativo possa ser definida nas propriedades do pacote de instalação, é aconselhável evitar este método de distribuição da licença porque é fácil obter acidentalmente o acesso de leitura aos arquivos na pasta. Você deve usar as chaves automaticamente distribuídas ou as tarefas de instalação para chaves de licença.

Propriedades MSI e arquivos de transformação

Outro modo de configurar a instalação na plataforma Windows é o de definir as propriedades MSI e arquivos de transformação. Este método pode ser usado ao executar a instalação através de ferramentas de terceiros para os instaladores no formato do Microsoft Installer, assim como ao executar a instalação através der políticas de grupo do Windows usando ferramentas padrão da Microsoft ou outras ferramentas de terceiros projetadas para tratar políticas de grupo do Windows.

Implementação com ferramentas de terceiros para a instalação remota de aplicativos

Quando qualquer ferramenta para a instalação remota de aplicativos (tal como o Microsoft System Center) estiver disponível em uma organização, é conveniente executar a implementação inicial usando estas ferramentas.

As seguintes ações devem ser executadas:

- Selecione o método para configurar a instalação melhor adequada para a ferramenta implementação a ser usada.
- Defina o mecanismo para a sincronização entre a modificação das configurações dos pacotes de instalação (através da interface do Console de Administração) e a operação das ferramentas de terceiros selecionadas e usadas para a implementação de aplicativos a partir dos dados do pacote de instalação.

Informação geral sobre as tarefas de instalação remotas no Kaspersky Security Center

O Kaspersky Security Center fornece uma ampla gama de métodos para a instalação remota de aplicativos, que são implementados como tarefas de instalação remotas. Você pode criar uma tarefa de instalação remota para um grupo de administração especificado e para dispositivos específicos ou para uma seleção de dispositivos (tais tarefas são exibidas no Console de Administração, na pasta **Tarefas**). Ao criar uma tarefa, você pode selecionar pacotes de instalação (aqueles do Agente de Rede e / ou outro aplicativo) a ser instalado dentro desta tarefa, assim como especificar determinadas configurações que definem o método da instalação remota.

As tarefas para grupos de administração afetam ambos os dispositivos incluídos em um grupo especificado e todos os dispositivos em todos os subgrupos dentro daquele grupo de administração. Uma tarefa cobre dispositivos de Servidores de Administração secundários incluídos em um grupo ou algum dos seus subgrupos se a configuração correspondente estiver ativada na tarefa.

As tarefas para dispositivos específicos atualizam a lista de dispositivos cliente em cada execução de acordo com o conteúdo da seleção no momento em que a tarefa é iniciada. Se uma seleção incluir dispositivos que foram conectados aos Servidores de Administração secundários, a tarefa também será executada naqueles dispositivos.

Para assegurar-se de uma operação bem-sucedida de uma tarefa de instalação remota nos dispositivos conectados aos Servidores de Administração secundários, você deve usar a tarefa de distribuição para distribuir os pacotes de instalação usados por sua tarefa aos Servidores de Administração secundários correspondentes com antecedência.

Implementar usando políticas de grupo do Microsoft Windows

Recomenda-se que você execute a implementação inicial de Agentes de Rede através da políticas de grupo do Microsoft Windows se as seguintes condições forem atendidas:

- Este dispositivo é membro de um domínio Active Directory.
- O acesso ao controlador do domínio é concedido com os direitos de administrador, que lhe permite criar e modificar políticas de grupo do Active Directory.
- Os pacotes de instalação configurados podem ser movidos para a rede que hospeda os dispositivos gerenciados alvo (para uma pasta compartilhada que está disponível para leitura por todos os dispositivos alvo).
- O esquema de implementação permite esperar pelo reinício da próxima rotina de dispositivos alvo antes da implementação inicial de Agentes de Rede neles (ou você pode forçar uma política de grupo do Windows a ser aplicada àqueles dispositivos).

Este esquema de implementação consiste no seguinte:

- O pacote de distribuição do aplicativo no formato do Microsoft Installer (pacote MSI) está localizado em uma pasta compartilhada (uma pasta onde as contas de LocalSystem de dispositivos alvo têm permissões de leitura).
- Na política de grupo do Active Directory, um objeto Instalação é criado para o pacote de distribuição.
- O escopo da instalação é definido especificando a unidade organizacional (UO) e/ou o grupo de segurança, que inclua os dispositivos alvo.
- Na próxima vez que um dispositivo alvo se conecta ao domínio (antes que os usuários do dispositivo se conectem ao sistema), todos os aplicativos instalados são verificados quanto a presença do aplicativo necessário. Se o aplicativo não for encontrado, o pacote de distribuição é baixado do recurso especificado na política e então é instalado.

Uma vantagem deste esquema de implementação é que os aplicativos atribuídos são instalados nos dispositivos alvo enquanto o sistema operacional está sendo carregado, ou seja, até antes que o usuário se conecte ao sistema. Mesmo se um usuário com direitos suficientes remova o aplicativo, ele será reinstalado na próxima inicialização do sistema operacional. Este problema do esquema implementação é que as modificações feitas pelo administrador à política de grupo não entrarão em vigor até que os dispositivos sejam reiniciados (se nenhuma ferramenta adicional estiver envolvida).

Você pode usar políticas de grupo para instalar o Agente de Rede assim como outros aplicativos se os seus respetivos instaladores estiverem no formato do Windows Installer.

> A instalação do Agente de Rede a partir do pacote MSI só é possível no modo silencioso. Não é possível realizar a instalação interativa a partir do pacote MSI.

Além disso, quando você seleciona este método de implementação, terá que avaliar a carga no recurso de arquivo do qual os arquivos serão copiados para os dispositivos após a política de grupo do Windows ter sido aplicada. Você também tem de escolher o método de entrega do pacote de instalação configurado àquele recurso, assim como o método de sincronizar as modificações relevantes nas suas configurações.

Tratar políticas do Microsoft Windows através da tarefa de instalação remota do Kaspersky Security Center

Este método de implementação somente está disponível se o acesso ao controlador do domínio, que contém os dispositivos alvo, for possível do dispositivo a partir do Servidor de Administração, enquanto a pasta compartilhada do Servidor de Administração (a que armazena os pacotes de instalação) for acessível para litura de dispositivos alvo. Devido aos motivos acima, este método de implementação não visto como aplicável ao MSP.

Instalação não assistida de aplicativos através das políticas do Microsoft Windows

O administrador pode criar os objetos necessários para a instalação em uma política de grupo do Windows em seu nome. Neste caso, você tem de carregar os pacotes para um servidor de arquivos independente e fornecer-lhes um link.

Os seguintes cenários de instalação são possíveis:

- O administrador cria um pacote de instalação e define suas propriedades no Console de Administração. Então o administrador copia a toda a subpasta EXEC deste pacote da pasta compartilhada do Kaspersky Security Center para uma pasta em um recurso de arquivo dedicado da organização. O objeto da política de grupo fornece um link para o arquivo MSI deste pacote armazenado em uma subpasta no recurso de arquivo dedicado da organização.

- O administrador baixa o pacote de distribuição do aplicativo (incluindo o do Agente de Rede) da Internet e carrega ele no recurso de arquivo dedicado da organização. O objeto da política de grupo fornece um link para o arquivo MSI deste pacote armazenado em uma subpasta no recurso de arquivo dedicado da organização. As configurações de instalação são definidas ao configurar as propriedades MSI ou ao configurar os arquivos de transformação MST.

Implementação forçada através da tarefa de instalação remota do Kaspersky Security Center

Para executar a implementação inicial do Agente de Rede ou outros aplicativos, é possível forçar a instalação de pacotes de instalação selecionados por meio do uso da tarefa de instalação remota do Kaspersky Security Center, desde que cada dispositivo tenha uma ou mais contas de usuário com direitos de administrador local.

A instalação forçada também pode ser aplicada se os dispositivos não puderem ser diretamente acessados pelo Servidor de Administração: por exemplo, os dispositivos estão em redes isoladas ou estão em uma rede local, enquanto o item Servidor de Administração está na DMZ.

No caso de implementação inicial, o Agente de Rede não é instalado. Portanto, nas configurações da tarefa de instalação remota, não é possível selecionar a distribuição dos arquivos necessários para a instalação do aplicativo com o uso do Agente de Rede. Você só pode optar por distribuir arquivos usando recursos do sistema operacional por meio do Servidor de Administração ou pontos de distribuição.

O serviço do Servidor de Administração deve ser executado em uma conta que tenha privilégios administrativos nos dispositivos de destino. Como alternativa, é possível especificar uma conta que tenha acesso ao compartilhamento admin$ nas configurações da tarefa de instalação remota.

Por padrão, a tarefa de instalação remota se conecta aos dispositivos usando as credenciais da conta sob a qual o Servidor de Administração está sendo executado, por exemplo, a conta para acessar o compartilhamento admin$. Você precisa especificar essa conta nas configurações da tarefa da instalação remota caso o Agente de Rede não esteja instalado nos dispositivos de destino.
Ao criar a tarefa de instalação remota que será executada nos dispositivos baseados no Linux, será sempre necessário especificar uma conta para criar a conexão SSH.

É possível especificar dispositivos de destino explicitamente (com uma lista), por meio de seleção do grupo de administração do Kaspersky Security Center ao qual eles pertencem ou por meio de criação de uma seleção de dispositivos com base em um critério específico. A hora início da instalação é definida pelo agendamento da tarefa. Caso a configuração **Executar tarefas ignoradas** esteja ativada nas propriedades da tarefa, a tarefa poderá ser executada imediatamente após os dispositivos de destino serem ligados ou quando eles forem movidos para o grupo de administração de destino.

A instalação forçada consiste em entregar pacotes de instalação aos dispositivos de destino, cópia subsequente de arquivos para o recurso admin$ em cada um dos dispositivos de destino e registro remoto de serviços de suporte nesses dispositivos. A entrega de pacotes de instalação a dispositivos-alvo é executada por meio de um recurso do Kaspersky Security Center que garante a interação da rede. As seguintes condições devem ser atendidas neste caso:

- Os dispositivos de destino podem ser acessados no lado do Servidor de Administração ou no lado do ponto de distribuição.
- A resolução de nomes para dispositivos de destino funciona corretamente na rede.
- Os compartilhamentos administrativos (admin$) permanecem ativados nos dispositivos-alvo.
- Os seguintes serviços do sistema estão em execução nos dispositivos de destino:
  - Server (LanmanServer)

    Por padrão, este serviço está em execução.
  - DCOM Server Process Launcher (DcomLaunch)
  - RPC Endpoint Mapper (RpcEptMapper)
  - Remote Procedure Call (RpcSs)
- A porta TCP 445 está aberta nos dispositivos de destino para permitir acesso remoto por meio das ferramentas do Windows.

  Os protocolos TCP 139, UDP 137 e UDP 138 são usados por protocolos mais antigos e não são mais necessários para aplicativos atuais.

  Portas de acesso de saída dinâmicas devem ser permitidas no firewall para conexões do Servidor de Administração e pontos de distribuição para dispositivos de destino.
- As configurações de segurança da política de domínio do Active Directory têm permissão para fornecer a operação do protocolo NTLM durante a implementação do Agente de Rede.

- Em dispositivos-alvo que executam o Microsoft Windows XP, o modo Compartilhamento Simples de Arquivo está desativado.

- Nos dispositivos de destino, o compartilhamento de acesso e o modelo de segurança são definidos como *Clássico: os usuários locais se autenticam como eles mesmos*. Ele não pode de forma alguma ser *apenas Visitante: os usuários locais são autenticados como Visitantes*.

- Os dispositivos-alvo são membros do domínio, ou as contas uniformes com direitos de administrador são criadas nos dispositivos-alvo com antecedência.

Para implementar com sucesso o Agente de Rede ou outros aplicativos em um dispositivo que não esteja associado a um domínio do Active Directory do Windows Server 2003 ou posterior, é necessário desativar o UAC remoto nesse dispositivo. O UAC remoto é um dos motivos que impedem que contas administrativas locais acessem admin$, o que é necessário para a implementação forçada do Agente de Rede ou de outros aplicativos. A desativação do UAC remoto não afeta o UAC local.

Durante a instalação em novos dispositivos que ainda não foram alocados à nenhum dos grupos de administração do Kaspersky Security Center, você pode abrir as propriedades da tarefa de instalação remota e especificar o grupo de administração para o qual os dispositivos serão movidos após a instalação do Agente de Rede.

Ao criar uma tarefa de grupo, tenha em mente que cada tarefa de grupo afeta todos os dispositivos em todos os grupos aninhados dentro de um grupo selecionado. Portanto, você deve evitar duplicar tarefas de instalação em subgrupos.

Uma maneira simplificada de criar tarefas para a instalação forçada de aplicativos é a instalação automática. Para fazer isso, você deve abrir as propriedades do grupo de administração, abrir a lista de pacotes de instalação e selecionar aqueles que devem ser instalados nos dispositivos deste grupo. Como resultado, os pacotes de instalação selecionados serão automaticamente instalados em todos os dispositivos neste grupo e em todos os seus subgrupos. O intervalo de tempo sobre o qual os pacotes serão instalados depende da produtividade da rede e o número total de dispositivos na rede.

Para reduzir a carga no Servidor de Administração durante a entrega de pacotes de instalação a dispositivos-alvo, é possível selecionar a instalação por meio dos pontos de distribuição na tarefa de instalação. Observe que este método de instalação coloca uma carga significativa nos dispositivos que atuam como pontos de distribuição. Portanto, é recomendável selecionar os dispositivos que atendam aos requisitos para pontos de distribuição. Se você usar pontos de distribuição, precisará garantir que eles estejam presentes em cada uma das sub-redes isoladas que hospedam os dispositivos de destino.

Usando pontos de distribuição como centros de instalação locais também pode ser útil ao executar a instalação em dispositivos em sub-redes comunicadas com o Servidor de Administração através de um canal de baixa potência enquanto um canal mais amplo esteja disponível entre os dispositivos na mesma sub-rede.

O espaço livre em disco na partição com a pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit deve exceder muitas vezes o tamanho total dos pacotes de distribuição dos aplicativos instalados.

Executar pacotes independentes criados pelo Kaspersky Security Center

Os métodos acima descritos da implementação inicial do Agente de Rede e de outros aplicativos nem sempre podem ser implementados porque não é possível atender todas as condições aplicáveis. Em tais casos, você pode criar um arquivo executável comum denominado como *pacote de instalação independente* através do Kaspersky Security Center, usando pacotes de instalação com as configurações de instalação relevantes que foram preparados pelo administrador. Um pacote de instalação independente pode ser publicado em um da Servidor da Web interno (incluído no Kaspersky Security Center) se isto for considerado razoável (fora do acesso àquele Servidor Web que foi configurado para usuários de dispositivo alvo), ou em um Servidor da Web exclusivamente implementado incluído no Kaspersky Security Center Web Console. Você também pode copiar pacotes independentes para outro Servidor da Web.

Você pode usar o Kaspersky Security Center para enviar aos usuários selecionados uma mensagem de e-mail contendo um link para o arquivo do pacote independente no Servidor da Web no momento em uso, solicitando-lhes que executem o arquivo (no modo interativo ou com a chave "-s" para a instalação silenciosa). Você pode anexar o pacote de instalação independente a uma mensagem de e-mail e então enviá-lo aos usuários dos dispositivos que não tenham acesso ao Servidor da Web. O administrador também pode copiar o pacote independente em um dispositivo externo, entregá-lo a um dispositivo relevante, e então executá-lo mais tarde.

Você pode criar um pacote independente a partir de um pacote de Agente de Rede, de um pacote de outro aplicativo (por exemplo, o aplicativo de segurança), ou ambos. Se o pacote independente foi criado a partir do Agente de Rede e de outro aplicativo, a instalação inicia com o Agente de Rede.

Ao criar um pacote independente com o Agente de Rede, você pode especificar o grupo de administração ao qual os novos dispositivos (aqueles que não foram alocados à nenhum dos grupos de administração) serão automaticamente movidos quando a instalação do Agente de Rede for concluída neles.

Os pacotes independentes podem ser executados no modo interativo (por padrão), exibindo o resultado da instalação de aplicativos que eles contêm, ou eles podem ser executados no modo silencioso (quando executados com a chave "-s"). O modo silencioso pode ser usado para a instalação de scripts, por exemplo, de scripts configurados para ser executados após a implementação da imagem do sistema operacional. O resultado da instalação no modo silencioso é determinado pelo código de retorno do processo.

Opções para a instalação manual de aplicativos

Os administradores ou os usuários experientes podem instalar os aplicativos manualmente no modo interativo. Eles podem usar pacotes de distribuição originais ou pacotes de instalação gerados a partir deles e armazenados na pasta compartilhada do Kaspersky Security Center. Por padrão, instaladores são executados no modo interativo e solicitam aos usuários todos os valores necessários. No entanto, ao executar o processo setup.exe a partir da raiz de um pacote de instalação com a chave "-s", o instalador será executado no modo silencioso e com as configurações que foram definidas ao configurar o pacote de instalação.

Ao executar o setup.exe a partir da raiz de um pacote de instalação, o pacote será primeiro copiado para uma pasta local temporária e, a seguir, o instalador do aplicativo será executado a partir da pasta local.

Como criar um arquivo MST

Para transformar o conteúdo de um pacote MSI e aplicar configurações personalizadas a um arquivo MSI existente, você deve criar um arquivo de transformação no formato MST. Para isso, use o editor Orca.exe, incluído no SDK do Windows.

Para criar um arquivo MST:

1. Execute o editor Orca.exe.
2. Acesse a guia **Arquivo** e, no menu, clique em **Abrir**.
3. Selecione o arquivo Kaspersky Network Agent.msi.
4. Acesse a guia **Transformação** e, no menu, selecione **Nova transformação**.
5. Na coluna **Tabelas**, selecione **Propriedade** e escreva os seguintes valores:
   - *EULA=1*
   - *SERVERADDRESS=<endereço do Servidor de Administração>*

   Clique no botão **Salvar**.
6. Acesse a guia **Transformar** e, no menu, selecione **Gerar transformação**.
7. Na janela exibida, especifique um nome do arquivo de transformação criado e clique no botão **Salvar**.

O arquivo MST é salvo.

Instalação remota de aplicativos em dispositivos com o Agente de Rede instalado

Se um Agente de Rede operável conectado ao Servidor de Administração principal (ou a algum dos seus Servidores secundários) for instalado em um dispositivo, você poderá fazer um upgrade do Agente de Rede neste dispositivo, assim como instalar, atualizar ou remover qualquer aplicativo compatível através do Agente de Rede.

Você pode ativar esta opção ao selecionar a caixa de seleção **Usando Agente de Rede** nas propriedades da tarefa de instalação remota.

Se esta caixa de seleção for selecionada, os pacotes de instalação com configurações de instalação definidas pelo administrador serão transferidos para os dispositivos alvo através dos canais de comunicação entre o Agente de Rede e o Servidor de Administração.

Para otimizar a carga do Servidor de Administração e minimizar o tráfego entre o Servidor de Administração e os dispositivos, é útil atribuir pontos de distribuição em cada rede remota ou em cada domínio emissor (consulte as seções Sobre os pontos de distribuição e Criar uma estrutura de grupos de administração e atribuir pontos de distribuição). Neste caso, os pacotes de instalação e as configurações do instalador são distribuídos a partir do Servidor de Administração para os dispositivos alvo através de pontos de distribuição.

Além disso, você pode usar pontos de distribuição para transmitir (multicast) a entrega de pacotes de instalação, que permite reduzir significativamente o tráfego de rede ao implementar aplicativos.

Ao transferir pacotes de instalação para dispositivos alvo através dos canais de comunicação entre os Agentes de Rede e o Servidor de Administração, todos os pacotes de instalação que tenham sido preparados para transferência, também serão colocados em cache na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\FTServer. Ao usar múltiplos grandes pacotes de instalação de vários tipos e ao envolver um grande número de pontos de distribuição, o tamanho desta pasta pode aumentar drasticamente.

Os arquivos não podem ser excluídos da pasta FTServer manualmente. Quando os pacotes de instalação originais forem excluídos, os dados correspondentes serão automaticamente excluídos da pasta FTServer.

Todos os dados recebidos nos pontos de distribuição são salvos na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1103\$FTCITmp.

Os arquivos não podem ser excluídos da pasta de $FTCITmp manualmente. Quando as tarefas usando dados desta pasta forem concluídas, o conteúdo desta pasta será automaticamente excluído.

Como os pacotes de instalação são distribuídos sobre os canais de comunicação entre o Servidor de Administração e os Agentes de Rede a partir de um repositório intermediário em um formato otimizado para transferências na rede, nenhuma modificação é permitida nos pacotes de instalação armazenados na pasta original de cada pacote de instalação. Estas modificações não serão automaticamente registradas pelo Servidor de Administração. Se você tiver de modificar os arquivos de pacotes de instalação manualmente (embora seja recomendado evitar este cenário), deverá editar qualquer configuração necessária de um pacote de instalação no Console de Administração. Editar as configurações de um pacote de instalação no Console de Administração faz com que o Servidor de Administração atualize a imagem do pacote na memória no cache que foi preparado para a transferência aos dispositivos alvo.

O gerenciamento do dispositivo reinicia na tarefa de instalação remota

Os dispositivos muitas vezes precisam de um reinício para concluir a instalação remota de aplicativos (em particular no Windows).

Caso a tarefa de instalação remota do Kaspersky Security Center seja usada, no assistente para novas tarefas ou na janela de propriedades da tarefa que foi criada (seção **Reinício do sistema operacional**), será possível selecionar a ação a ser executada quando o dispositivo Windows precisar ser reiniciado:

- **Não reiniciar o dispositivo**. Neste caso, nenhum reinício automático será executado. Para concluir a instalação, você deve reiniciar o dispositivo (por exemplo, manualmente ou através da tarefa de gerenciamento de dispositivo). As informações sobre o reinício necessário serão salvas nos resultados da tarefa e no status do dispositivo. Esta opção é adequada para tarefas de instalação em servidores e em outros dispositivos onde a operação contínua é crítica.

- **Reiniciar o dispositivo**. Neste caso, o dispositivo sempre é reiniciado automaticamente se um reinício for necessário para a conclusão da instalação. Esta opção é útil para tarefas de instalação em dispositivos que fornecem pausas regulares na sua operação (desligamento ou reinício).

- **Perguntar ao usuário o que fazer**. Neste caso, o lembrete de reinício é exibido na tela do dispositivo cliente, solicitando ao usuário que o reinicie manualmente. Algumas configurações avançadas podem ser definidas para esta opção: texto da mensagem para o usuário, a frequência de exibição da mensagem e o intervalo de tempo após o qual um reinício será forçado (sem a confirmação do usuário). A opção **Perguntar ao usuário o que fazer** é a mais adequada para estações de trabalho onde os usuários precisam da possibilidade de selecionar a hora mais conveniente para um reinício.

Adequabilidade da atualização dos bancos de dados em um pacote de instalação de um aplicativo de antivírus

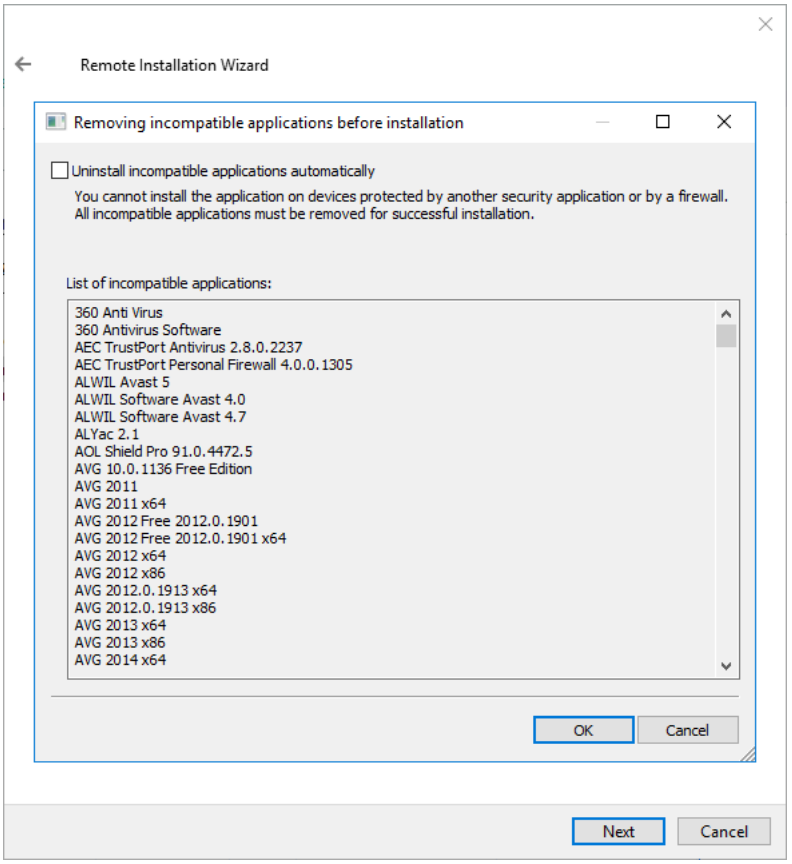
Antes de iniciar a implementação da proteção, você deve ter em mente a possibilidade de atualizar os bancos de dados antivírus (incluindo os módulos de patches automáticas), fornecidos junto com o pacote de distribuição do aplicativo de segurança. É útil atualizar os bancos de dados no pacote de instalação do aplicativo antes de iniciar a implementação (por exemplo, usando o comando correspondente no menu de contexto de um pacote de instalação selecionado). Isto reduzirá o número de reinícios necessários para a conclusão da implementação da proteção em dispositivos alvo. Se a sua instalação remota envolve pacotes de instalação que foram retransmitidos aos Servidores virtuais pelo Servidor de Administração principal, você precisa somente atualizar os bancos de dados no pacote original no Servidor principal. Neste caso, você não tem de atualizar os bancos de dados em pacotes encaminhados em Servidores virtuais.

Removendo aplicativos de segurança de terceiros incompatíveis

A Instalação de aplicativos de segurança da Kaspersky através do Kaspersky Security Center pode necessitar a remoção de software de terceiros incompatível com o aplicativo sendo instalado. Há dois modos principais para remover os aplicativos de terceiros.

Remoção automática de aplicativos incompatíveis usando o instalador

Ao executar o instalador, ele mostra uma lista de aplicativos incompatíveis com um aplicativo da Kaspersky:



A lista de aplicativos incompatíveis exibida no Assistente de instalação remota

O Kaspersky Security Center detecta softwares incompatíveis. Assim, você pode selecionar a caixa de seleção **Desinstalar automaticamente aplicativos incompatíveis** para continuar a instalação. Se você desmarcar esta caixa de seleção e não desinstalar o software incompatível, um erro ocorre e o aplicativo Kaspersky não é instalado.

A remoção automática de aplicativos incompatíveis tem suporte em vários tipos de instalação.

Remover aplicativos incompatíveis através de uma tarefa dedicada

Para remover aplicativos incompatíveis, use a tarefa *Desinstalar aplicativo remotamente*. Esta tarefa deve ser executada nos dispositivos antes da execução da tarefa de instalação do aplicativo de segurança. Por exemplo, na tarefa de instalação, você pode selecionar **Na conclusão de outra tarefa** como tipo de agendamento em que a outra tarefa é *Desinstalar aplicativo remotamente*.

Este método da desinstalação é útil quando o instalador do aplicativo de segurança não puder remover apropriadamente um aplicativo incompatível.

Remoção do Agente de Rede protegido por senha usando o prompt de comando

Para desinstalar remotamente o Agente de Rede para o qual uma senha de desinstalação foi definida, é possível usar o prompt de comando.

Se você perder ou esquecer a senha do Agente de Rede protegido por senha instalado no dispositivo que não está mais sob o gerenciamento da Kaspersky Security Center, não será possível remover o Agente de Rede usando o utilitário klmover, a ferramenta Cleaner (cleaner.exe) ou o prompt de comando. Nesse caso, será necessário reinstalar o sistema operacional no dispositivo com o Agente de Rede instalado e protegido por senha.

Para desinstalar o Agente de Rede via prompt de comando:

1. Converta a senha de desinstalação em um código hexadecimal.

   Use um recurso da Internet, ambiente de programação, editor de texto ou outra ferramenta adequada para converter a senha em um código hexadecimal.

   > Certifique-se de que o delimitador de saída usado para separar o código hexadecimal gerado em partes esteja definido como `00`. Por exemplo, o código hexadecimal `51 77 65 72 74 79` está incorreto, e o código hexadecimal `5100770065007200740079 00` está correto.

2. Digite o seguinte comando no prompt de comando e pressione **ENTER**:

   `msiexec.exe /x{<código do produto>} /qn KLUNINSTPASSWD=<código hexadecimal da senha de desinstalação>`

   É possível encontrar o código do produto do Agente de Rede na tabela abaixo.

Códigos do produto do Agente de Rede

Localização	Código do produto
Árabe	{FA7BF140-F356-404A-BDA3-3EF0878D7C63}
Búlgaro	{4DBF6741-FA51-4C14-AFD2-B7D9246995F6}
Tcheco	{478A6A0B-D177-4402-B703-808C05C56B13}
Inglês	{BCF4CF24-88AB-45E1-A6E6-40C8278A70C5}
Francês	{2924BEDA-E0D7-4DAF-A224-50D2E0B12F5B}
Alemão	{2F383CB3-6D7C-449D-9874-164E49E1E0F5}
Húngaro	{8899A4D4-D678-49F8-AD96-0B784F58D355}
Italiano	{DC3A3164-36B3-4FB4-B7BF-16A41C35A728}
Japonês	{790C176F-7780-4C84-8B9C-455F5C0E61C5}
Coreano	{70812A40-973B-4DA1-96B9-C2011280CD99}
Polonês	{1A7B331A-ABBE-4230-995E-BCD99C5A18CF}
Português	{0F05E4E5-5A89-482C-9A62-47CC58643788}
Romeno	{FF802D76-E241-41D3-AAB4-DC7FBD659446}
Russo	{ED1C2D7E-5C7A-48D8-A697-57D1C080ABA7}
Chinês simplificado	{FBD7C01E-49CB-4182-8714-9DB1EAE255CB}
Espanhol	{F03982CF-1C5C-4E12-9F9E-D36C35E62402}
Espanhol-mx	{29748B5F-D88A-4933-B614-1CCCD6EFB0B7}
Chinês tradicional	{F6AD731A-36B4-4739-B1D4-70D6EDA35147}
Turco	{2475A66D-698B-4050-93FF-9B48EE82E2BA}

Usar as ferramentas da instalação remota de aplicativos no Kaspersky Security Center para executar arquivos executáveis relevantes em dispositivos gerenciados

Usando o Assistente de novo pacote, você pode selecionar qualquer arquivo executável e definir as configurações da linha de comando para ele. Para isto você pode adicionar ao pacote de instalação o próprio arquivo selecionado ou a pasta inteira na qual este arquivo está armazenado. Então você deve criar a tarefa de instalação remota e selecionar o pacote de instalação que foi criado.

Enquanto a tarefa estiver em execução, o arquivo executável especificado com as configurações definidas do prompt de comando serão executadas em dispositivos alvo.

Se você usar instaladores no formato do Microsoft Windows Installer (MSI), o Kaspersky Security Center analisa os resultados da instalação por meio de ferramentas padrão.

Se a licença do Gerenciamento de patches e vulnerabilidades estiver disponível, o Kaspersky Security Center (ao criar um pacote de instalação de qualquer aplicativo suportado no ambiente corporativo), também usa as regras para a instalação e análise dos resultados de instalação que estão no seu banco de dados atualizável.

De outra forma, a tarefa padrão para arquivos executáveis espera pela conclusão do processo de execução e de todos os seus processos secundários. Após a conclusão de todos os processos em execução, a tarefa será concluída dom êxito a despeito do código de retorno do processo inicial. Para modificar tal comportamento desta tarefa, antes de criar a tarefa, você deve modificar manualmente os arquivos .kpd gerados pelo Kaspersky Security Center na pasta do pacote de instalação recentemente criado e suas subpastas.

Os arquivos .kpd usam codificação ASCII. Os arquivos .kud usam codificação Unicode.

Para que a tarefa não espere pela conclusão do processo em execução, defina o valor da configuração Wait como 0 na seção [SetupProcessResult]:

```
[SetupProcessResult]
Wait=0
```

Para a tarefa somente esperar pela conclusão do processo em execução no Windows, não para a conclusão de todos os processos secundários, defina o valor da configuração WaitJob como 0 na seção [SetupProcessResult], por exemplo:

```
[SetupProcessResult]
WaitJob=0
```

Para que a tarefa seja concluída com sucesso ou retorne um erro dependendo do código de retorno do processo em execução, crie um arquivo executável .bat que salve o código de erro em um arquivo, por exemplo:

```
echo [ResponseResult] > setup.log
echo ResultCode=2 >> setup.log
exit 0
```

E, depois, modifique os arquivos .kud que foram gerados pelo Kaspersky Security Center na pasta do pacote de instalação recém-criado:

```
[SetupMainResult]
File=setup.log
Section=ResponseResult
Value=ResultCode
[SetupMainResult_SuccessCodes]
0=Instalação concluída com êxito.
[SetupMainResult_ErrorCodes]
1=Erro de script de instalação
2=Erro personalizado
```

Neste caso, qualquer outro código que os dos listados resultará em um erro retornado.

Para exibir uma sequência de caracteres com um comentário sobre a conclusão bem sucedida da tarefa ou sobre um erro nos resultados da tarefa, insira breves descrições dos erros que correspondem aos códigos de retorno do processo na seção [SetupProcessResult_SuccessCodes] e [SetupProcessResult_ErrorCodes], por exemplo:

```
[SetupProcessResult_SuccessCodes]
0 = Instalação concluída com êxito
3010=Um reinício é necessário para concluir a instalação
[SetupProcessResult_ErrorCodes]
1602=Instalação cancelada pelo usuário
1603=Erro fatal durante a instalação
```

Para usar as ferramentas do Kaspersky Security Center para gerenciar o reinício do dispositivo (se um reinício for necessário para concluir uma operação), liste os códigos de retorno do processo que indicam que um reinício deve ser executado, na seção [SetupProcessResult_NeedReboot]:

```
[SetupProcessResult_NeedReboot]
3010=
```

Monitorar a implementação

Para monitorar a implementação do Kaspersky Security Center e assegurar-se de que um aplicativo de segurança e um Agente de Rede sejam instalados nos dispositivos gerenciados, você deve verificar o sinal luminoso na seção **Implementação**. Este sinal luminoso está localizado no espaço de trabalho do nó Servidor de Administração na janela principal do Console de Administração. O sinal luminoso reflete o status da implementação atual. O número de dispositivos com Agente de Rede e aplicativos de segurança instalados é exibido ao lado do sinal luminoso. Quando qualquer tarefa de instalação estiver em execução, você pode monitorar aqui seu andamento. Se algum erro de instalação ocorrer, o número de erros é aqui exibido. Você pode exibir os detalhes de qualquer erro clicando no link.

Você também pode usar o esquema de implementação no espaço de trabalho da pasta **Dispositivos gerenciados** na guia **Grupos**. O gráfico reflete o processo de implementação, mostrando o número de dispositivos sem o Agente de Rede, com o Agente de Rede, ou com o Agente de Rede e um aplicativo de segurança.

Para obter mais detalhes sobre o andamento da implementação (ou da operação de uma tarefa de instalação específica) abra a janela de resultados da tarefa de instalação remota relevante: clique com o botão direito do mouse na tarefa e selecione **Resultados** no menu de contexto. A janela exibe duas listas: a superior contém os status da tarefa em dispositivos, enquanto a mais baixa contém os eventos de tarefas no dispositivo que está atualmente selecionado na lista superior.

As informações sobre erros de implementação são adicionadas ao Log de Eventos Kaspersky no Servidor de Administração. As informações sobre os erros também estão disponíveis na seleção correspondente de eventos na pasta **Relatórios e notificações**, na subpasta **Eventos**.

Configurar os instaladores

Esta seção fornece informações sobre os arquivos de instaladores do Kaspersky Security Center e as configurações de instalação, assim como recomendações sobre como instalar o Servidor de Administração e o Agente de Rede no modo silencioso.

Informações gerais

Os Instaladores dos componentes do Kaspersky Security Center 14.2 (Servidor de Administração, Agente de Rede e Console de Administração) são desenvolvidos com base na tecnologia do Windows Installer. Um pacote MSI é o núcleo de um instalador. Este formato de empacotar permite usar todas das vantagens fornecidas pelo Windows Installer: dimensionalidade, disponibilidade de um sistema de correção, sistema de transformação, instalação centralizada através de soluções de terceiros e o registro transparente com o sistema operacional.

Instalação em modo silencioso (com um arquivo de resposta)

Os instaladores do Servidor de Administração e do Agente de Rede têm o recurso de funcionar com o arquivo de resposta (ss_install.xml), onde os parâmetros para a instalação no modo silencioso sem a participação de usuário estão integradas. O arquivo ss_install.xml está localizado na mesma pasta que o pacote MSI; ele é usado automaticamente durante a instalação no modo silencioso. Você pode ativar o modo de instalação silenciosa com a tecla de linha de comando "/s".

Uma visão geral de uma execução de exemplo segue:

```
setup.exe /s
```

Antes de iniciar o instalador no modo silencioso, leia o Contrato de Licença do Usuário Final (EULA). Caso o kit de distribuição do Kaspersky Security Center não inclua um arquivo TXT com o texto do EULA, é possível baixá-lo no site da Kaspersky.

O arquivo ss_install.xml é uma instância do formato interno dos parâmetros do instalador do Kaspersky Security Center. Os pacotes de distribuição contêm o arquivo ss_install.xml com os parâmetros padrão.

Não modifique manualmente o arquivo ss_install.xml. Este arquivo pode ser modificado pelas ferramentas do Kaspersky Security Center ao editar os parâmetros de pacotes de instalação no Console de Administração.

Para modificar o arquivo de resposta para instalação do Servidor de Administração:

1. Abra o pacote de distribuição do Kaspersky Security Center. Caso use um pacote completo com arquivo EXE, é necessário descompactá-lo.

2. A partir da pasta Servidor, abra a linha de comando e, em seguida, execute o seguinte comando:
   ```
   setup.exe /r ss_install.xml
   ```
   O instalador do Kaspersky Security Center é iniciado.

3. Siga as etapas do assistente para configurar a instalação do Kaspersky Security Center.

   Ao concluir o assistente, o arquivo de resposta é modificado automaticamente de acordo com as novas configurações especificadas.

Instalação do Agente de Rede no modo silencioso (sem um arquivo de resposta)

Você pode instalar o Agente de Rede com um pacote .msi único, especificando os valores das propriedades MSI no modo padrão. Este cenário permite que o Agente de Rede seja instalado usando políticas de grupo.

Não renomeie o pacote de instalação Kaspersky Network Agent.msi. Renomear este pacote pode causar erros de instalação durante futuras atualizações do Agente de Rede.

Para evitar conflitos entre configurações definidas através dos parâmetros MSI e os parâmetros definidos no arquivo de resposta, você pode desativar o arquivo de resposta ao definir a propriedade `DONT_USE_ANSWER_FILE=1`. O arquivo MSI está localizado no pacote de distribuição do Kaspersky Security Center, na pasta Packages\NetAgent\exec. Um exemplo de uma execução do instalador do Agente de Rede com um pacote .msi é como segue.

A instalação do Agente de Rede no modo silencioso requer o aceite dos termos do Contrato de Licença de Usuário Final. Use o parâmetro `EULA=1` somente se você tiver lido, entende e aceita por completo os termos do Contrato de Licença do Usuário Final.

Exemplo:
```
msiexec /i "Kaspersky Network Agent.msi" /qn DONT_USE_ANSWER_FILE=1 SERVERADDRESS=kscserver.mycompany.com EULA=1
```

Você também pode definir os parâmetros de instalação para um pacote .msi ao preparar o arquivo de resposta com antecedência (um com uma extensão .mst). Este comando aparece como segue:

Exemplo:
```
msiexec /i "Kaspersky Network Agent.msi" /qn TRANSFORMS=test.mst;test2.mst
```

Você pode especificar vários arquivos de resposta em um comando único.

Se você quiser atualizar o Agente de Rede usando o Windows Installer, execute o seguinte comando:

```
msiexec /i "Kaspersky Network Agent.msi" /qn /l*vx c:\windows\temp\nag_inst.log
REINSTALL=ALL REINSTALLMODE=vomus /norestart
```

Configuração de instalação parcial através de setup.exe

Ao executar a instalação de aplicativos por meio do setup.exe, é possível adicionar os valores de qualquer propriedade de MSI ao pacote MSI.

Este comando aparece como segue:

Exemplo:
```
/v"PROPERTY_NAME1=PROPERTY_VALUE1 PROPERTYNAME2=PROPERTYVALUE2"
```

Parâmetros de instalação do Servidor de Administração

A tabela abaixo descreve as propriedades MSI que você pode configurar ao instalar o Servidor de Administração. Todos os parâmetros são opcionais, exceto para o EULA e PRIVACYPOLICY.

Parâmetros da instalação do Servidor de Administração no modo silencioso

Propriedade de MSI	Descrição	Valores disponíveis
EULA	Aceitação dos termos do Contrato de Licença (necessária)	• 1 – Eu li, entendo e aceito por completo os termos do Contrato de Licença do Usuário Final. • Outro valor ou nenhum valor – Não aceito os termos do Contrato de Licença (a instalação não é executada).
PRIVACYPOLICY	Aceitação dos termos da Política de Privacidade (necessária)	• 1 – Estou ciente e concordo que meus dados serão tratados e transmitidos (inclusive para países terceiros), como descrito na Política de Privacidade. Confirmo que Eu li e entendo por completo a Política de Privacidade. • Outro valor ou nenhum valor – Não aceito os termos da Política de Privacidade (a instalação não é executada).
INSTALLATIONMODETYPE	Tipo de instalação do Servidor de Administração	• Padrão. • Personalizado.
INSTALLDIR	Pasta de instalação do aplicativo	Valor da sequência de caracteres.
ADDLOCAL	Lista de componentes para instalar (separado por vírgulas)	CSAdminKitServer, NAgent, CSAdminKitConsole, NSAC, MobileSupport, KSNProxy, SNMPAgent, GdiPlusRedist, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86. Lista mínima de componentes suficientes para a instalação correta do Servidor de Administração: `ADDLOCAL=CSAdminKitServer, CSAdminKitConsole, KSNProxy, Microsoft_VC90_CRT_x86, Microsoft_VC100_CRT_x86`
NETRANGETYPE	Tamanho da rede	• NRT_1_100 – De 1 a 100 dispositivos. • NRT_100_1000 – De 101 a 1000 dispositivos. • NRT_GREATER_1000 – Mais de 1000 dispositivos.
SRV_ACCOUNT_TYPE	Modo de especificar o usuário para a operação do serviço Servidor de Administração	• SrvAccountDefault – A conta de usuário será criada automaticamente. • SrvAccountUser – A conta de usuário é definida manualmente.
SERVERACCOUNTNAME	Nome do usuário para o serviço	Valor da sequência de caracteres.
SERVERACCOUNTPWD	Senha de usuário para o serviço	Valor da sequência de caracteres.
DBTYPE	Tipo de banco de dados	• MySQL – Um banco de dados MySQL ou MariaDB será usado. • MSSQL – Um banco de dados do Microsoft SQL Server (SQL Express) será usado.
MYSQLSERVERNAME	Nome completo do servidor MySQL ou MariaDB	Valor da sequência de caracteres.
MYSQLSERVERPORT	Número de uma porta para conexão ao MySQL Server ou MariaDB	Valor numérico.
MYSQLDBNAME	Nome do banco de dados do MySQL Server ou MariaDB	Valor da sequência de caracteres.
MYSQLACCOUNTNAME	Nome do usuário para a conexão ao banco de dados do MySQL Server ou MariaDB	Valor da sequência de caracteres.
MYSQLACCOUNTPWD	Senha do usuário para a conexão ao banco de dados do MySQL Server ou MariaDB	Valor da sequência de caracteres.
MSSQLCONNECTIONTYPE	Tipo de uso do banco de dados MSSQL	• InstallMSSEE – Instalar a partir de um pacote. • ChooseExisting – Usar o servidor instalado.
MSSQLSERVERNAME	Nome completo da instância do SQL Server	Valor da sequência de caracteres.

Propriedade de MSI	Descrição	Valores disponíveis
MSSQLDBNAME	Nome do banco de dados do SQL Server	Valor da sequência de caracteres.
MSSQLAUTHTYPE	Método de autenticação para a conexão ao SQL Server	• Windows. • SQLServer.
MSSQLACCOUNTNAME	Nome do usuário para a conexão ao SQL Server no modo SQLServer	Valor da sequência de caracteres.
MSSQLACCOUNTPWD	Senha do usuário para a conexão ao SQL Server no modo SQLServer	Valor da sequência de caracteres.

CREATE_SHARE_TYPE	Método para especificar a pasta compartilhada	• Create – Criar uma nova pasta compartilhada. Neste caso, as seguintes propriedades devem ser definidas:
		  • SHARELOCALPATH – Caminho a uma pasta local.
		  • SHAREFOLDERNAME – Nome da rede de uma pasta.
		• Null – A propriedade EXISTSHAREFOLDERNAME deve ser especificada.

EXISTSHAREFOLDERNAME	Caminho completo para uma pasta compartilhada existente	Valor da sequência de caracteres.
SERVERPORT	O número da porta usado para conectar ao Servidor de Administração	Valor numérico.
SERVERSSLPORT	Número de uma porta para estabelecer a conexão SSL ao Servidor de Administração	Valor numérico.
SERVERADDRESS	Administration Server address	Valor da sequência de caracteres.
SERVERCERT2048BITS	Tamanho da chave para o certificado do Servidor de Administração (bits)	• 1 – O tamanho da chave para o certificado do Servidor de Administração é de 2048 bits. • 0 – O tamanho da chave para o certificado do Servidor de Administração é de 1024 bits. • Se nenhum valor for especificado – O tamanho da chave para o certificado do Servidor de Administração é de 2048 bits.
MOBILESERVERADDRESS	Endereço do Servidor de Administração para a conexão de dispositivos móveis; ignorado se o componente MobileSupport não foi selecionado	Valor da sequência de caracteres.

Parâmetros de instalação do Agente de Rede

A tabela abaixo descreve as propriedades MSI que você pode configurar ao instalar o Agente de Rede. Todos os parâmetros são opcionais, exceto para o EULA e SERVERADDRESS.

Parâmetros da instalação do Agente de Rede no modo silencioso

Propriedade de MSI	Descrição	Valores disponíveis
EULA	Aceitação dos termos do Contrato de Licença	• 1 – Confirmo que li, entendi e aceito totalmente os termos e condições deste Contrato de Licença de Usuário Final. • 0 – Eu não aceito os termos do Contrato de Licença (a instalação não é executada). • Nenhum valor – Eu não aceito os termos do Contrato de Licença (a instalação não é executada).
DONT_USE_ANSWER_FILE	Ler as configurações de instalação a partir do arquivo de resposta	• 1 – Não usar. • Outro valor ou sem valor – Leitura.
INSTALLDIR	Caminho para a pasta de instalação do Agente de Rede	Valor da sequência de caracteres.
SERVERADDRESS	Endereço do Servidor de Administração (necessário)	Valor da sequência de caracteres.
SERVERPORT	Número de uma porta para conexão ao Servidor de Administração	Valor numérico.
SERVERSSLPORT	Número da porta para a conexão criptografada ao Servidor de Administração usando protocolo SSL	Valor numérico.
USESSL	Decida se deseja usar uma conexão SSL	• 1 – Usar. • Outro valor ou sem valor – Não usar.
OPENUDPPORT	Decida se deseja abrir uma porta UDP	• 1 – Abrir. • Outro valor ou sem valor – Não abrir.
UDPPORT	Número da porta UDP	Valor numérico.
USEPROXY	Se um servidor proxy deve ser usado. Para fins de compatibilidade, não é recomendável especificar as configurações de conexão proxy nas configurações do pacote de instalação do Agente de Rede.	• 1 – Usar. • Outro valor ou sem valor – Não usar.
PROXYLOCATION (PROXYADDRESS:PROXYPORT)	Endereços de proxy e número de uma porta para conexão ao servidor de proxy	Valor da sequência de caracteres.
PROXYLOGIN	Conta para a conexão ao servidor proxy	Valor da sequência de caracteres.
PROXYPASSWORD	Senha da conta para conexão ao servidor proxy (Não especifique nenhum detalhe de contas privilegiadas nos parâmetros dos pacotes de instalação.)	Valor da sequência de caracteres.
GATEWAYMODE	Modo de uso do gateway de conexão	• 0 – Não usar gateway de conexão. • 1 – Usar este Agente de Rede como gateway de conexão. • 2 – Conectar-se ao Servidor de Administração usando o gateway de conexão.
GATEWAYADDRESS	Endereço gateway-conexão	Valor da sequência de caracteres.
CERTSELECTION	Método para receber um certificado	• GetOnFirstConnection – Receber um certificado a partir do Servidor de Administração. • GetExistent – Selecionar um certificado existente; se esta opção estiver selecionada, a propriedade CERTFILE deve ser especificada.
CERTFILE	Caminho para o arquivo do certificado	Valor da sequência de caracteres.

Propriedade de MSI	Descrição	Valores disponíveis
VMVDI	Ativar o modo dinâmico para a Virtual Desktop Infrastructure (VDI)	• 1 – Ativar. • 0 - Não ativar. • Sem valor – Não ativar.
VMOPTIMIZE	Define as configurações do Agente de Rede são ideais para o hypervisor	• 1 – Ativar. • 0 - Não ativar. • Sem valor – Não ativar.
LAUNCHPROGRAM	Decida se deseja iniciar o serviço Agente de Rede após a instalação. O parâmetro é ignorado se VMVDI=1	• 1 – Iniciar. • Outro valor ou sem valor – Não iniciar.
NAGENTTAGS	Tag para o Agente de Rede (tem prioridade sobre a tag fornecida no arquivo de resposta)	Valor da sequência de caracteres.

Infraestrutura virtual

O Kaspersky Security Center é compatível com o uso de máquinas virtuais. Você pode instalar o Agente de Rede e do aplicativo de segurança em cada máquina virtual, assim como a proteção de máquinas virtuais em nível de hipervisor. No primeiro caso, você pode usar o aplicativo de segurança padrão ou o Kaspersky Security for Virtualization Light Agent para proteger suas máquinas virtuais. No segundo caso, você pode usar o Kaspersky Security for Virtualization Agentless.

O Kaspersky Security Center comporta reversões de máquinas virtuais ao estado anterior.

Dicas sobre como reduzir a carga em máquinas virtuais

Ao instalar o Agente de Rede em uma máquina virtual, você é aconselhado a considerar a desativação de alguns recursos do Kaspersky Security Center que parecem ser de um pouco uso para máquinas virtuais.

Ao instalar o Agente de Rede em uma máquina virtual ou em um modelo destinado para a geração de máquinas virtuais, recomendamos executar as seguintes ações:

- Se estiver executando uma instalação remota, na janela Propriedades do pacote de instalação do Agente de Rede na seção **Avançado**, selecione a opção **Otimizar as configurações para VDI**.
- Se você estiver executando uma instalação interativa por meio de um assistente, na janela assistente, selecione a opção **Otimizar as configurações do Agente de Rede para a infraestrutura virtual**.

Selecionar essas opções alterará as configurações do Agente de Rede para que os seguintes recursos permaneçam desativados por padrão (antes da política ser aplicada):

- Recuperar informações sobre o software instalado
- Recuperar informações sobre o hardware
- Recuperar informações sobre as vulnerabilidades detectadas
- Recuperar informações sobre as atualizações necessárias

Normalmente, aqueles recursos não são necessários em máquinas virtuais porque elas usam o software uniforme e o hardware virtual.

A desativação dos recursos é irreversível. Se algum dos recursos desativados for necessário, você pode ativá-lo através da política do Agente de Rede ou através das configurações locais do Agente de Rede. As configurações locais do Agente de Rede estão disponíveis através do menu de contexto do dispositivo relevante no Console de Administração.

Suporte de máquinas virtuais dinâmicas

O Kaspersky Security Center Cloud Console é compatível com as máquinas virtuais dinâmicas. Se uma infraestrutura virtual tiver sido implementada na rede da organização, as máquinas virtuais dinâmicas (temporárias) podem ser usadas em determinados casos. As VMs dinâmicas são criadas sob nomes únicos com base em um modelo que foi preparado pelo administrador. O usuário trabalha em uma VM durante algum tempo, então, depois ser desligada, esta máquina virtual será removida da infraestrutura virtual. Se o Kaspersky Security Center tiver sido implementado na rede da organização, uma máquina virtual com o Agente de Rede instalado será adicionada ao banco de dados do Servidor de Administração. Depois que você desliga uma máquina virtual, a entrada correspondente também deve ser removida do banco de dados do Servidor de Administração.

Para tornar funcional o recurso de remoção automática de entradas em máquinas virtuais, ao instalar o Agente de Rede em um modelo para máquinas virtuais dinâmicas, selecione a opção **Ativar modo dinâmico para VDI**:

- Para a instalação remota - na janela de propriedades do pacote de instalação do Agente de Rede (seção **Avançado**)
- Para a instalação interativa - No Assistente de instalação do Agente de Rede

> Evite selecionar a opção **Ativar modo dinâmico para VDI** ao instalar o Agente de Rede em dispositivos físicos.

Se desejar que os eventos das máquinas virtuais dinâmicas sejam armazenados no Servidor de Administração durante algum tempo após essas máquinas virtuais serem removidas, então, na janela Propriedades do Servidor de Administração, na seção **Repositório de eventos**, selecione a opção **Armazenar eventos após a exclusão dos dispositivos** e especifique o período máximo de armazenamento para eventos (em dias).

> Não recomendamos ativar a criptografia de unidade em máquinas virtuais dinâmicas.

Suporte para copiar máquinas virtuais

Copiar uma máquina virtual com o Agente de Rede instalado ou criar um a partir de um modelo com o Agente de Rede instalado, é idêntico a implementação de Agentes de Rede ao capturar e copiar uma imagem do disco rígido. Deste modo, no caso geral, ao copiar máquinas virtuais, você tem de executar as mesmas ações feitas ao implementar o Agente de Rede copiando uma imagem do disco.

No entanto, as duas caixas descritas abaixo apresentam o Agente de Rede que detecta a cópia automaticamente. Devido aos motivos acima, você não tem que executar as operações sofisticadas descritas sob "Implementar ao capturar e copiar o disco rígido de um dispositivo":

- A opção **Ativar modo dinâmico para VDI** foi selecionada durante a instalação do Agente de Rede. Após cada reinicialização do sistema operacional, esta máquina virtual será reconhecida como um novo dispositivo, independentemente de ter sido copiada ou não.

- Um dos seguintes hypervisors está em uso: VMware™, HyperV®, ou Xen®: o Agente de Rede detecta a cópia da máquina virtual através das IDs alteradas do hardware virtual.

A análise das modificações no hardware virtual não é absolutamente confiável. Antes de aplicar este método amplamente, você deve testá-lo em um pequeno conjunto de máquinas virtuais da versão do hypervisor atualmente usado na sua organização.

O suporte do sistema de arquivos reverte para dispositivos com o Agente de Rede

O Kaspersky Security Center é um aplicativo distribuído. Reverter o sistema de arquivos a um estado anterior em um dispositivo com o Agente de Rede instalado conduzirá a dessincronização e ao funcionamento impróprio do Kaspersky Security Center.

O sistema de arquivos (ou uma parte dele) pode ser revertido nos seguintes casos:

- Ao copiar uma imagem do disco rígido.

- Ao restaurar um estado da máquina virtual por meio da infraestrutura virtual.

- Ao restaurar os dados de uma cópia backup ou de um ponto de recuperação.

Os cenários sob os quais o software de terceiros nos dispositivos com o Agente de Rede instalado que afetam a pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ somente são cenários críticos para o Kaspersky Security Center. Portanto, você sempre deve excluir esta pasta do procedimento de recuperação, se possível.

Como as regras do local de trabalho de algumas organizações compreendem a possibilidade para a reversão do sistema de arquivos em dispositivos, o suporte para a reversão do sistema de arquivos em dispositivos com o Agente de Rede instalado foi adicionado ao Kaspersky Security Center, a partir da versão 10 Maintenance Release 1 (Servidor de Administração e os Agentes de Rede devem ser da versão 10 Maintenance Release 1 ou posterior). Quando detectado, estes dispositivos são automaticamente reconectados ao Servidor de Administração com a total limpeza dos dados e a total sincronização.

Por padrão, o suporte da reversão de detecção do sistema de arquivos está ativado no Kaspersky Security Center 14.2.

Tanto quanto possível, evite reverter a pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\ nos dispositivos com o Agente de Rede instalado, porque a ressincronização completa dos dados requer uma grande quantidade de recursos.

A reversão do estado de sistema não é absolutamente permitida em um dispositivo com o Servidor de Administração instalado. A reversão do banco de dados também não é usada pelo Servidor de Administração.

Você pode restaurar um estado do Servidor de Administração a partir de uma cópia backup somente com o utilitário klbackup padrão.

Sobre a configuração de perfis de conexão para usuários ausentes

Os usuários ausentes de laptops (aqui também referidos como "dispositivos") podem precisar alterar o método da conexão a um Servidor de Administração ou alternar entre Servidores de Administração dependendo da localização atual do dispositivo na rede corporativa.

Os perfis de conexão têm suporte somente para dispositivos que executam Windows e macOS.

Usar endereços diferentes de um Servidor de Administração único

Os dispositivos com o Agente de Rede instalado podem conectar-se ao Servidor de Administração da intranet da organização ou a partir da Internet. Esta situação pode necessitar que o Agente de Rede use endereços diferentes para a conexão ao Servidor de Administração: o endereço do Servidor de Administração externo para a conexão com a Internet e o endereço do Servidor de Administração interno para a conexão da rede interna.

Para fazer isto, você deve adicionar um perfil (para a conexão ao Servidor de Administração a partir da Internet) à política do Agente de Rede. Adicione o perfil nas propriedades da política (Seção **Conectividade**, subsecção **Perfis de conexão**). Na janela de criação do perfil, você deve desativar a opção **Usar somente para receber atualizações** e selecionar a opção **Sincronizar as configurações de conexão com as configurações do Servidor de Administração especificadas nesse perfil**. Se você usa um gateway de conexão para acessar o Servidor de Administração (por exemplo, em uma configuração do Kaspersky Security Center que está descrita em No acesso à Internet: Agente de Rede como um gateway de conexão em DMZ), deverá especificar o endereço do gateway de conexão no campo correspondente do perfil de conexão.

Alternar entre Servidores de Administração dependendo da rede atual

Se a organização tiver múltiplos escritórios com diferentes Servidores de Administração e alguns dispositivos com o Agente de Rede instalado se moverem entre eles, você precisa do Agente de Rede para conectar-se ao Servidor de Administração da rede local no escritório onde o dispositivo está atualmente localizado.

Neste caso, você deve criar um perfil para a conexão ao Servidor de Administração nas propriedades da política do Agente de Rede de cada um dos escritórios, exceto para o escritório doméstico onde o Servidor de Administração mestre original esteja localizado. Você deve especificar os endereços dos Servidores de Administração em perfis de conexão e ativar ou desativar a opção **Usar somente para receber atualizações**:

- Selecione a opção se você precisar que o Agente de Rede seja sincronizado com o Servidor de Administração mestre, usando o Servidor local somente para baixar as atualizações.
- Desative a opção se for necessário que o Agente de Rede seja gerenciado completamente pelo Servidor de Administração local.

Após isso, você deve definir as condições da troca para os perfis recém criados: ao menos uma condição de cada um dos escritórios, exceto para o escritório doméstico. Cada propósito de condição consiste na detecção de itens que são específicos para o ambiente de rede de um escritório. Se uma condição for verdadeira, o perfil correspondente é ativado. Se nenhuma das condições for verdadeira, o Agente de Rede alterna para o Servidor de Administração mestre.

Implementar o recurso de Gerenciamento de dispositivos móveis

Esta seção providencia informação da implementação inicial da função Gerenciamento de dispositivos móveis.

Conectar dispositivos KES ao Servidor de Administração

Dependendo do método usado para a conexão de dispositivos ao Servidor de Administração, dois esquemas de implementação são possíveis para o Kaspersky Device Management for iOS para dispositivo KES:

- Esquema de implementação com conexão direta dos dispositivos ao Servidor de Administração
- Esquema de implementação envolvendo um proxy reverso que dá suporte à delegação restrita de Kerberos

Conexão direta de dispositivos ao Servidor de Administração

Os dispositivos KES podem conectar-se diretamente à porta 13292 do Servidor de Administração.

Dependendo do método usado para a autenticação, duas opções são possíveis para a conexão de dispositivos KES ao Servidor de Administração:

- Conectar dispositivos com um certificado do usuário
- Conectar dispositivos sem um certificado do usuário

Conectar um dispositivo com um certificado do usuário

Ao conectar um dispositivo com um certificado do usuário, aquele dispositivo é associado com a conta de usuário à qual o certificado correspondente foi atribuído através das ferramentas do Servidor de Administração.

Neste caso, a autenticação SSL de duas vias (autenticação mútua) será usada. Tanto o Servidor de Administração quanto o dispositivo serão autenticados com certificados.

Conectar um dispositivo sem um certificado do usuário

Ao conectar um dispositivo sem um certificado do usuário, aquele dispositivo não se associa com nenhuma das contas de usuário no Servidor de Administração. No entanto, quando o dispositivo recebe qualquer certificado, ele é associado ao usuário ao qual o certificado correspondente foi atribuído através das ferramentas do Servidor de Administração.

Ao conectar aquele dispositivo ao Servidor de Administração, a autenticação SSL bilateral será aplicada, o que significa que somente o Servidor de Administração será autenticado com o certificado. Após o dispositivo recuperar o certificado do usuário, o tipo de autenticação mudará para a autenticação SSL bilateral (autenticação bilateral SSL, autenticação mútua).

Esquema para conectar dispositivos KES ao servidor envolvendo a delegação de restrição Kerberos (KCD)

O esquema para conectar dispositivos KES ao Servidor de Administração envolvendo a delegação restringida Kerberos (KCD) fornece o seguinte:

- Integração com um proxy reverso compatível com KCD.
- Uso do Kerberos Constrained Delegation (aqui referido como KCD) para a autenticação de dispositivos móveis.
- Integração com a Infraestrutura de chaves públicas (aqui referida como PKI) para aplicar certificados de usuário.

Ao usar este esquema de conexão, observe o seguinte:

- O tipo de conexão dos dispositivos KES com o proxy reverso deve ser "autenticação SSL bilateral", ou seja, um dispositivo deve se conectar ao proxy reverso por meio de seu certificado do usuário proprietário. Para fazer isto, você deve integrar o certificado do usuário no pacote de instalação de Kaspersky Endpoint Security for Android que foi instalado no dispositivo. Este pacote KES deve ser criado pelo Servidor de Administração especificamente para este dispositivo (usuário).
- Você deve especificar o certificado especial (personalizado) em vez do certificado de servidor padrão para o protocolo móvel:

  1. Na janela de propriedades do Servidor de Administração, na seção **Configurações**, marque a caixa de seleção **Abrir a porta para dispositivos móveis** e selecione **Adicionar certificado** na lista suspensa.
  2. Na janela exibida, especifique o mesmo certificado definido no proxy reverso quando o ponto de acesso ao protocolo móvel foi publicado no Servidor de Administração.

- Os certificados de usuário de dispositivos KES devem ser emitidos por Certificate Authority (CA) do domínio. Não se esqueça de que, se o domínio incluir CAs de múltiplas raízes, os certificados de usuário devem ser emitidos pela CA, definida na publicação no proxy reverso.

  Você pode assegurar-se de que o certificado do usuário esteja em conformidade com requisito acima descrito, usando um dos seguintes métodos:

  - Especifique o certificado do usuário especial no Assistente de novo pacote e no Assistente de instalação de certificados.
  - Integre o Servidor de Administração com o PKI do domínio e defina a configuração correspondente nas regras de emissão de certificados:

    1. Na árvore do console, expanda a pasta **Gerenciamento de Dispositivos Móveis** e selecione a subpasta **Certificados**.
    2. No espaço de trabalho da pasta **Certificados**, clique no botão **Configurar as regras de emissão de certificados** para abrir a janela **Regras de emissão do certificado**.
    3. Na seção **Integração com PKI**, configure a integração com a infraestrutura de chaves públicas.
    4. Na seção **Emissão de certificados móveis**, especifique a origem dos certificados.

Abaixo encontra-se um exemplo da Kerberos Constrained Delegation (KCD) com as seguintes suposições:

- O ponto do acesso ao protocolo móvel no Servidor de Administração é definido na porta 13292.
- O nome do dispositivo com o proxy reverso é firewall.mydom.local.
- O nome do dispositivo com o Servidor de Administração é ksc.mydom.local.
- O nome da publicação externa do ponto de acesso ao protocolo móvel é kes4mob.mydom.global.

Conta de domínio para o Servidor de Administração

Você deve criar uma conta de domínio (por exemplo, KSCMobileSrvcUsr) sob a qual o serviço Servidor de Administração será executado. Você pode especificar uma conta do serviço Servidor de Administração ao instalar o Servidor de Administração ou através do utilitário klsrvswch. O utilitário klsrvswch está localizado na pasta de instalação do Servidor de Administração. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

Uma conta de domínio deve ser especificada pelos seguintes motivos:

- O recurso para o gerenciamento de dispositivos KES é uma parte integral do Servidor de Administração.
- Para assegurar um funcionamento apropriado do Kerberos Constrained Delegation (KCD), o lado recebedor (ou seja, o Servidor de Administração) deve ser executado sob uma conta de domínio.

Nome do serviço principal para http/kes4mob.mydom.local

No domínio, sob a conta KSCMobileSrvcUsr, adicione um SPN para publicar o serviço de protocolo móvel na porta 13292 do dispositivo com o Servidor de Administração. Para o dispositivo kes4mob.mydom.local com o Servidor de Administração, isto aparecerá como segue:

```
setspn -a http/kes4mob.mydom.local:13292 mydom\KSCMobileSrvcUsr
```

Configuração das propriedades de domínio do dispositivo com o proxy reverso (firewall.mydom.local)

Para delegar o tráfego, é necessário confiar o dispositivo com o proxy reverso (firewall.mydom.local) ao serviço definido pelo SPN (http/kes4mob.mydom.local:13292).

Para confiar o dispositivo com proxy reverso ao serviço definido pelo SPN (http/kes4mob.mydom.local:13292), o administrador deve executar as seguintes ações:

1. No snap-in Microsoft Management Console nomeado “usuários e computadores do Active Directory”, selecione o dispositivo com o proxy reverso instalado (firewall.mydom.local).
2. Nas propriedades do dispositivo, na guia **Delegação**, defina **Confiar neste computador somente para a delegação ao serviço especificado** alterne para **Usar qualquer protocolo de autenticação**.
3. Na lista **Serviços aos quais esta conta pode apresentar credenciais delegadas**, adicione o SPN http/kes4mob.mydom.local:13292.

Certificado especial (personalizado) para a publicação (kes4mob.mydom.global)

Para publicar o protocolo móvel do Servidor de Administração, você deve emitir um certificado especial (personalizado) para o FQDN kes4mob.mydom.global e especificá-lo em vez do certificado de servidor padrão nas configurações do protocolo móvel do Servidor de Administração no Console de Administração. Para fazer isso, na janela de propriedades do Servidor de Administração, na seção **Configurações**, selecione a caixa de seleção **Abrir a porta para dispositivos móveis** e, a seguir, selecione **Adicionar certificado** na lista suspensa.

Observe que o contêiner de certificado do servidor (arquivo com a extensão p12 ou pfx) também deve conter uma cadeia de certificados raiz (chaves públicas).

Configuração da publicação no proxy reverso

No proxy reverso, para o tráfego que vai de um dispositivo móvel até a porta 13292 do kes4mob.mydom.global, é necessário configurar a KCD no SPN (http/kes4mob.mydom.global:13292) usando o certificado emitido para o FQND (kes4mob.mydom.global). Observe que publicar e ponto de acesso publicado (porta 13292 do Servidor de Administração) deve compartilhar o mesmo certificado de servidor.

Usar o Firebase Cloud Messaging

Para assegurar a entrega em tempo dos comandos para dispositivos KES gerenciados pela sistema operacional Android, o Kaspersky Security Center usa o mecanismo de notificações push. As notificações push são trocadas entre os dispositivos KES e o Servidor de Administração por meio do Firebase Cloud Messaging (aqui referido como FCM). No Console de Administração do Kaspersky Security Center, é possível especificar as configurações do Firebase Cloud Messaging para conectar dispositivos KES ao serviço.

Para recuperar as configurações do Firebase Cloud Messaging, é necessário ter uma conta do Google.

Para ativar o uso do FCM:

1. No console de administração, selecione o nó **Gerenciamento de Dispositivos Móveis** e a pasta **Dispositivos móveis**.
2. No menu de contexto da pasta **Dispositivos móveis**, selecione **Propriedades**.
3. Nas propriedades da pasta, selecione a seção **Configurações do Google Firebase Cloud Messaging**.
4. No campo **ID do Remetente**, especifique o ID do remetente do FCM.
5. No campo **Arquivo de chave privada (em formato JSON)**, selecione o arquivo de chave privada.

   Na próxima sincronização com o Servidor de Administração, os dispositivos KES gerenciados por sistemas operacionais Android serão conectados ao Firebase Cloud Messaging.

É possível editar as configurações do Firebase Cloud Messaging clicando no botão **Redefinir as configurações**.

Ao alternar para um projeto diferente do Firebase, é necessário aguardar 10 minutos para que o FCM seja retomado.

O serviço FCM é executado nas seguintes faixas de endereços:

- Do dispositivo KES, o acesso é necessário às portas 443 (HTTPS), 5228 (HTTPS), 5229 (HTTPS) e 5230 (HTTPS) dos seguintes endereços:
  - google.com
  - fcm.googleapis.com
  - android.apis.google.com
  - Todos dos endereços IP listados no ASN da Google de 15169
- No Servidor de Administração, o acesso é necessário à porta 443 (HTTPS) dos seguintes endereços:
  - fcm.googleapis.com
  - Todos dos endereços IP listados no ASN da Google de 15169

Se as configurações do servidor proxy (**Avançado** / **Configurações de conexão à Internet**) tiverem sido especificadas nas propriedades do Servidor de Administração no Console de Administração, elas serão usadas para a interação com o FCM.

Como configurar o FCM: obter o ID do remetente e o arquivo de chave privada

Para configurar o FCM:

1. Registre-se no portal do Google.
2. Acesse o Console do Firebase.
3. Execute uma das seguintes ações:
   - Para criar um novo projeto, clique em **Criar um projeto** e siga as instruções na tela.
   - Abra um projeto existente.
4. Clique no ícone de engrenagem e escolha **Configurações do projeto**.

   A janela **Configurações do projeto** é aberta.
5. Selecione a guia **Mensagens na nuvem**.
6. Obtenha o ID do remetente relevante no campo **ID do remetente** na seção **Firebase Cloud Messaging API (V1)**.
7. Selecione a guia **Contas de serviço** e clique em **Gerar nova chave privada**.
8. Na janela exibida, clique em **Gerar chave** para gerar e baixar um arquivo de chave privada.

O Firebase Cloud Messaging agora está configurado.

Integração com a infraestrutura de chaves públicas

A integração com a infraestrutura de chaves públicas (aqui referido como PKI) é principalmente destinada para simplificar a emissão de certificados de usuário de domínio pelo Servidor de Administração.

O administrador pode atribuir um certificado de domínio para um usuário no Console de Administração. Isto pode ser feito usando um dos seguintes métodos:

- Atribuir ao usuário um certificado especial (personalizado) de um arquivo no Assistente de instalação de certificados.
- Execute a integração com PKI e atribua o PKI a atuar como a fonte de certificados de um tipo específico de certificados ou para todos os tipos de certificados.

As configurações de integração com a PKI estão disponíveis na área de trabalho da pasta **Gerenciamento de Dispositivos Móveis** / **Certificados** ao clicar no link **Integrar com infraestrutura de chave pública**.

Princípio geral de integração com PKI para a emissão de certificados de usuário de domínio

No Console de Administração, clique no link **Integrar com infraestrutura de chave pública** no espaço de trabalho da pasta **Gerenciamento de Dispositivos Móveis** / **Certificados** que será usada pelo Servidor de Administração para emitir os certificados do usuário do domínio através do CA do domínio CA (aqui referido como a conta sob a qual a integração com PKI é executada).

Observe o seguinte:

- As configurações da integração com PKI fornecem-lhe a possibilidade de especificar o modelo padrão para todos os tipos de certificados. Observe que as regras de emissão de certificados (disponível no espaço de trabalho da pasta **Gerenciamento de Dispositivos Móveis**/**Certificados** clicando no botão **Configurar as regras de emissão de certificados**) permitem especificar um modelo individual para cada tipo de certificado.
- Um certificado de Enrollment Agent (EA) especial deve ser instalado no dispositivo com o Servidor de Administração, no repositório de certificados da conta sob a qual a integração com PKI é executada. O certificado Enrollment Agent (EA) é emitido pelo administrador da CA do domínio (Autoridade de Certificado).

A conta sob a qual a integração com PKI é executada deve atender os seguintes critérios:

- É um usuário do domínio.
- É um administrador local do dispositivo com o Servidor de Administração a partir do qual a integração com PKI é iniciada.
- Tem o direito de fazer *Login como serviço*.
- O dispositivo com o Servidor de Administração instalado deve ser executado ao menos uma vez sob desta conta para criar um perfil de usuário permanente.

Servidor Web do Kaspersky Security Center

O Servidor Web do Kaspersky Security Center (aqui referido como Servidor Web) é um componente do Kaspersky Security Center. O Servidor da Web foi projetado para publicar pacotes de instalação independentes, pacotes de instalação independentes para dispositivos móveis e arquivos da pasta compartilhada.

Os pacotes de instalação que foram criados são publicados no Servidor da Web automaticamente e então removidos após o primeiro download. O administrador pode enviar o novo link ao usuário de qualquer forma prática: por exemplo, por e-mail.

Ao clicar no link, o usuário poderá baixar as informações necessárias para um dispositivo móvel.

Configurações do Servidor Web

Se um ajuste fino do Servidor Web for necessário, suas propriedades lhe permitem alterar as portas para HTTP (8060) e HTTPS (8061). Além de alterar as portas, você pode substituir o certificado do servidor por HTTPS e alterar o FQDN o servidor da Web para HTTP.

Outro trabalho de rotina

Esta seção fornece recomendações no trabalho de rotina com o Kaspersky Security Center.

Monitorando as luzes de tráfego e os eventos registrados no Console de Administração

O Console de Administração permite avaliar rapidamente o status atual do Kaspersky Security Center e dos dispositivos gerenciados ao verificar os sinais luminosos. Os sinais luminosos são mostrados no espaço do nó do **Servidor de Administração**, na guia **Monitoramento**. A guia fornece seis painéis de informações com luzes de tráfego e eventos registrados. O sinal luminoso é uma barra vertical colorida no lado esquerdo de um painel. Cada painel com um sinal luminoso corresponde a um escopo funcional específico do Kaspersky Security Center (veja a tabela abaixo).

Escopos cobertos por sinais luminosos no Console de Administração

Nome do painel	Escopo do sinal luminoso
Implementação	Instalar Agente de Rede e aplicativos de segurança em dispositivos em uma rede da organização
Esquema do gerenciamento	Estrutura de grupos de administração. Verificação da rede. Regras de migração de dispositivos
Configurações de proteção	Funcionalidade do aplicativo de segurança: status de proteção, verificação de malwares
Atualizar	Atualizações e patches
Monitoramento	Status de proteção
Servidor de Administração	Recursos e propriedades do Servidor de Administração

Cada sinal luminoso pode ser para qualquer de uma destas quatro cores (veja a tabela abaixo). A cor de um sinal luminoso depende do status atual do Kaspersky Security Center e dos eventos que foram registrados.

Códigos em cores de sinais luminosos

Status	Cor do sinal luminoso	Significação da cor do sinal luminoso
Informativo	Verde	Intervenção do administrador não é necessária.
Advertência	Amarelo	Intervenção do administrador é necessária.
Crítico	Vermelho	Problemas sérios foram encontrados. A intervenção do administrador é necessária para solucioná-los.
Informativo	Azul-claro	Os eventos foram registrados e que são não relacionados com ameaças potenciais ou reais à segurança de dispositivos gerenciados.

A meta do administrador é manter verdes os sinais luminosos em todos dos painéis de informações da guia **Monitoramento**.

Os painéis de informações também mostram eventos registrados que afetam as luzes de tráfego e o status do Kaspersky Security Center (consulte a tabela abaixo).

Nome, descrição e cores das luzes de tráfego de eventos registrados

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Vermelho	**A licença expirou em %1 dispositivo(s)**	IDS_AK_STATUS_LIC_EXPAIRED	Eventos desse tipo ocorrem quando a licença comercial expirou. Uma vez ao dia, o Kaspersky Security Center verifica se a licença expirou nos dispositivos. Quando a licença comercial expirar, o Kaspersky Security Center fornecerá apenas a funcionalidade básica. Para continuar usando o Kaspersky Security Center, é necessário renovar sua licença comercial.
Vermelho	**O aplicativo de segurança não está em execução em: %1 dispositivos**	IDS_AK_STATUS_AV_NOT_RUNNING	Eventos desse tipo ocorrem quando o aplicativo de segurança instalado no dispositivo não está em execução. Verifique e confirme se o Kaspersky Endpoint Security está em execução no dispositivo.
Vermelho	**A proteção está desativada em: %1 dispositivos**	IDS_AK_STATUS_RTP_NOT_RUNNING	Eventos desse tipo ocorrem quando o aplicativo de segurança no dispositivo foi desativado por mais tempo que o intervalo especificado. Verifique o status atual da proteção em tempo real no dispositivo e confirme se todos os componentes da proteção necessários estão ativados.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Vermelho	**Foi detectada uma vulnerabilidade de software nos dispositivos**	IDS_AK_STATUS_VULNERABILITIES_FOUND	Eventos desse tipo ocorrem quando a tarefa *Encontrar vulnerabilidades e atualizações necessárias* detecta vulnerabilidades com o nível de gravidade especificado em aplicativos instalados no dispositivo. Verifique a lista de atualizações disponíveis na subpasta **Atualizações de Software** updates incluída na pasta **Gerenciamento de aplicativos**. Essa pasta contém uma lista das atualizações para aplicativos da Microsoft e para produtos de software de outros fornecedores recuperadas pelo Servidor de Administração para que possam ser distribuídas para os dispositivos. Após visualizar as informações sobre as atualizações disponíveis, instale-as nos dispositivos.
Vermelho	**Eventos críticos registrados no Servidor de Administração**	IDS_AK_STATUS_EVENTS_OCCURED	Eventos desse tipo ocorrem quando eventos críticos do Servidor de Administração são detectados. Verifique a lista de eventos armazenados no Servidor de Administração e, a seguir, corrija os eventos críticos um a um.
Vermelho	**Foram registrados erros em eventos no Servidor de Administração**	IDS_AK_STATUS_ERROR_EVENTS_OCCURED	Eventos desse tipo ocorrem quando os erros inesperados são registrados no lado do Servidor de Administração. Verifique a lista de eventos armazenados no Servidor de Administração e, a seguir, corrija os erros um a um.
Vermelho	**Conexão perdida para %1 dispositivos**	IDS_AK_STATUS_ADM_LOST_CONTROL1	Eventos desse tipo ocorrem quando a conexão entre o Servidor de Administração e o dispositivo é perdida. Visualize a lista de dispositivos desconectados e tente reconectá-los.
Vermelho	**%1 dispositivos(s) não conectado(s) ao Servidor de Administração há muito tempo**	IDS_AK_STATUS_ADM_NOT_CONNECTED1	Eventos desse tipo ocorrem quando o dispositivo não se conectou ao Servidor de Administração dentro do intervalo de tempo especificado, pois o dispositivo foi desligado. Verifique e confirme se o dispositivo está ligado e se que o Agente de Rede está em execução.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Vermelho	**%1 dispositivo(s) com status diferente de OK**	IDS_AK_STATUS_HOST_NOT_OK	Eventos desse tipo ocorrem quando o status *OK* do dispositivo conectado ao Servidor de Administração muda para *Crítico* ou *Aviso*. É possível solucionar o problema usando o utilitário de diagnóstico remoto do Kaspersky Security Center.
Vermelho	**Bancos de dados desatualizados em: %1 dispositivo(s)**	IDS_AK_STATUS_UPD_HOSTS_NOT_UPDATED	Eventos desse tipo ocorrem quando os bancos de dados de antivírus não foram atualizados no dispositivo dentro do intervalo de tempo especificado. Siga as instruções para atualizar os bancos de dados da Kaspersky.
Vermelho	**Dispositivos nos quais a verificação de atualizações do Windows Update não é executada há muito tempo: %1**	IDS_AK_STATUS_WUA_DATA_OBSOLETE	Eventos desse tipo ocorrem quando a tarefa *Executar a sincronização do Windows Update* não foi executada dentro do intervalo de tempo especificado. Siga as instruções para sincronizar as atualizações do Windows Update com o Servidor de Administração.
Vermelho	**%1 plug-in(s) do Kaspersky Security Center deve(m) ser instalado(s)**	IDS_AK_STATUS_PLUGINS_REQUIRED2	Eventos desse tipo ocorrem quando é necessário instalar plug-ins adicionais para aplicativos da Kaspersky. Baixe e instale os plug-ins de gerenciamento necessários para o aplicativo Kaspersky a partir da página da Web do Suporte Técnico da Kaspersky.
Vermelho	**As ameaças ativas são detectadas em %1 dispositivo(s)**	IDS_AK_STATUS_NONCURED_FOUND	Eventos desse tipo ocorrem quando ameaças ativas são detectadas em dispositivos gerenciados. Visualize informações sobre as ameaças detectadas e siga as recomendações.
Vermelho	**A tarefa %1 foi concluída com um erro**	IDS_AK_STATUS_TASK_FAILED	Eventos desse tipo ocorrem quando a execução de uma tarefa é concluída com um erro. Verifique as propriedades da tarefa e, a seguir, reconfigure a tarefa.
Vermelho	**Muitos vírus foram detectados em: %1 dispositivo(s)**	IDS_AK_STATUS_TOO_MANY_THREATS	Eventos desse tipo ocorrem quando vírus são detectados em dispositivos gerenciados. Visualize informações sobre os vírus detectados e siga as recomendações.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Vermelho	**Ataque de vírus**	IDS_AK_STATUS_VIRUS_OUTBREAK	Eventos deste tipo ocorrem quando o número de objetos maliciosos detectados em diversos dispositivos gerenciados exceder o limite dentro de um curto período de tempo. Visualize informações sobre as ameaças detectadas e siga as recomendações.
Vermelho	**Os bancos de dados no repositório não foram atualizados há muito tempo**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	Eventos desse tipo ocorrem quando os bancos de dados de antivírus não são atualizados no dispositivo em dois dias. Verifique a frequência de atualização dos bancos de dados de antivírus e, a seguir, atualize os bancos de dados de antivírus.
Amarelo	**Os bancos de dados no repositório não foram atualizados há muito tempo**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	Eventos desse tipo ocorrem quando os bancos de dados de antivírus não são atualizados no dispositivo por mais de um dia, mas menos de dois dias. Verifique a frequência de atualização dos bancos de dados de antivírus e, a seguir, atualize os bancos de dados de antivírus.
Amarelo	**O conflito de nomes NetBIOS foi detectado nos dispositivos**	IDS_AK_STATUS_ADM_NAME_CONFLICT	Eventos desse tipo ocorrem quando os dispositivos têm os mesmos nomes de NetBIOS. Renomeie os dispositivos.
Amarelo	**No(s) dispositivo(s) %s, a criptografia de dados mudou para o status especificado nos critérios de detecção de status do dispositivo**	IDS_AK_STATUS_ENCRYPTION_FAULTS_FOUND	Eventos desse tipo ocorrem quando a criptografia de dados falha em dispositivos gerenciados.
Amarelo	**A licença %1 expira em %2 dias**	IDS_AK_STATUS_LIC_EXPAIRING	Eventos desse tipo ocorrem quando a licença no dispositivo expira em um número de dias especificado. Para continuar usando o Kaspersky Security Center, é necessário renovar sua licença comercial.
Amarelo	**Dispositivos não atribuídos que tiveram o Agente de Rede instalado: %1**	IDS_AK_STATUS_NAGENTS_IN_UNASSIGNED	Eventos desse tipo ocorrem quando novos dispositivos são descobertos na rede. Mova os dispositivos com o Agente de Rede para os grupos de dispositivos gerenciados.
Amarelo	**Os Agentes de Rede em %1 dispositivo(s) não poderão ser executados até o reinício. Da última vez, este estado era %2**	IDS_AK_STATUS_NAGENTS_NOT_RUNNING_UNTIL_REBOOT	Eventos desse tipo ocorrem quando o Agente de Rede não está em execução nos dispositivos. Reiniciar os dispositivos.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Amarelo	**Os arquivos detectados devem ser enviados para a Kaspersky para análise adicional**	IDS_AK_STATUS_NEW_APS_FILE_APPEARED	Eventos desse tipo ocorrem quando os arquivos provavelmente infectados com vírus são detectados e movidos para a Quarentena. Envie os arquivos para a Kaspersky para análise adicional.
Amarelo	**Dispositivo(s) gerenciado(s): %1. O aplicativo de segurança está instalado em: %2 dispositivo(s)**	IDS_AK_STATUS_NO_AV	Eventos desse tipo ocorrem quando o Kaspersky Endpoint Security não está instalado em todos os dispositivos gerenciados. Instale o Kaspersky Endpoint Security em todos os dispositivos gerenciados.
Amarelo	**A tarefa de instalação %1 foi concluída com êxito em %2 dispositivo(s); a reinicialização é necessária em %3 dispositivo(s)**	IDS_AK_STATUS_RI_NEED_REBOOT	Eventos desse tipo ocorrem quando o Kaspersky Endpoint Security acaba de ser instalado em dispositivos gerenciados. Reinicialize os dispositivos após a instalação do Kaspersky Endpoint Security.
Amarelo	**A verificação de malware não foi executada por um longo tempo em: %1 dispositivo(s)**	IDS_AK_STATUS_SCAN_LATE	Eventos desse tipo ocorrem quando é necessário executar uma verificação de malware em dispositivos gerenciados. Execute uma verificação de vírus.
Amarelo	**Dispositivo(s) com vulnerabilidades de software detectadas: %1**	IDS_AK_STATUS_VULNERABLE_HOSTS_FOUND	Eventos desse tipo ocorrem quando vulnerabilidades são detectadas em um dispositivo gerenciado. Visualize as informações sobre as vulnerabilidades detectadas e as corrija.
Verde	**Dispositivo(s) gerenciado(s): %3. Dispositivo(s) não atribuído(s) detectado(s): %1**	IDS_AK_STATUS_ADM_OK1	Eventos desse tipo ocorrem quando novos dispositivos são detectados nos grupos de administração.
Verde	**O aplicativo de segurança é instalado em todos os dispositivos gerenciados**	IDS_AK_STATUS_DEPLOYMENT_OK	Eventos desse tipo ocorrem quando o Kaspersky Endpoint Security é instalado em todos os dispositivos gerenciados.
Verde	**O Kaspersky Security Center está funcionando corretamente**	IDS_AK_STATUS_GENERAL_OK	Eventos desse tipo ocorrem quando o Kaspersky Security Center está funcionando corretamente.
Verde	**O aplicativo de proteção em tempo real não está instalado**	IDS_AK_STATUS_RTP_NA	Eventos desse tipo ocorrem quando o aplicativo antivírus não está instalado nos dispositivos gerenciados.
Verde	**A proteção está ativada**	IDS_AK_STATUS_RTP_OK	Eventos desse tipo ocorrem quando a proteção em tempo real é ativada em dispositivos gerenciados.
Verde	**O aplicativo de segurança não está instalado**	IDS_AK_STATUS_SCAN_NA	Eventos desse tipo ocorrem quando o aplicativo antivírus não está instalado nos dispositivos gerenciados.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Verde	**A verificação de malware está sendo executada conforme o agendamento**	IDS_AK_STATUS_SCAN_OK	Eventos desse tipo ocorrem quando a tarefa de *Verificação de malware* está sendo executada conforme o agendamento.
Verde	**O repositório de atualizações foi atualizado pela última vez: %1**	IDS_AK_STATUS_UPD_OK	Eventos desse tipo ocorrem quando o repositório de atualizações é atualizado.
Azul-claro	**Os bancos de dados no repositório não foram atualizados há muito tempo**	IDS_AK_STATUS_UPD_SERVER_NOT_UPTODATE	Eventos desse tipo ocorrem quando os bancos de dados de antivírus são atualizados durante o dia.
Azul-claro	**A Declaração da Kaspersky Security Network aceita está obsoleta**	IDS_AK_STATUS_ACCEPTED_KSN_AGREEMENT_OBSOLETE	Eventos desse tipo ocorrem quando a Declaração da Kaspersky Security Network está desatualizada.
Azul-claro	**As atualizações de software da Kaspersky não foram aprovadas**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_NOT_APPROVED	Eventos desse tipo ocorrem quando o administrador ainda não aprovou os patches aplicáveis para os aplicativos Kaspersky gerenciados.
Azul-claro	**As atualizações do aplicativo Kaspersky foram revogadas**	IDS_AK_STATUS_APPLICABLE_KL_PATCHES_REVOKED	Eventos desse tipo ocorrem quando o administrador ainda não recusou os patches revogados.
Azul-claro	**O Contrato de Licença de Usuário Final do software móvel da Kaspersky não foi aceito**	IDS_AK_STATUS_KL_MOBILE_EULAS_NOT_ACCEPTED	Eventos desse tipo ocorrem quando o administrador ainda não aceitou o Contrato de Licença de Usuário Final para o software móvel da Kaspersky.
Azul-claro	**O Contrato de Licença de Usuário Final para atualizações de software da Kaspersky não foi aceito**	IDS_AK_STATUS_KL_PATCHES_EULAS_NOT_ACCEPTED	Eventos desse tipo ocorrem quando o administrador ainda não aceitou o Contrato de Licença de Usuário Final para as atualizações de software da Kaspersky.
Azul-claro	**A Declaração da Kaspersky Security Network para atualizações de software da Kaspersky não foi aceita**	IDS_AK_STATUS_KL_PATCHES_KSN_AGREEMENTS_NOT_ACCEPTED	Eventos desse tipo ocorrem quando o administrador ainda não aceitou a Declaração da Kaspersky Security Network para as atualizações de software da Kaspersky.
Azul-claro	**O usuário deve aceitar o Contrato de Licença para instalar as atualizações**	IDS_AK_STATUS_NEED_ACCEPT_EULA	Eventos desse tipo ocorrem quando novas atualizações estão disponíveis para instalação, mas o administrador ainda não aceitou o Contrato de Licença.
Azul-claro	**Novas versões dos aplicativos da Kaspersky estão disponíveis**	IDS_AK_STATUS_NEW_DISTRIBUTIVES_AVAILABLE	Eventos desse tipo ocorrem quando novas versões dos aplicativos Kaspersky estão disponíveis para instalação em dispositivos gerenciados.
Azul-claro	**As atualizações estão disponíveis para os componentes do Kaspersky Security Center**	IDS_AK_STATUS_NEW_KSC_VERSIONS_AVAILABLE	Eventos desse tipo ocorrem quando as atualizações estão disponíveis para os componentes do Kaspersky Security Center.

Cor do sinal luminoso	Nome de exibição do tipo de evento	Tipo de evento	Descrição
Azul-claro	**As atualizações estão disponíveis para os aplicativos da Kaspersky**	IDS_AK_STATUS_NEW_VERSIONS_AVAILABLE	Eventos desse tipo ocorrem quando as atualizações estão disponíveis para os aplicativos da Kaspersky.
Azul-claro	**A tarefa de instalação do aplicativo %1 foi concluída com êxito em %2 dispositivo(s), mas falhou em %3 dispositivo(s)**	IDS_AK_STATUS_RI_FAILED	Eventos desse tipo ocorrem quando a tarefa *Instalação do aplicativo* apenas instalou o software em alguns dispositivos no pool especificado.
Azul-claro	**Execução da tarefa de implementação - %1 (%2%%)**	IDS_AK_STATUS_RI_RUNNING	Eventos desse tipo ocorrem quando a tarefa de implementação está sendo executada em dispositivos gerenciados.
Azul-claro	**A verificação completa nunca foi executada em %1 dispositivo(s)**	IDS_AK_STATUS_SCAN_NOT_SCANNED	Eventos desse tipo ocorrem quando uma verificação completa nunca foi executada no número especificado de dispositivos.
Azul-claro	**Executando a tarefa de download da atualização (progresso: %1 %%)**	IDS_AK_STATUS_UPD_SRV_UPDATE_IN_PROGRESS	Eventos desse tipo ocorrem quando uma tarefa para baixar atualizações está sendo executada em dispositivos gerenciados.

Acesso remoto aos dispositivos gerenciados

Esta seção fornece informações sobre o acesso remoto aos dispositivos gerenciados.

Uso da opção "Não desconectar do Servidor de Administração" para fornecer conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração

Caso os servidores push não sejam usados, o Kaspersky Security Center não fornece conectividade contínua entre dispositivos gerenciados e o Servidor de Administração. Os Agentes de Rede em dispositivos gerenciados periodicamente estabelecem conexões e sincronizam com o Servidor de Administração. O intervalo entre as sessões de sincronização é definido em uma política do agente de rede. Caso seja necessária uma sincronização antecipada, o Servidor de Administração (ou um ponto de distribuição, se estiver em uso) enviará um pacote de rede assinado por uma rede IPv4 ou IPv6 para a porta UDP do agente de rede. Por padrão, o número de porta é 15000. Caso nenhuma conexão via UDP seja possível entre o Servidor de Administração e um dispositivo gerenciado por qualquer motivo, a sincronização será executada na próxima conexão regular entre o agente de rede e o Servidor de Administração dentro do intervalo de sincronização.

Algumas operações não podem ser executadas sem uma conexão antecipada entre o agente de rede e o Servidor de Administração, como executar e interromper tarefas locais, receber estatísticas de um aplicativo gerenciado ou criar um túnel. Para resolver esse problema, caso os servidores push não estejam sendo usados, será possível usar a opção **Não desconectar do Servidor de Administração** para se certificar de que haja conectividade contínua entre um dispositivo gerenciado e o Servidor de Administração.

Para fornecer conexão contínua entre um dispositivo gerenciado e o Servidor de Administração:

1. Na árvore do console, selecione a pasta **Dispositivos gerenciados**.
2. Na área de trabalho da pasta, selecione o dispositivo gerenciado com o qual deseja fornecer conectividade contínua.
3. No menu de contexto do dispositivo, selecione **Propriedades**.

   A janela de propriedades do dispositivo selecionado é aberta.
4. Na seção **Geral** da janela exibida, selecione a opção **Não desconectar do Servidor de Administração**.

A conectividade contínua é estabelecida entre o dispositivo gerenciado e o Servidor de Administração.

O número total máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada é 300.

Sobre verificar o tempo de conexão entre um dispositivo e o Servidor de Administração

Para desligar um dispositivo, o Agente de Rede notifica o Servidor de Administração sobre este evento. No Console de Administração, esse dispositivo é exibido como desligado. No entanto, o Agente de Rede não pode notificar o Servidor de Administração sobre todos tais eventos. O Servidor de Administração, portanto, periodicamente analisa o atributo **Conectado ao Servidor de Administração** (o valor deste atributo é exibido no Console de Administração, nas propriedades do dispositivo, na seção **Geral**) para cada dispositivo e compara-o com o intervalo de sincronização a partir das configurações atuais do Agente de Rede. Se um dispositivo não tiver respondido ao longo de mais de três intervalos de sincronização sucessivos, aquele dispositivo é marcado como desligado.

Sobre a sincronização forçada

Embora o Kaspersky Security Center automaticamente sincronize o status, configurações, tarefas e políticas para dispositivos gerenciados, em alguns casos o administrador precisa saber exatamente se a sincronização já foi executada para um dispositivo especificado no presente momento.

No menu de contexto dos dispositivos gerenciados no Console de Administração, o item de menu **Todas as tarefas** contém o comando **Forçar a sincronização**. Quando o Kaspersky Security Center 14.2 executa este comando, o Servidor de Administração tenta se conectar ao dispositivo. Se esta tentativa for bem sucedida, a sincronização forçada será executada. Caso contrário, a sincronização será forçada somente após a próxima conexão entre o Agente de Rede e o Servidor de Administração.

Sobre tunelamento

O Kaspersky Security Center permite o tunelamento de conexões de TCP, do Console de Administração via Servidor de Administração, e então via Agente de Rede a uma porta especificada em um dispositivo gerenciado. O tunelamento é projetado para conectar um aplicativo cliente em um dispositivo com o Console de Administração instalado à uma porta TCP em um dispositivo gerenciado – se nenhuma conexão direta for possível entre o Console de Administração e o dispositivo alvo.

Por exemplo, o tunelamento é usado para conexões a uma área de trabalho remota, para conectar-se a uma sessão existente e para criar uma nova sessão remota.

O tunelamento também pode ser ativado usando ferramentas externas. Por exemplo, o administrador pode executar o utilitário putty, o cliente VNC e outras ferramentas desta forma.

Guia de dimensionamento

Esta seção fornece informações sobre o dimensionamento do Kaspersky Security Center.

Sobre este Guia

O Guia de Dimensionamento do Kaspersky Security Center 14.2 (também conhecido como "Kaspersky Security Center") destina-se aos profissionais que instalam e administram o Kaspersky Security Center, assim como a todos os que fornecem suporte técnico a organizações que usam o Kaspersky Security Center.

Todas as recomendações e os cálculos são fornecidos para redes nas quais o Kaspersky Security Center gerencia a proteção dos dispositivos com o software da Kaspersky instalado, incluindo dispositivos móveis. Se os dispositivos móveis ou algum outro dispositivo gerenciado precisar ser considerado separadamente, isso será mencionado especificamente.

Para obter e manter o desempenho ideal sob a variação de condições operacionais, você deverá levar em conta o número de dispositivos na rede, a topologia da rede e o conjunto de recursos do Kaspersky Security Center de que você necessita.

Esta Guia fornece as seguintes informações:

- Limitações do Kaspersky Security Center
- Cálculos para os nós-chave do Kaspersky Security Center (Servidores de Administração e pontos de distribuição):
  - Requisitos de hardware para Servidores de Administração e pontos de distribuição
  - Cálculo do número e hierarquia de Servidores de Administração
  - Cálculo do número e da configuração de pontos de distribuição
- Configuração de registro de evento no banco de dados dependendo do número de dispositivos na rede
- Práticas recomendadas comuns para otimização de desempenho
- Configuração de tarefas específicas objetivadas ao ótimo desempenho do Kaspersky Security Center
- Taxa de tráfego (carga da rede) entre Servidor de Administração do Kaspersky Security Center e cada dispositivo protegido

A consulta deste guia é recomendada nos seguintes casos:

- Planejando recursos antes da instalação do Kaspersky Security Center
- Planejando mudanças significativas à escala da rede na qual o Kaspersky Security Center será implementado
- Ao mudar do Kaspersky Security Center em um segmento de rede limitado (um ambiente de teste) para a implantação em larga escala do Kaspersky Security Center na rede corporativa
- Ao efetuar modificações no conjunto de recursos do Kaspersky Security Center utilizados

Informações sobre as limitações do Kaspersky Security Center

A tabela a seguir exibe as limitações da versão atual do Kaspersky Security Center.

Limitações do Kaspersky Security Center

Tipo de limitação	Valor
Número máximo de dispositivos gerenciados por Servidor de Administração	100.000
Número máximo de dispositivos com a opção **Não desconectar do Servidor de Administração** selecionada	300
Número máximo de grupos de administração	10.000
Número de eventos a armazenar	45.000.000
Número máximo de políticas	2000
Número máximo de tarefas	2000
Número total máximo de objetos do Active Directory (unidades organizacionais, UOs) e contas de usuários, dispositivos e grupos de segurança)	1.000.000
Número máximo de perfis em uma política	100
Número máximo de Servidores de Administração secundários em um Servidor de Administração principal único	500
Número máximo de Servidores de Administração virtuais	500
O número máximo de dispositivos que um ponto de distribuição único pode cobrir (os pontos de distribuição podem cobrir dispositivos não móveis somente)	10.000
Número máximo de dispositivos que podem usar um único gateway de conexão	10.000, incluindo dispositivos móveis
Número máximo de dispositivos móveis por Servidor de Administração	100.000, menos o número de dispositivos gerenciados estacionários

Cálculos para os Servidores de Administração

Esta seção fornece o os requisitos de software e hardware para dispositivos usados como Servidores de Administração. Também são fornecidas recomendações para calcular o número e a hierarquia de Servidores de Administração dependendo da configuração da rede da organização.

Cálculo de recursos de hardware para o Servidor de Administração

Esta seção contém cálculos que fornecem a orientação para planejar recursos de hardware para o Servidor de Administração. Uma recomendação no cálculo de espaço disponível quando o recurso de Gerenciamento de patches e vulnerabilidades é usado, é fornecida separadamente.

Requisitos de hardware para o DBMS e para o Servidor de Administração

As tabelas a seguir fornecem os requisitos mínimos de hardware recomendados para um DBMS e para um Servidor de Administração obtidos durante os testes. Para obter uma lista completa de sistemas operacionais e DBMSs suportados, refira-se à lista de requisitos de hardware e software.

O Servidor de Administração e o DBMS estão em dispositivos diferentes, a rede inclui 50 mil dispositivos

Configuração do dispositivo com o Servidor de Administração instalado

Hardware	Valor
CPU	4 cores, 2.500 MHz
RAM	8 GB
Disco rígido	300 GB, RAID recomendado
Adaptador de rede	1 Gbits

Configuração do dispositivo com o DBMS instalado

Hardware	Valor
CPU	4 cores, 2.500 MHz
RAM	16 GB
Disco rígido	200 GB, SATA RAID
Adaptador de rede	1 Gbits

O Servidor de Administração e o DBMS estão no mesmo dispositivo, a rede inclui 50 mil dispositivos

Configuração do dispositivo com o Servidor de Administração e o DBMS instalados

Hardware	Valor
CPU	8 cores, 2.500 MHz
RAM	16 GB
Disco rígido	500 GB, SATA RAID
Adaptador de rede	1 Gbits

O Servidor de Administração e o DBMS estão em dispositivos diferentes, a rede inclui 100 mil dispositivos

Configuração do dispositivo com o Servidor de Administração instalado

Hardware	Valor
CPU	8 núcleos, 2,13 GHz
RAM	8 GB
Disco rígido	1 TB, com RAID
Adaptador de rede	1 Gbits

Configuração do dispositivo com o DBMS instalado

Hardware	Valor
CPU	8 núcleos, 2,53 GHz
RAM	26 GB
Disco rígido	500 GB, SATA RAID
Adaptador de rede	1 Gbits

O DBMS SQL Server na máquina virtual, a rede inclui 50 mil dispositivos

Configuração da máquina virtual com o SQL Server instalado, até 50 mil dispositivos

Recursos reservados no Hypervisor	Valor
CPU	10 GHz
RAM	16 GB
IOPS do disco	150 IOPS
Espaço livre em disco	200 GB
Compartilhamento de instâncias do SQL Server	Sem compartilhamento

DBMS SQL Server na máquina virtual, a rede inclui 100 mil dispositivos

Configuração da máquina virtual com o SQL Server instalado, até 100 mil dispositivos

Recursos reservados no Hypervisor	Valor
CPU	20 GHz
RAM	26 GB
IOPS do disco	150 IOPS
Espaço livre em disco	500 GB
Compartilhamento de instâncias do SQL Server	Sem compartilhamento

Os testes foram executados sob as seguintes configurações:

- A atribuição automática de Agentes de Atualização é ativada no Servidor de Administração, ou os pontos de distribuição são atribuídos manualmente de acordo com tabela recomendada.
- A tarefa de backup salva cópias backup em um recurso de arquivo localizado em um servidor dedicado.
- O intervalo de sincronização para Agentes de Rede é definido como especificado na tabela abaixo.

  Intervalo de sincronização para Agentes de Rede

Intervalo de sincronização (minutos)	Número de dispositivos gerenciados
15	10.000
30	20.000
45	30.000
60	40.000
75	50.000
150	100.000

Cálculo do espaço do banco de dados

A quantidade aproximada de espaço deve ser reservada no banco de dados pode ser calculado usando a seguinte fórmula:

(600 * C + 2.3 * E + 2.5 * A + 1.2 * N * F), KB

onde:

- C é o número de dispositivos.
- E é o número de eventos a armazenar.
- A é o número total do objetos do Active Directory:
  - Contas de dispositivo
  - Contas de usuário
  - Contas dos grupos de segurança
  - Unidades organizacionais do Active Directory

  Se a verificação do Active Directory estiver desativada, A é considerado como igual a zero.
- N é o número médio de arquivos executáveis inventariados em um dispositivo de endpoint.
- F é o número de dispositivos de endpoint onde os arquivos executáveis foram inventariados.

Se você planejar ativar (nas configurações da política do Kaspersky Endpoint Security) a notificação do Servidor de Administração em aplicativos que você executa, precisará de uma quantidade adicional de (0.03 * C) gigabytes para armazenar no banco de dados as informações sobre os aplicativos em execução.

Se o Servidor de Administração distribui atualizações do Windows (agindo como o servidor Windows Server Update Services), o banco de dados exigirá 2,5 GB adicionais.

Durante a operação, um determinado *espaço não alocado* sempre estará presente no banco de dados. Portanto, o tamanho real do arquivo do banco de dados, (por padrão o arquivo KAV.MDF se você usa o SQL Server como o DBMS) com frequência é de aproximadamente o dobro de tamanho do que a quantidade de espaço ocupado pelo banco de dados.

Não se recomenda limitar explicitamente o tamanho do log de transações (por padrão, o arquivo KAV_log. LDF, se você usa o SQL Server como o DBMS). Recomenda-se deixar o valor padrão do parâmetro MAXSIZE. Contudo, se você precisar limitar o tamanho desse arquivo, leve em consideração que o valor mínimo necessário típico do parâmetro MAXSIZE para KAV_log.LDF é 20.480 MB.

Cálculo de espaço em disco (sem e com o uso do recursos de Gerenciamento de vulnerabilidade e de correção)

Cálculo de espaço em disco sem o uso do recurso de Gerenciamento de patches e vulnerabilidades

O espaço em disco do Servidor de Administração necessário para a pasta %ALLUSERSPROFILE %\ApplicationData\KasperskyLab\adminkit pode ser estimado aproximadamente usando a fórmula:

(724 * C + 0.15 * E + 0.17 * A), KB

onde:

- C é o número de dispositivos.
- E é o número de eventos a armazenar.
- A é o número total do objetos do Active Directory:
  - Contas de dispositivo
  - Contas de usuário
  - Contas dos grupos de segurança
  - Unidades organizacionais do Active Directory

Se a verificação do Active Directory estiver desativada, A é considerado como igual a zero.

Cálculo de espaço em disco com o uso do recurso de Gerenciamento de patches e vulnerabilidades

- Atualizações. A pasta compartilhada requer ao menos 4 GB adicionais para armazenar as atualizações.
- Pacotes de instalação. Se alguns pacotes de instalação forem armazenados no Servidor de Administração, a pasta compartilhada necessitará de uma quantidade adicional de espaço em disco livre, igual ao tamanho total de todos os pacotes de instalação disponíveis para instalação.

- Tarefas de instalação remota. Se alguma tarefas de instalação remota estiverem presentes no Servidor de Administração, uma quantidade adicional de espaço livre no disco (na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit) igual ao tamanho total de todos os pacotes de instalação a ser instalados será necessário.

- Correções. Se o Servidor de Administração estiver envolvido na instalação de correções, uma quantidade adicional de espaço no disco será necessária:

  - A pasta de correções deve ter uma quantidade de espaço em disco igual ao tamanho total de todas as correções que foram baixadas. Por padrão, os patches são armazenados na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\.working\wusfiles.

    É possível usar o utilitário klsrvswch para especificar uma pasta diferente para armazenar patches. O utilitário klsrvswch está localizado na pasta onde o Servidor de Administração está instalado. O caminho de instalação padrão: <Disco>:\Program Files (x86)\Kaspersky Lab\Kaspersky Security Center.

    Se o Servidor de Administração for usado como o servidor WSUS, você é aconselhado a alocar ao menos 100 GB para esta pasta.

  - A pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit deve ter uma quantidade de espaço em disco igual ao tamanho total destas correções que são referenciadas por instâncias existentes da instalação da atualização (correção) e de tarefas de correção de vulnerabilidades.

Cálculo do número e configuração de Servidores de Administração

Para reduzir a carga do Servidor de Administração principal, você pode atribuir um Servidor de Administração separado à cada grupo de administração. O número de Servidores de Administração secundários não pode exceder 500 para um único Servidor de Administração principal.

Recomendamos que você crie a configuração dos Servidores de Administração em relação à configuração da sua rede corporativa.

Recomendações para conectar máquinas virtuais dinâmicas ao Kaspersky Security Center

As máquinas virtuais dinâmicas (também conhecidas como VMs dinâmicas) consomem mais recursos do que as máquinas virtuais estáticas.

Para obter mais informações sobre máquinas virtuais dinâmicas, consulte Suporte de máquinas virtuais dinâmicas.

Quando uma nova VM dinâmica é conectada, o Kaspersky Security Center cria um ícone para essa VM dinâmica no Console de Administração e move a VM dinâmica para o grupo de administração. Depois disso, a VM dinâmica é adicionada ao banco de dados do Servidor de Administração. O Servidor de Administração está totalmente sincronizado com o Agente de Rede instalado nesta VM dinâmica.

Na rede de uma organização, o Agente de Rede cria as seguintes listas de rede para cada VM dinâmica:

- Hardware

- Software instalado

- Vulnerabilidades detectadas
- Eventos e listas de arquivos executáveis do componente de Controle de Aplicativos

O Agente de Rede transfere essas listas de rede para o Servidor de Administração. O tamanho das listas de rede depende dos componentes instalados na VM dinâmica e pode afetar o desempenho do Kaspersky Security Center e do sistema de gerenciamento do banco de dados (DBMS). Observe que a carga pode crescer de forma não linear.

Após o usuário terminar de trabalhar com a VM dinâmica e desligá-la, esta máquina será removida da infraestrutura virtual e as entradas sobre esta máquina serão removidas do banco de dados do Servidor de Administração.

Todas essas ações consomem muitos recursos do banco de dados do Kaspersky Security Center e do Servidor de Administração e podem reduzir o desempenho do Kaspersky Security Center e do DBMS. Recomendamos que você conecte até 20.000 VMs dinâmicas ao Kaspersky Security Center.

Você pode conectar mais de 20.000 VMs dinâmicas ao Kaspersky Security Center se as VMs dinâmicas conectadas executarem operações padrão (por exemplo, atualizações do banco de dados) e consumirem não mais que 80% da memória e 75–80% dos núcleos disponíveis.

Alterar configurações de política, software ou sistema operacional na VM dinâmica pode reduzir ou aumentar o consumo de recursos. O consumo de 80 a 95% dos recursos é considerado ideal.

Cálculos para pontos de distribuição e gateways de conexão

Esta seção fornece os requisitos de hardware para dispositivos usados como pontos de distribuição junto com recomendações sobre como calcular o número de pontos de distribuição e os gateways conexão dependendo da configuração da rede corporativa.

Requisitos para um ponto de distribuição

Para processar até 10.000 dispositivos cliente, um ponto de distribuição deve atender aos seguintes requisitos mínimos (é fornecida uma configuração para teste):

- CPU: Intel® Core™ i7-7700 CPU, 3,60 GHz 4 núcleos.
- RAM: 8 GB.
- Espaço de armazenamento livre: 120 GB.

Não é recomendado atribuir o Servidor de Administração como um ponto de distribuição, pois isso aumentará a carga nele.

Se quaisquer tarefas de instalação remota estiverem disponíveis no Servidor de Administração, o dispositivo com o ponto de distribuição também requer uma quantidade de espaço livre em disco que seja igual ao tamanho total dos pacotes de instalação a serem instalados.

Se uma ou múltiplas instâncias da tarefa para a instalação da atualização (patch) e de correção de vulnerabilidades estiverem pendentes no Servidor de Administração, o dispositivo com o ponto de distribuição também exigirá espaço livre adicional no disco que seja igual ao dobro do tamanho total de todos os patches a serem instalados.

Se você usar o esquema quando os pontos de distribuição receberem atualizações de bancos de dados e módulos de software do aplicativo diretamente dos servidores de atualização da Kaspersky, os pontos de distribuição deverão estar conectados à Internet.

Calcular o número e a configuração de pontos de distribuição

Quanto mais dispositivos clientes uma rede contiver, mais pontos de distribuição ela exigirá. Recomendamos que você não desative a atribuição automática de pontos de distribuição. Quando a atribuição automática de pontos de distribuição estiver ativada, o Servidor de Administração atribui pontos de distribuição se o número de dispositivos clientes for bastante grande e define a sua configuração.

Usar pontos de distribuição exclusivamente atribuídos

Se você planejar usar determinados dispositivos específicos como pontos de distribuição (ou seja, servidores exclusivamente atribuídos), você pode optar por não utilizar a atribuição automática de pontos de distribuição. Neste caso, assegure-se de que os dispositivos aos quais você pretende tornar pontos de distribuição tenham volume suficiente de espaço livre em disco, não sejam desligados regularmente e estejam com o modo Suspenso desativado.

Número de pontos de distribuição exclusivamente atribuídos em uma rede que contém um segmento de rede único, com base no número de dispositivos na rede

Número de dispositivos clientes no segmento da rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Número de pontos de distribuição exclusivamente atribuídos em uma rede que contém vários segmentos de rede, com base no número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10–100	1
Mais de 100	Aceitável: (N/10.000 + 1), recomendado: (N/5000 + 2), onde N é o número de dispositivos em rede

Usar dispositivos clientes padrão (estações de trabalho) como pontos de distribuição

Se você planejar usar dispositivos clientes padrão (isto é, estações de trabalho) como pontos de distribuição, recomendamos atribuir pontos de distribuição, como mostrado nas tabelas abaixo, para evitar a carga excessiva dos canais de comunicação e do Servidor de Administração:

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém um segmento de rede único, com base no número de dispositivos na rede

Número de dispositivos clientes no segmento da rede	Número de pontos de distribuição
Menos de 300	0 (Não atribuir os pontos de distribuição)
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

O número de estações de trabalho que funcionam como pontos de distribuição em uma rede que contém vários segmentos de rede, com base no número de dispositivos na rede

Número de dispositivos cliente por segmento de rede	Número de pontos de distribuição
Menos de 10	0 (Não atribuir os pontos de distribuição)
10–30	1
31–300	2
Mais de 300	(N/300 + 1), onde N é o número de dispositivos em rede; deve haver pelo menos 3 pontos de distribuição

Se um ponto de distribuição estiver desativado (ou não disponível por algum outro motivo), os dispositivos gerenciados no escopo poderão acessar o Servidor de Administração para as atualizações.

Cálculo do número de gateways de conexão

Se você planejar usar um gateway de conexão, recomendamos que designe um dispositivo especial para essa função.

Um gateway de conexão pode cobrir no máximo 10.000 dispositivos gerenciados, inclusive dispositivos móveis.

Registro de informações sobre eventos de tarefas e políticas

Esta seção fornece os cálculos associados com o armazenamento de evento no banco de dados do Servidor de Administração e oferece recomendações sobre como minimizar o número de eventos, portanto reduzindo a carga no Servidor de Administração.

Por padrão, as propriedades de cada tarefa e política fornecem o armazenamento de todos os eventos relativos à execução da tarefa e da obrigatoriedade da política.

No entanto, se uma tarefa for executada com bastante frequência (por exemplo, mais do que uma vez por semana) e em um número bem grande de dispositivos (por exemplo, mais de 10.000), o número de eventos pode resultar ser demasiado grande e os eventos podem inundar o banco de dados. Neste caso, recomenda-se selecionar uma das duas opções nas configurações da tarefa:

- **Salvar eventos relacionados ao progresso da tarefa**. Neste caso, o banco de dados somente recebe informações sobre inicialização, andamento e conclusão da tarefa (com êxito, com uma advertência ou erro) de cada dispositivo no qual a tarefa for executada.

- **Salvar apenas os resultados da execução da tarefa**. Neste caso, o banco de dados somente recebe informações sobre a conclusão da tarefa (com êxito, com um aviso ou erro) de cada dispositivo no qual a tarefa for executada.

Se uma política tiver sido definida para um número bem grande de dispositivos (por exemplo, mais de 10.000), o número de eventos também pode resultar ser grande, e os eventos podem inundar o banco de dados. Neste caso, recomenda-se somente selecionar os eventos mais críticos nas configurações da política e ativar o seu registro. Você é aconselhado a desativar o registro de todos outros eventos.

Ao fazer isso, você reduzirá o número de eventos no banco de dados, aumentará a velocidade da execução dos cenários associados com a análise da tabela de eventos no banco de dados e abaixará o risco de que os eventos críticos sejam substituídos por um grande número de eventos.

Você também pode reduzir o período de armazenamento para eventos associados com uma tarefa ou política. O período padrão é de 7 dias para eventos relacionados à tarefa e de 30 dias para eventos relacionados à política. Ao modificar o período de armazenamento do evento, considere os procedimentos de trabalho em vigor na sua organização e quanto tempo o administrador de sistema pode dedicar à análise de cada evento.

É aconselhável modificar as configurações de armazenamento do evento em alguns dos seguintes casos:

- Os eventos relativos a modificações nos estados intermediários de tarefas de grupo e eventos relativos à aplicação de políticas correspondem a um grande percentual de todos os eventos no banco de dados do Kaspersky Security Center.

- O Log de Eventos Kaspersky começa a mostrar as entradas sobre a remoção automática de eventos quando o limite estabelecido no número total de eventos armazenados no banco de dados for excedido.

Escolha as opções de registro de evento com base na suposição de que o número ótimo de eventos que vêm de um dispositivo único por dia não deve exceder 20. Você pode aumentar este limite ligeiramente, se necessário, mas somente se o número de dispositivos na sua rede for relativamente pequeno (menos do que 10.000).

Considerações específicas e configurações ótimas de determinadas tarefas

Determinadas tarefas estão sujeitas a considerações específicas relativas ao número de dispositivos na rede. Esta seção oferece recomendações sobre a definição ótima das configurações para tais tarefas.

A descoberta de dispositivos, a tarefa de backup de dados, a tarefa de manutenção do Servidor de Administração e as tarefas de grupo para atualização do Kaspersky Endpoint Security fazem parte da funcionalidade básica do Kaspersky Security Center.

Frequência da descoberta de dispositivos

Não é aconselhável aumentar a frequência padrão da descoberta de dispositivos, já que isso pode criar uma carga excessiva nos controladores de domínio. Ao contrário, recomenda-se agendar a amostragem com a mínima frequência possível permitida pelas necessidades da sua organização. As recomendações sobre o cálculo do agendamento ótimo são fornecidas na tabela abaixo.

Agendamento da descoberta de dispositivos

Número de dispositivos na rede	Frequência da descoberta de dispositivos recomendada
Menos de 10.000	Frequência padrão ou menos
10.000 ou mais	Uma vez por dia ou menos

Tarefa de backup de dados do Servidor de Administração e tarefa de manutenção do Servidor de Administração

O Servidor de Administração para de funcionar enquanto as seguintes tarefas estão em execução:

- Backup de dados do Servidor de Administração
- Manutenção do Servidor de Administração

Enquanto estas tarefas estão em execução, o banco de dados não pode receber nenhum dado.

Você poderá ter que reagendar estas tarefas para que eles não sejam executadas ao mesmo tempo que outras tarefas de Servidor de Administração.

Tarefas de grupo para atualizar o Kaspersky Endpoint Security

Se o Servidor de Administração atuar como a fonte de atualização, a opção de agendamento recomendada para o Kaspersky Endpoint Security 10 e versões posteriores é **Quando novas atualizações são baixadas no repositório** com a caixa de seleção **Usar atraso randomizado automaticamente para início da tarefas**.

Se uma tarefa local para baixar as atualizações dos servidores da Kaspersky para o repositório que for criado em cada ponto de distribuição, o agendamento periódico é recomendado para a tarefa de atualização em grupo do Kaspersky Endpoint Security. O valor do período de randomização deve ser uma hora neste caso.

Tarefa de inventário

É possível reduzir a carga no banco de dados enquanto as informações sobre os arquivos executáveis são obtidas. Para isso, recomendamos executar uma tarefa de inventário do Kaspersky Endpoint Security em dispositivos de referência onde esteja instalado um conjunto padrão de softwares.

O número de arquivos executáveis recebidos pelo Servidor de Administração de um único dispositivo não pode exceder 150.000. Quando o Kaspersky Security Center alcançar este limite, ele não poderá receber nenhum novo arquivo.

Normalmente, o número de arquivos em um dispositivo cliente comum não excede 60.000. O número de arquivos executáveis em um servidor de arquivos pode ser maior e pode até exceder o limite de 150.000.

Medições de teste demonstraram que a tarefa de inventário tem os seguintes resultados em um dispositivo que executa o sistema operacional Windows 7 com o Kaspersky Endpoint Security 11 instalados e nenhum outro aplicativo de terceiros instalado:

- Com as caixas de seleção **Inventário de módulos DLL** e **Inventário de arquivos de script** desmarcadas: aproximadamente 3000 arquivos.
- Com as caixas de seleção **Inventário de módulos DLL** e **Inventário de arquivos de script** marcadas: 10.000 a 20.000 arquivos, dependendo do número de service packs do sistema operacional instalados.
- Com somente a caixa de seleção **Inventário de arquivos de script** marcada: aproximadamente 10.000 arquivos.

Detalhes da carga da rede espalhada entre o Servidor de Administração e os dispositivos protegidos

Esta seção fornece os resultados de medições de teste do tráfego da rede com uma descrição das condições sob as quais as medições foram executadas. Você pode usar estas informações como referência ao planejar a infraestrutura da rede e a capacidade de produtividade dos canais da rede dentro da sua organização (ou entre o Servidor de Administração e outros dispositivos da organização a proteger). Conhecendo a capacidade de produtividade da rede, você também pode estimar aproximadamente quanto tempo as diferentes operações de transmissão de dados levarão.

Consumo de tráfego sob diversos cenários

A tabela abaixo mostra os resultados dos testes de medição conduzidos no tráfego entre o Servidor de Administração e um dispositivo gerenciado em diferentes cenários.

Por padrão, os dispositivos são sincronizados com o Servidor de Administração a cada 15 minutos ou em um intervalo mais longo. Contudo, se você modificar as configurações de uma política ou tarefa no Servidor de Administração, a primeira sincronização ocorre em dispositivos aos quais a política ou tarefa for aplicável para que as novas configurações sejam transmitidas aos dispositivos.

Taxa de tráfego entre o Servidor de Administração e um dispositivo gerenciado

Cenário	Tráfego do Servidor de Administração ao dispositivo gerenciado	Tráfego de cada dispositivo gerenciado ao Servidor de Administração
Instalar o Kaspersky Endpoint Security 11.7 for Windows com bancos de dados atualizados	390 MB	3,3 MB
Instalação do Agente de Rede	75 MB	397 KB
Instalação simultânea do Agente de Rede e do Kaspersky Endpoint Security 11.7 for Windows	459 MB	3.6 MB
Atualização inicial dos bancos de dados antivírus sem atualizar os bancos de dados no pacote (se a participação na Kaspersky Security Network for desativada)	113 MB	1,8 MB
Atualização diária dos bancos de dados antivírus (caso a participação na Kaspersky Security Network esteja ativada)	22 MB	373 MB
Sincronização inicial antes da atualização dos bancos de dados em um dispositivo (transferência de políticas e tarefas)	382 KB	446 KB
Sincronização inicial após atualizar os bancos de dados em um dispositivo	20 KB	157 KB

Cenário	Tráfego do Servidor de Administração ao dispositivo gerenciado	Tráfego de cada dispositivo gerenciado ao Servidor de Administração
Sincronização sem modificações no Servidor de Administração (de acordo com o agendamento)	18 KB	23 KB
Sincronização quando uma definição única em uma política de grupo é modificada (assim que a definição for alterada)	19 KB	20 KB
Sincronização quando uma definição única em uma tarefa de grupo é modificada (assim que a definição for alterada)	14 KB	11 KB
Sincronização forçada	110 KB	109 KB
Evento **Vírus detectado** (1 vírus)	44 KB	50 KB
Evento **de Vírus detectado** (10 vírus)	58 KB	77 KB
Tráfego único após ativar a lista de registro de aplicativos	até 10 KB	até 12 KB
Tráfego diário quando a lista de registro de aplicativo está ativada	até 840 KB	até 1 MB

Uso de tráfego médio durante 24 horas

O uso médio de tráfego de 24 horas entre o Servidor de Administração e um dispositivo gerenciado é o seguinte:

- O tráfego do Servidor de Administração para o dispositivo gerenciado é 840 KB.
- O tráfego do dispositivo gerenciado para o Servidor de Administração é 1 MB.

O tráfego foi medido nas seguintes condições:

- O dispositivo gerenciado tinha o Agente de Rede e o Kaspersky Endpoint Security 11.6 for Windows instalados.
- O dispositivo não havia sido atribuído a um ponto de distribuição.
- O Gerenciamento de patches e vulnerabilidades não estava ativado.
- A frequência da sincronização com o Servidor de Administração era de 15 minutos.

Contatar o Suporte Técnico

Esta seção descreve como adquirir o suporte técnico e os termos com os quais está disponível.

Como obter suporte técnico

Caso não consiga encontrar uma solução para seu problema na documentação do Kaspersky Security Center ou em nenhuma das fontes de informação sobre o aplicativo, contate o Suporte Técnico da Kaspersky. Os especialistas do Suporte Técnico responderão a todas as suas dúvidas sobre instalação e uso do Kaspersky Security Center.

A Kaspersky fornece suporte ao Kaspersky Security Center durante seu ciclo de vida (consulte a página do ciclo de vida do suporte do aplicativo). Antes de entrar em contato com o Serviço de Suporte Técnico, leia as regras de suporte.

Você pode entrar em contato com o Suporte Técnico de uma das seguintes maneiras:

- Visitando o site de Suporte Técnico
- Enviando uma solicitação para o Suporte Técnico a partir do portal Kaspersky CompanyAccount

Suporte técnico via Kaspersky CompanyAccount

O Kaspersky CompanyAccount é um portal para empresas que usam aplicativos Kaspersky. O portal Kaspersky CompanyAccount foi projetado para facilitar a interação entre os usuários e os especialistas da Kaspersky através de solicitações online. Você pode usar o Kaspersky CompanyAccount para monitorar o status e também armazenar um histórico das suas solicitações online.

Você pode registrar todos os funcionários da sua empresa com uma única conta no Kaspersky CompanyAccount. Uma única conta permite gerenciar centralmente solicitações de funcionários registrados enviadas para a Kaspersky, além de gerenciar os privilégios desses funcionários através do Kaspersky CompanyAccount.

O portal Kaspersky CompanyAccount está disponível nos seguintes idiomas:

- Inglês
- Espanhol
- Italiano
- Alemão
- Polonês
- Português

- Russo
- Francês
- Japonês

Para saber mais sobre o Kaspersky CompanyAccount, visite o site do Suporte Técnico.

Obter arquivos de dump do Servidor de Administração

Os arquivos de dump do Servidor de Administração contêm todas as informações sobre os seus processos em um determinado momento. Os arquivos de dump do Servidor de Administração são armazenados na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\~dumps. Os arquivos de dump são armazenados enquanto o Kaspersky Security Center estiver em uso e serão excluídos permanentemente quando forem removidos. Os arquivos de dump não são enviados para o Kaspersky automaticamente.

Caso o Servidor de Administração trave, é possível entrar em contato com o Suporte Técnico da Kaspersky. Um especialista do Suporte Técnico pode solicitar o envio dos arquivos de dump do Servidor de Administração para que seja feita a análise adicional na Kaspersky.

Os arquivos de dump podem conter dados pessoais. Recomendamos proteger as informações contra acesso não autorizado antes de enviá-las à Kaspersky.

Fontes de informação sobre o aplicativo

Página do Kaspersky Security Center no site da Kaspersky

Na página do Kaspersky Security Center no site da Kaspersky, é possível exibir informações gerais sobre o aplicativo, suas funções e recursos.

Página do Kaspersky Security Center na Base de conhecimento

A *Base de Dados de Conhecimento* é uma seção do site de suporte técnico da Kaspersky.

Na página do Kaspersky Security Center na Base de conhecimento, é possível ler artigos que fornecem informações úteis, recomendações e respostas às perguntas frequentes sobre como comprar, instalar e usar o aplicativo.

Os artigos na Base de Dados de Conhecimento podem fornecer respostas às perguntas relacionadas ao Kaspersky Security Center como também a outros aplicativos Kaspersky. Os artigos na Base de dados de conhecimento também podem conter novidades sobre o suporte técnico.

Discutir questões sobre os aplicativos Kaspersky com a comunidade

Se a sua pergunta não precisar de uma resposta imediata, você pode discuti-la com os especialistas da Kaspersky e outros usuários no nosso Fórum.

No Fórum, você pode visualizar tópicos de discussão, postar seus comentários e criar novos tópicos de discussão.

> É necessária uma conexão com a Internet para acessar os recursos do site.

Se você não puder encontrar uma solução para o problema, entre em contato com o Suporte técnico.

Glossário

Administrador cliente

Um membro da equipe de uma empresa cliente que é responsável por monitorar o status da proteção antivírus.

Administrador do Kaspersky Security Center

A pessoa que gerencia a operação de aplicativos através do sistema Kaspersky Security Center de administração centralizada remota.

Administrador do provedor de serviço

Um membro da equipe em um provedor de serviço de proteção antivírus. Esse administrador efetua tarefas de instalação e manutenção em sistemas de proteção antivírus de acordo com os produtos da Kaspersky e também fornece suporte técnico aos clientes.

Agente de autenticação

Uma interface que permite concluir a autenticação para acessar discos rígidos criptografados e carregar o sistema operacional após a unidade de disco rígido do sistema ter sido criptografada.

Agente de Rede

Um componente do Kaspersky Security Center que permite a interação entre o Servidor de Administração e os aplicativos Kaspersky instalados em um nó específico da rede (estação de trabalho ou servidor). Este componente é comum a todos os aplicativos da empresa para Microsoft® Windows®. Existem versões separadas do Agente de Rede para os aplicativos da Kaspersky desenvolvidos os SO Unix e macOS.

Ambiente nuvem

Máquinas virtuais e outros recursos virtuais que são baseados em uma plataforma na nuvem e são combinados em redes.

Aplicativo incompatível

Um aplicativo antivírus de um desenvolvedor de terceiros ou um aplicativo da Kaspersky que não aceita o gerenciamento através do Kaspersky Security Center.

Arquivo de chave

Um arquivo com o formato xxxxxxxx.key que torna possível usar um aplicativo da Kaspersky com uma licença de avaliação ou licença comercial.

Ataque de vírus

Uma série de tentativas deliberadas para infectar um dispositivo com um vírus.

Ataque MITM

Man in The Middle. Um ataque à infraestrutura de TI de uma organização no qual um hacker sequestra o link de comunicação entre dois pontos de acesso, o retransmite e modifica a conexão entre esses pontos de acesso, caso necessário.

Atualização disponível

Um conjunto de atualizações dos módulos de aplicativo da Kaspersky com atualizações críticas acumuladas por um determinado período e alterações à arquitetura do aplicativo.

Atualizar

O procedimento de substituição ou inclusão de novos arquivos (bancos de dados ou módulos de aplicativo), recebidos a partir dos servidores de atualização da Kaspersky.

Backup de dados do Servidor de Administração

Cópia dos dados do Servidor de Administração para backup e subsequente restauração realizada, usando o utilitário de backup. O utilitário pode salvar:

- O banco de dados do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração)
- Informações de configuração sobre a estrutura dos grupos de administração e dispositivos cliente
- Repositório dos arquivos de instalação para instalação remota de aplicativos (conteúdo das pastas: Pacotes, Atualizações de Desinstalação)
- Certificado do Servidor de Administração

Bancos de dados antivírus

Bancos de dados que contêm informações sobre ameaças à segurança do computador conhecidas da Kaspersky na data de publicação dos bancos de dados antivírus. As entradas em bancos de dados antivírus permitem a detecção de código malicioso em objetos verificados. Bancos de dados antivírus são criados pelos especialistas da Kaspersky e são atualizados a cada hora.

Certificado compartilhado

Um certificado destinado a identificar o dispositivo móvel do usuário.

Certificado do Servidor de Administração

O certificado que o Servidor de Administração usa para os seguintes propósitos:

- Autenticação de Servidor de Administração ao conectar-se ao Console de Administração baseado em MMC ou ao Kaspersky Security Center Web Console
- Interação segura entre o Servidor de Administração e os Agentes de Rede em dispositivos gerenciados
- Autenticação de Servidores de Administração ao conectar um Servidor de Administração principal a um Servidor de Administração secundário

O certificado é criado automaticamente quando o servidor de administração é instalado e, a seguir, armazenado no servidor de administração.

Chave ativa

Uma chave usada atualmente pelo aplicativo.

Chave de acesso AWS IAM

Uma combinação consistindo na ID da chave (que se parece com "AKIAIOSFODNN7EXAMPLE") e uma chave secreta (que se parece com "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"). Este par pertence ao Usuário do IAM e é usado para obter o acesso aos serviços AWS.

Chave de licença adicional (ou chave reserva)

Uma chave que certifica que o usuário tem o direito de usar o aplicativo, mas que não está sendo usado no momento.

Configurações de Programa

As configurações do aplicativo que forem comuns para todos os tipos de tarefas e controlam a operação total do aplicativo, como: configurações de desempenho do aplicativo, configurações de relatórios e configurações de backup.

Configurações de tarefa

Configurações do aplicativo específicas para cada tipo de tarefa.

Console de Administração

Um componente do Kaspersky Security Center baseado no Windows (também chamado de Console de Administração baseado em MMC). Este componente fornece uma interface de usuário para os serviços administrativos do Servidor de Administração e do Agente de Rede.

Console de Gerenciamento AWS

A interface da Web para visualizar e gerenciar recursos AWS. Console de Gerenciamento AWS está disponível na Web em https://aws.amazon.com/pt/.

Direitos de administrador

O nível de direitos e privilégios do usuário para administração de objetos Exchange numa organização Exchange.

Dispositivo Android

Um dispositivo móvel conectado a um Servidor de Administração do Kaspersky Security Center e gerenciado pelo aplicativo Kaspersky Endpoint Security for Android.

Dispositivo de proteção UEFI

O dispositivo com a solução ou aplicativo da Kaspersky para UEFI integrado no nível da BIOS. A proteção integrada assegura a segurança do dispositivo do momento do início do sistema, enquanto a proteção nos dispositivos sem software integrado somente começa a funcionar após o início do aplicativo de segurança.

Dispositivo EAS

Um dispositivo móvel conectado ao Servidor de Administração através do protocolo Exchange ActiveSync. Os dispositivos com os sistemas operacionais iOS, Android e Windows Phone® podem ser conectados e gerenciados usando o protocolo Exchange ActiveSync.

Dispositivo KES

Um dispositivo móvel conectado a um Servidor de Administração do Kaspersky Security Center e gerenciado pelo aplicativo Kaspersky Endpoint Security for Android.

Dispositivo MDM do iOS

Um dispositivo móvel que é conectado ao Servidor de MDM do iOS através do protocolo MDM do iOS. Os dispositivos que executam sistema operacional iOS podem ser conectados e gerenciados através de protocolo MDM do iOS.

Dispositivos gerenciados

Dispositivos na rede corporativa que estão incluídos em um grupo de administração.

Domínio de difusão

A área lógica de uma rede na qual todos os nós podem intercambiar dados usando o canal de difusão no nível do OSI (Open Systems Interconnection Basic Reference Model).

Estação de trabalho do administrador

Um dispositivo no qual o Console de Administração está instalado ou que você usa para abrir o Kaspersky Security Center Web Console. Este componente fornece uma interface de gerenciamento do Kaspersky Security Center.

A estação de trabalho do administrador é usada para configurar e gerenciar o lado do servidor do Kaspersky Security Center. Usando a estação de trabalho, o administrador cria e gerencia um sistema centralizado de proteção antivírus para uma LAN corporativa, com base em aplicativos Kaspersky.

Função do IAM

Conjunto de direitos para fazer solicitações aos serviços com base no AWS. As funções do IAM não são vinculadas à um usuário específico ou grupo; elas fornecem direitos de acesso sem as chaves de acesso AWS IAM. Você pode atribuir uma função do IAM aos usuários IAM, instâncias EC2, e aplicativos com base em AWS ou serviços.

Gateway de conexão

Um *gateway de conexão* é um Agente de Rede atuando em um modo especial. Um gateway de conexão aceita conexões de outros Agentes de Rede e os canaliza para o Servidor de Administração por meio de sua própria conexão com o Servidor. Ao contrário de um Agente de Rede comum, um gateway de conexão aguarda por conexões do Servidor de Administração, em vez de estabelecer conexões com o Servidor de Administração.

Gerenciamento centralizado de aplicativos

O gerenciamento remoto de aplicativo utilizando os serviços de administração fornecidos no Kaspersky Security Center.

Gerenciamento de identidades e acesso (IAM)

O serviço AWS que ativa o gerenciamento de acesso do usuário a outros serviços e recursos AWS.

Gerenciamento direto de aplicativos

Gerenciamento de aplicativos através de interface local.

Gravidade do evento

Propriedade de um evento encontrado durante a operação de um aplicativo da Kaspersky. Existem os seguintes níveis de gravidade:

- Evento crítico
- Falha funcional
- Advertência
- Informação

Eventos do mesmo tipo podem ter níveis de gravidade diferentes dependendo da situação na qual ocorreu o evento.

Grupo de administração

Um grupo de dispositivos agrupados por função e por aplicativos da Kaspersky instalados. Os dispositivos são agrupados como uma entidade única para a conveniência de gerenciamento. Um grupo pode incluir outros grupos. As políticas de grupo e tarefas de grupo podem ser criadas para cada aplicativo instalado no grupo.

Grupo de aplicativos licenciados

Um grupo de aplicativos criado com base no critério definido pelo administrador (por exemplo, por fornecedor), para o qual as estatísticas de instalações dos dispositivos cliente são mantidas.

Grupo de funções

Um grupo de usuários de dispositivos móveis Exchange ActiveSync que recebem direitos de administrador idênticos.

HTTPS

Protocolo seguro para transferência de dados, usando criptografia, entre um navegador e um Servidor Web. HTTPS é usado para acessar informações restritas, como dados corporativos e financeiros.

Imagem de máquina da Amazon (AMI, Amazon Machine Image)

O modelo que contém a configuração do software necessária para executar a máquina virtual. Múltiplas instâncias podem ser criadas com base em uma única AMI.

Instalação forçada

O método para a instalação remota de aplicativos da Kaspersky que permite instalar o software em dispositivos cliente específicos. Para a conclusão com êxito da instalação forçada, a conta usada para essa tarefa deve ter direitos suficientes para a iniciar o aplicativo remotamente em dispositivos cliente. Esse método é recomendado para instalar aplicativos em dispositivos que executam os sistemas operacionais Microsoft Windows e que são compatíveis com essa funcionalidade.

Instalação local

Instalação de um aplicativo de segurança em um dispositivo em uma rede corporativa que supõe a inicialização de instalação manual do pacote de distribuição do aplicativo de segurança ou a inicialização manual de um pacote de instalação publicado que foi baixado previamente no dispositivo.

Instalação manual

A instalação de um aplicativo de segurança em um dispositivo na rede corporativa do pacote de distribuição. A instalação manual requer uma participação de um administrador ou outro especialista de TI. A instalação manual típica é efetuada caso a instalação remota tenha sido concluída com um erro.

Instalação remota

Instalação de aplicativos Kaspersky usando os serviços fornecidos pelo Kaspersky Security Center.

Instância Amazon EC2

Uma máquina virtual criada com base em uma imagem AMI usando Amazon Web Services.

Interface do Programa de Aplicativo AWS (AWS API)

A interface de programação do aplicativo da plataforma AWS que é usada pelo Kaspersky Security Center. Especificamente, as ferramentas AWS API são usadas para a sondagem do segmento da nuvem e para instalar o Agente de Rede nas instâncias.

JavaScript

Uma linguagem de programação que expande o desempenho de páginas da Web. As páginas da Web criadas com JavaScript podem executar funções (por exemplo, alterar a visualização de elementos da interface ou abrir janelas adicionais) sem atualizar a página da Web com novos dados de um Servidor Web. Para visualizar as páginas criadas ao utilizar o JavaScript, ative o suporte do JavaScript na configuração do seu navegador.

Kaspersky Private Security Network (KPSN)

Kaspersky Private Security Network é uma solução que dá a usuários de dispositivos com aplicativos instalados da Kaspersky acesso a bancos de dados de reputação do Kaspersky Security Network e outros dados estatísticos sem enviar dados dos dispositivos ao Kaspersky Security Network. O Kaspersky Private Security Network foi projetado para clientes corporativos que não podem participar do Kaspersky Security Network por algum dos seguintes motivos:

- Os dispositivos não estão conectados à Internet.
- A transmissão de quaisquer dados fora do país ou da LAN corporativa é proibida pela lei ou por políticas de segurança corporativas.

Kaspersky Security Network (KSN)

Uma infraestrutura de serviços online que fornece o acesso aos banco de dados da Kaspersky, que contém informações sobre a reputação de arquivos, recursos da Web e software constantemente atualizadas. O Kaspersky Security Network garante respostas mais rápidas dos aplicativos da Kaspersky quanto a ameaças, aprimora o desempenho de alguns componentes de proteção e reduz a probabilidade ocorrerem falsos positivos.

Lightweight Nagent (LWNGT)

Um protocolo para interação com o Kaspersky Endpoint Security em dispositivos móveis. O LWNGT (também chamado de protocolo móvel) funciona como um Agente de Rede sem que seja necessário instalá-lo nos dispositivos móveis.

Limite de atividade de vírus

Número máximo permitido de eventos do tipo especificado dentro de um tempo limitado; quando excedido, é interpretado como um aumento da atividade de vírus e como uma ameaça de um ataque de vírus. Este recurso é importante durante períodos de ataques de vírus, já que permite aos administradores reagirem de modo oportuno às ameaças de ataques de vírus.

Loja de aplicativos

Componente do Kaspersky Security Center. A Loja de aplicativos é usada para instalar aplicativos em dispositivos Android possuídos por usuários. A Loja de aplicativos permite publicar os arquivos APK de aplicativos e os links aos aplicativos no Google Play.

Nível de importância do patch

Atributo do patch. Há cinco níveis de importância para patches da Microsoft e para patches de terceiros:

- Crítico
- Alto
- Médio
- Baixo
- Desconhecido

O nível de importância de uma aplicação de patches de terceiros ou da aplicação de patches da Microsoft é determinado pelo nível de gravidade menos favorável entre as vulnerabilidades que os patches deveriam corrigir.

Operador do Kaspersky Security Center

Usuário que monitora o status e operação de um sistema de proteção gerenciado através do Kaspersky Security Center.

Pacote de instalação

Um conjunto de arquivos criados para a instalação remota de um aplicativo da Kaspersky usando o sistema de administração remota do Kaspersky Security Center. O pacote de instalação contém um intervalo de configurações necessárias para instalar o aplicativo e colocá-lo em funcionamento imediatamente após a instalação. As configurações correspondem aos padrões do aplicativo. O pacote de instalação é criado usando arquivos com as extensões .kpd e .kud incluídas no kit de distribuição do aplicativo.

Pasta de backup

Pasta especial para armazenamento das cópias de dados do Servidor de Administração criados usando o utilitário de backup.

Perfil

Um conjunto de configurações de Dispositivos móveis Exchange que define seu comportamento quando conectado a um Microsoft Exchange Server.

Perfil de configuração

Política que contém um conjunto de configurações e restrições para um dispositivo móvel MDM do iOS.

Perfil de MDM do iOS

Conjunto de configurações para a conexão de dispositivos móveis iOS ao Servidor de Administração. O usuário instala um perfil de MDM do iOS a um dispositivo móvel, a partir do qual o dispositivo móvel conecta-se ao Servidor de Administração.

Perfil de provisionamento

Conjunto de configurações para operação de aplicativos em dispositivos móveis iOS. Um perfil de provisionamento contém informações sobre a licença. Está associado a um aplicativo em específico.

Período da licença

Um período durante o qual você tem acesso aos recursos do aplicativo e possui direitos de usar serviços adicionais. Os serviços que você pode usar dependem do tipo de licença.

Plugin de gerenciamento

Um componente especializado que fornece a interface para o gerenciamento de aplicativos através do Console de Administração. Cada aplicativo possui seu próprio plugin. Ele está incluído em todos os aplicativos Kaspersky que podem ser gerenciados através do Kaspersky Security Center.

Política

Uma política determina as configurações de um aplicativo e gerencia a capacidade de configurar esse aplicativo em computadores dentro de um grupo de administração. Uma política individual deve ser criada para cada aplicativo. Você pode criar várias políticas para aplicativos instalados nos computadores de cada grupo de administração, mas apenas uma política pode ser aplicada a cada aplicativo por vez em um grupo de administração.

Ponto de distribuição

Um computador que tenha um Agente de Rede instalado e é usado para a distribuição da atualização, instalação remota de aplicativos, obtenção de informações sobre os computadores em um grupo de administração e/ou domínio de broadcasting. Os pontos de distribuição são projetados para reduzir a carga no Servidor de Administração durante a distribuição da atualização e para otimizar o tráfego na rede. Os pontos de distribuição podem ser atribuídos automaticamente pelo Servidor de Administração ou manualmente pelo administrador. O ponto de distribuição era anteriormente conhecido como agente de atualização.

Proprietário do dispositivo

Proprietário do dispositivo é um usuário que pode ser contatado pelo administrador quando a necessidade surgir para executar determinadas operações em um dispositivo cliente.

Proteção antivírus da rede

Um conjunto de medidas técnicas e organizacionais que reduzem a probabilidade de penetração de vírus e spam em uma rede da organização e que previnem ataques na rede, phishing e outras ameaças. A segurança da rede aumenta quando você usa aplicativos e serviços de segurança e ao aplicar e aderir à política de segurança de dados corporativa.

Provedor de serviço de proteção antivírus

Uma organização que fornece a uma organização cliente serviços de proteção antivírus com base nas soluções da Kaspersky.

Reconhecimento de Localização de Rede (NLA)

Um serviço do Windows que ajuda um sistema operacional a identificar a rede atual. O NLA faz a detecção de alterações na rede e ajusta a configuração de segurança do dispositivo.

Repositório de eventos

Uma parte do banco de dados do Servidor de Administração dedicada ao armazenamento de informações sobre eventos que ocorrem no Kaspersky Security Center.

Restauração

A realocação do objeto original da Quarentena ou Backup para sua pasta original onde o objeto foi armazenado antes de entrar na Quarentena, antes de ter sido desinfetado ou excluído, ou realocação para uma pasta definida pelo usuário.

Restauração dos dados do Servidor de Administração

Restauração dos dados do Servidor de Administração a partir de informações salvas na cópia backup usando o utilitário de backup. O utilitário pode restaurar:

- O banco de dados do Servidor de Administração (políticas, tarefas, configurações de aplicativo, eventos salvos no Servidor de Administração)
- Informações de configuração sobre a estrutura dos grupos de administração e dispositivos cliente
- Repositório dos arquivos de instalação para instalação remota de aplicativos (conteúdo das pastas: Pacotes, Atualizações de Desinstalação)
- Certificado do Servidor de Administração

Servidor de Administração

Um componente do Kaspersky Security Center que armazena centralmente informações sobre todos os aplicativos Kaspersky instalados na rede empresarial. Pode também ser usado para gerenciar estes aplicativos.

Servidor de Administração cliente (Dispositivo cliente)

Um dispositivo, servidor ou estação de trabalho no qual o Agente de Rede está instalado e os aplicativos Kaspersky gerenciados estão em execução.

Servidor de Administração Principal

Servidor de Administração principal é o Servidor de Administração que foi especificado durante a instalação do Agente de Rede. O Servidor de Administração principal pode ser usado em configurações de perfis de conexão do Agente de Rede.

Servidor de Administração virtual

Um componente do Kaspersky Security Center designado para gerenciamento do sistema de proteção de uma rede corporativa cliente.

O Servidor de Administração virtual é um caso particular de um Servidor de Administração secundário com as seguintes restrições em comparação com o Servidor de Administração físico:

- O Servidor de Administração virtual só pode ser criado no Servidor de Administração principal.
- O Servidor de Administração virtual usa o banco de dados do Servidor de Administração principal. Tarefas de backup e restauração de dados, bem como tarefas de verificação de atualização e download, não são compatíveis com um Servidor de Administração virtual.
- O Servidor virtual não é compatível com a criação de Servidores de Administração secundários (incluindo Servidores virtuais).

Servidor de dispositivos móveis

Um componente do Kaspersky Security Center que fornece acesso a dispositivos móveis e permite gerenciá-los através do Console de Administração.

Servidor de dispositivos móveis Exchange

Um componente do Kaspersky Security Center que permite conectar os dispositivos móveis Exchange ActiveSync com o Servidor de Administração.

Servidor MDM do iOS

Um componente do Kaspersky Security Center instalado em um dispositivo cliente e que permite a conexão de dispositivos móveis iOS ao Servidor de Administração e o gerenciamento de dispositivos móveis iOS através do serviço Apple Push Notifications (APNs).

Servidor Web do Kaspersky Security Center

Um componente do Kaspersky Security Center que é instalado em conjunto com o Servidor de Administração. O Servidor da Web foi projetado para a transmissão, através de uma rede, de pacotes de instalação independentes, perfis MDM do iOS e arquivos de uma pasta compartilhada.

Servidores de atualização da Kaspersky

Servidores HTTP(S) na Kaspersky a partir dos quais os aplicativos da Kaspersky baixam atualizações dos bancos de dados e módulos do aplicativo.

SSL

Um protocolo de criptografia de dados usado na Internet e em redes locais. O protocolo Secure Sockets Layer (SSL) é usado em aplicativos da Web para criar uma conexão segura entre o cliente e o servidor.

Status de proteção

Status de proteção atual, que reflete o nível de segurança do computador.

Status de proteção da rede

O status de proteção atual, o qual define a segurança dos dispositivos na rede corporativa. O status de proteção da rede inclui fatores como os aplicativos de segurança instalados, o uso de chaves de licença e o número e os tipos de ameaças detectadas.

Tarefa

Funções executadas pelo aplicativo da Kaspersky são implementadas como tarefas, tais como: Proteção do arquivo em tempo real, Verificação Completa do dispositivo, Atualização do banco de dados.

Tarefa de grupo

Uma tarefa definida para um grupo de administração e executada em todos os dispositivos cliente incluídos em tal grupo de administração.

Tarefa local

Uma tarefa definida e executada em um único computador cliente.

Tarefa para dispositivos específicos

Uma tarefa atribuída para um conjunto de dispositivos cliente a partir de grupos de administração arbitrários e executada nesses dispositivos.

Usuário do IAM

O usuário dos serviços AWS. Um usuário do IAM pode ter os direitos para executar a sondagem do segmento da nuvem.

Usuários internos

As contas dos usuários internos são usadas para trabalhar com os Servidores de Administração virtuais. O Kaspersky Security Center concede direitos de usuários reais a usuários internos do aplicativo.

As contas de usuários internos só são criadas e usadas dentro do Kaspersky Security Center. Os dados sobre os usuários internos não são transferidos para o sistema operacional. O Kaspersky Security Center autentica os usuários internos.

Validador de Integridade do Sistema do Kaspersky Security Center (SHV)

Um componente do Kaspersky Security Center concebido para verificar a operabilidade do sistema operacional em caso da operação simultânea do Kaspersky Security Center e do Microsoft NAP.

Vulnerabilidade

Uma falha de um sistema operacional ou aplicativo que pode ser explorada por desenvolvedores de malware para invadir o sistema operacional ou aplicativo e violar sua integridade. Presença de um grande número de vulnerabilidades em um sistema operacional torna seu funcionamento não confiável, porque os vírus que invadiram o sistema operacional podem causar interrupções no próprio sistema operacional e em aplicativos instalados.

Windows Server Update Services (WSUS)

Um aplicativo usado para distribuição de atualizações de aplicativos Microsoft em computadores de usuários em uma rede corporativa.

Zona desmilitarizada (DMZ)

A zona desmilitarizada é um segmento da rede local que contém servidores, os quais respondem a solicitações da Web global. Para assegurar a segurança da rede local de uma organização, o acesso à LAN a partir da zona desmilitarizada é protegido por um firewall.

Informação sobre código de terceiros

As informações sobre o código de terceiros podem ser encontradas no arquivo legal_notices.txt e armazenadas na pasta de instalação do aplicativo.

Avisos de marca registrada

As marcas comerciais e as marcas de serviço registradas são de propriedade de seus respectivos proprietários.

Adobe, Acrobat, Flash Shockwave e PostScript são marcas comerciais registradas ou marcas comerciais da Adobe nos Estados Unidos e/ou outros países.

AMD, AMD64 são marcas comerciais ou marcas registradas da Advanced Micro Devices, Inc.

Amazon, Amazon Web Services, AWS, Amazon EC2, AWS Marketplace são marcas comerciais da Amazon.com, Inc. ou de suas afiliadas.

Apache é uma marca registrada ou uma marca comercial da Apache Software Foundation.

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 são marcas comerciais da Apple Inc.

Arm é uma marca registrada da Arm Limited (ou de suas subsidiárias) nos Estados Unidos e/ou em outros lugares.

A palavra, marca e os logótipos Bluetooth são propriedade da Bluetooth SIG, Inc.

Ubuntu LTS são marcas comerciais registradas da Canonical Ltd.

Cisco Systems, Cisco, Cisco Jabber, IOS são marcas comerciais registradas ou marcas comerciais da Cisco Systems, Inc. e/ou de suas afiliadas nos Estados Unidos e em outros países específicos.

Citrix, XenServer são marcas registradas ou marcas comerciais da Cloud Software Group, Inc., e/ou suas subsidiárias nos Estados Unidos e/ou em outros países.

Corel é uma marca comercial ou marca comercial registrada da Corel Corporation e/ou de suas subsidiárias no Canadá, nos Estados Unidos e/ou em outros países.

Cloudflare, o logotipo da Cloudflare e Cloudflare Workers são marcas comerciais e/ou marcas registradas da Cloudflare, Inc. nos Estados Unidos e em outras jurisdições.

Dropbox é uma marca registrada da Dropbox, Inc.

Radmin é marca registrada da Famatech.

Firebird é uma marca comercial registrada da Firebird Foundation.

Foxit é uma marca comercial registrada da Foxit Corporation.

FreeBSD é uma marca comercial registrada da The FreeBSD Foundation.

Google, Android, Chrome, Chromium, Dalvik, Firebase, Google Chrome, Google Earth, Google Play, Google Maps, Hangouts, Google Public DNS e YouTube são marcas comerciais da Google LLC.

EulerOS, FusionCompute, FusionSphere são marcas comerciais da Huawei Technologies Co., Ltd.

Intel, Core e Xeon são marcas comerciais da Intel Corporation ou de suas subsidiárias.

IBM, QRadar são marcas comerciais da International Business Machines Corporation registradas em muitas jurisdições em todo o mundo.

Node.js é uma marca registrada da Joyent, Inc.

Linux é uma marca comercial registrada da Linus Torvalds nos Estados Unidos e em outros locais.

Logitech é uma marca registrada ou marca comercial da Logitech nos Estados Unidos e/ou em outros países.

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 são marcas comerciais registradas do grupo de empresas da Microsoft.

CVE é uma marca comercial registrada da The MITRE Corporation.

Mozilla, Firefox e Thunderbird são marcas registradas da Mozilla Foundation nos EUA e em outros países.

Novell é uma marca comercial registrada da Novell Enterprises Inc. nos Estados Unidos e em outros países.

NetWare é uma marca comercial registrada da Novell Inc. nos Estados Unidos e em outros países.

OpenSSL é uma marca registrada de propriedade da OpenSSL Software Foundation.

OpenVPN é uma marca registrada da OpenVPN, Inc.

Oracle, Java, JavaScript e TouchDown são marcas comerciais registradas da Oracle e/ou suas afiliadas.

Parallels, o logotipo da Parallels e Coherence são marcas comerciais ou marcas registradas da Parallels International GmbH.

Chef é uma marca comercial ou marca registrada da Progress Software Corporation e/ou uma de suas subsidiárias ou afiliadas nos EUA e/ou em outros países.

Puppet é uma marca comercial ou marca registrada da Puppet, Inc.

Python é uma marca comercial ou marca registrada da Python Software Foundation.

Red Hat, Fedora e Red Hat Enterprise Linux são marcas comerciais da Red Hat Inc. ou de suas subsidiárias registradas nos Estados Unidos e em outros países.

Ansible é uma marca comercial registrada da Red Hat, Inc. nos Estados Unidos e em outros países.

CentOS é uma marca comercial ou marca comercial registrada da Red Hat, Inc. ou de suas subsidiárias nos Estados Unidos e em outros países.

BlackBerry é propriedade da Research In Motion Limited e está registrada nos Estados Unidos e poderá estar registrada ou com registro pendente em outros países.

Samsung é uma marca registrada da SAMSUNG nos Estados Unidos ou outros países.

Debian é uma marca registrada da Software in the Public Interest, Inc.

Splunk, SPL são marcas comerciais e marcas comerciais registradas da Splunk Inc. nos Estados Unidos e em outros países.

SUSE é uma marca comercial registrada da SUSE LLC nos Estados Unidos e em outros locais.

A marca comercial Symbian é propriedade da Symbian Foundation Ltd.

OpenAPI é uma marca registrada da Linux Foundation.

UNIX é uma marca comercial registrada nos Estados Unidos e em outros países, licenciada exclusivamente pela X/Open Company Limited.

Zabbix é uma marca comercial registrada da Zabbix SIA.

Problemas conhecidos

O Kaspersky Security Center Web Console tem algumas limitações que não são críticas para a operação do aplicativo:

- Se você alterar a hora ou o fuso horário no seu dispositivo, será necessário reiniciar o serviço do Kaspersky Security Center Web Console.
- Caso um proxy seja usado no dispositivo e as variáveis de ambiente do proxy sejam definidas, o instalador do Kaspersky Security Center Web Console poderá travar.
- Caso o plug-in do Kaspersky Endpoint Detection and Response Optimum seja atualizado e, em seguida, o certificado do Kaspersky Security Center Web Console seja reemitido, o plug-in do Kaspersky Endpoint Detection and Response Optimum será automaticamente revertido para a versão incluída no kit de distribuição.
- Quando a tarefa *Baixar atualizações para os repositórios de pontos de distribuição* ou *Verificação de atualizações* é importada, a opção **Selecionar dispositivos aos quais a tarefa será atribuída** é ativada. Essas tarefas não podem ser atribuídas para uma seleção de dispositivos ou dispositivos específicos. Caso a tarefa *Baixar atualizações aos repositórios de pontos de distribuição* ou *Verificação de atualizações* seja atribuída aos dispositivos específicos, ela será importada incorretamente.
- Se você executar a sondagem do Active Directory usando um ponto de distribuição do Linux com o Agente de Rede versão 15 instalado, poderá sondar somente domínios do Active Directory para os quais o endereço e as credenciais do usuário foram especificados. A sondagem do domínio atual do Active Directory e da floresta de domínios do Active Directory não está disponível.
- Caso uma regra de Controle de Aplicativos seja baseada em uma categoria de aplicativos que inclua aplicativos detectados em dispositivos Linux, a regra não funcionará. Ao selecionar os aplicativos a partir do registro de aplicativos para adicioná-los a uma categoria de aplicativos, verifique e confirme se os aplicativos detectados em dispositivos Windows foram selecionados.
- Caso um aplicativo da seção de **Registro de aplicativos** tenha sido detectado em um dispositivo Linux, as propriedades do aplicativo não conterão as informações sobre os arquivos executáveis relacionados.
- Caso o Agente de Rede seja instalado em um dispositivo que executa o sistema operacional ALT Linux por meio de uma tarefa de instalação remota e essa tarefa seja executada em uma conta sem privilégios root, a tarefa falhará. Execute a tarefa de instalação remota sob a conta root ou crie e use um pacote de instalação independente do Agente de Rede para instalar o aplicativo localmente.
- Caso a lista contenha mais de 20 itens que são exibidos em várias páginas e o usuário marque a caixa de seleção **Selecionar tudo**, o Web Console selecionará apenas os itens exibidos na página atual. Observe que isso não se aplica às listas nas seções **Dispositivos gerenciados**, **Seleções de dispositivos** e **Tarefas**, onde é possível selecionar todos os itens da lista.
- Após a conclusão de uma tarefa local de *Verificação de IOC*, o status da tarefa é exibido como *Agendado*.
- Os dispositivos cliente podem não ser encontrados após a sondagem de rede do Windows.
- Na política do Kaspersky Endpoint Security for Windows, ao selecionar e aplicar uma categoria de aplicativo durante a configuração do recurso Controle de Aplicativos, a categoria é aplicada, mas não é exibida como selecionada depois que a política é salva e reaberta.
- Após desabilitar o serviço de Proxy da KSN, os dispositivos do grupo Dispositivos gerenciados mudam de status para *Crítico*, mas os dispositivos em subgrupos são exibidos com status *OK*.

- Caso o agrupamento com distinção entre maiúsculas e minúsculas seja definido para o banco de dados usado no Kaspersky Security Center, use o mesmo modelo ao especificar um nome DNS nas regras de movimentação do dispositivo e regras de marcação automática. Caso contrário, as regras não funcionarão.

- No **Assistente para Adicionar Servidor de Administração secundário**, caso queira especificar uma conta com verificação em duas etapas ativada para autenticação no futuro Servidor secundário, o assistente terminará com um erro. Para resolver esse problema, especifique uma conta para a qual a verificação em duas etapas está desativada ou crie a hierarquia do futuro Servidor secundário.

- Ao entrar no Kaspersky Security Center Web Console, se você usar autenticação de domínio e especificar um Servidor de Administração virtual ao qual se conectar, e, em seguida, sair e tentar entrar no Servidor de Administração principal, o Kaspersky Security Center Web Console se conectará com o Servidor de Administração virtual. Para se conectar ao Servidor de Administração principal, reabra o navegador.

- Um status incorreto de uma tarefa local pode ser exibido na lista de tarefas nas propriedades do dispositivo.

- A pesquisa de rede rápida/completa do Windows retorna um resultado vazio.

- Caso o Kaspersky Security Center Web Console seja instalado com o Identity and Access Manager e, em seguida, o Servidor de Administração for alterado para o Kaspersky Security Center Web Console, o Identity and Access Manager não obterá as informações sobre o novo Servidor de Administração.

- Se o Kaspersky Security Center Web Console for aberto em navegadores diferentes e for baixado o arquivo de certificado do Servidor de Administração na janela de propriedades do Servidor de Administração, os arquivos baixados terão nomes diferentes.

- Ocorre um erro ao tentar restaurar um objeto do repositório **Backup** (**Operações → Repositórios → Backup**) ou enviar o objeto para a Kaspersky.

- Um dispositivo gerenciado que possui mais de um adaptador de rede envia informações ao Servidor de Administração sobre o endereço MAC do adaptador de rede que não é aquele usado para se conectar ao Servidor de Administração.

- Caso o Kaspersky Security Center Web Console seja instalado com o Identity and Access Manager e, em seguida, o Servidor de Administração for alterado para o Kaspersky Security Center Web Console, o Identity and Access Manager não obterá as informações sobre o novo Servidor de Administração.

- Caso uma tarefa Executar scripts seja iniciada remotamente para uma conta especificada e uma conta para a qual ela foi atribuída seja alterada nas configurações da tarefa, as alterações não serão salvas. Para alterar a conta para a qual a tarefa está atribuída, pare a tarefa nas configurações da tarefa e reinicie-a.